FIAU Implementing Procedures

CAMILLERI PREZIOSI
ADVOCATES

16th November 2021

Dr Kyra Borg

www.21Academy.education

Agenda

- Introduction
- Subject Persons
- Implementing Procedures
- Key Obligations
- Risk Assessments
- Record-keeping
- Suspicious Transaction Reporting
- Training and Awareness
- Questions

CAMILLERI PREZIOSI
ADVOCATES

Subject Persons

RELEVANT ACTIVITY	RELEVANT FINANCIAL BUSINESS

i.e. the activity of the following persons when acting in the exercise of their professional activities:
 	
• Auditors, external accountants and tax advisors, notaries and other legal professionals when they participate in any financial or real estate transactions or by assisting in the planning or carrying out of transactions for their clients concerning, inter alia, the:
  • buying and selling of property or business entities;
  • opening or management of bank accounts;
  • Creation, operation or management of companies, trusts, foundations or similar structures, or when acting as a trus or CSP.
 	
• Real estate agents where the monthly rent amounts to €10,000 or more
 	
• Licensed casino and gaming operators
 	
• Any persons trading in goods where a transaction involves in case in an amount of 10,000 € or more
	i.e. activities carried out by, inter alios:
	
	• Credit institutions (banks)
	
	• Payment institutions
	
	• Electronic money institutions
	
	• Insurance undertakings carrying out long term insurance business (other than the business of reinsurance) and intermediaries carrying out distribution activities related to long-term insurance business
	
	• Collective investment schemes
	
	• Service providers under the Investment Services Act
	
	• Service providers under the Retirement Pension Act
	
	• Virtual financial assets agents

Why are subject persons important?

To adopt measures to ensure that money gained through unlawful means is not channelled and laundered through the system and/or that such money, or even money from legitimate sources, is not used for finance terrorism

To ensure that their AML/CFT policies, controls, processes and procedures are designed, implemented and operated in a way which reduces the risk of them being used in connection with money laundering or terrorist financing activities

To be able to recognise transactions which are harmful to the financial system and the Maltese economy as a whole

CAMILLERI PREZIOSI
ADVOCATES

The Implementing Procedures (IPs)

Part I & Part II

Implementing Procedures (PtI)

Remote Gaming Sector (PtII)

Land Based Casinos (PtII)

Virtual Financial Assets Sector (PtII)

Company Service Providers (PtII)

CAMILLERI PREZIOSI
ADVOCATES

Aim

To assist persons who meet the requirements of subject persons to understand and fulfil their obligations under the law

To provide guidance to implement effective AML/CFT policies and measures to detect and flag suspicious transactions

Why?

- To avoid the misuse of the financial system to channel illicit gains or even lawful gains destined for unlawful purposes (terrorism);
- To reduce the risk to the **integrity, proper functioning, reputation and stability** of the financial system; and
- To uphold legal and professional standards for the integrity of financial markets.

Purpose of IPs

To assist subject persons to understand and fulfil their obligation and effectively implement the provisions under the PMLFTR.

To achieve the following objectives:

(a) To outline the requirements set out in the PMLFTR and other obligations emanating from the PMLA;

(b) To interpret the requirements of the PMLFTR and PMLA and to provide measures on how these should be effectively implemented in practice, promoting the use of a proportionate risk-based approach;

(c) To provide industry-specific good practice guidance and direction on AML/CFT procedures; and

(d) To assist subject persons in designing and implementing system and controls for the prevention and detection of ML/FT.

Key aims & obligations

Overview of key aims & obligations

CAMILLERI PREZIOSI
ADVOCATES

1. Identification & Verification of a Customer and BO

Determine who the customer is	Determine who the BO is, where applicable	Verify customer & BO (where applicable)
Determine whether such person is acting on behalf of another person	Establish purpose and intended nature of the business relationship & business & risk profile of customer	In the case of a business relationship, monitor the same on an ongoing basis

Application of CDD measures

Subject persons are to apply CDD measures in the following circumstances:

- **When establishing or entering a business relationship;**
- **When carrying out an occasional transaction that amounts to €15,000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked;**
- **When there is a suspicion of money laundering or terrorist financing, irrespective of any derogation, exemption or threshold;**
- **When there are doubts about the truth or adequacy of previously obtained customer identification data; and**
- *For existing customers:*
  - At appropriate times and on a risk-sensitive basis, including at times when the subject person becomes aware that the relevant circumstances surrounding a business relationship have changed;
  - Whenever doubts arise about the veracity or adequacy of the previously obtained customer identification information, data or documentation.

Who is the customer?

- A person (whether natural or legal)
- Who seeks to form a business relationship (i.e. a prospective customer); or
- With whom a business relationship is formed (i.e. existing customer); or
- For whom an occasional transaction is carried out.

Natural person: *Identification*

- Verification of the customer's identity must happen based on documents, data or information that is obtained from a reliable and independent source.

- The customer's identity may be verified by referring to documents (e.g. passports, ID cards, driving licences, utility bills, and bank statements) or by making use of electronic sources (e.g. e-IDs, Bank-IDs and electronic commercial databases).

This procedure should apply in the same manner with respect to both a resident and non-resident applicant for business

Natural persons: *Verification*

- Verification of the customer's identity must happen based on documents, data or information that is obtained from a reliable and independent source.

- The customer's identity may be verified by referring to documents (e.g. passports, ID cards, driving licences, utility bills, and bank statements) or by making use of electronic sources (e.g. e-IDs, Bank-IDs and electronic commercial databases).

Authenticity Checks

1. Examining security features present on a document and confirming that these can be seen

2. Examining the lamination of an ID card document to check for any suspicious signs

3. Ensuring that the document does not have any uneven colours and text which is non-uniform or the use of irregular fonts or typefaces

4. Verifying or decoding the Machine Readable Zone (MRZ) code contained on the ID card document or the alternative code reproduced on the ID document

5. Checking open-source information that may be of assistance in carrying out authenticity checks

6. Being aware of receiving documentation in a format that could easily be tampered with such as Microsoft Word documents

Legal persons: *Identification & Verification*

Nature of principal	Identification & verification procedures
Public / Private company **Commercial partnership**	• Identification: official full name; registration number; date of incorporation or registration; and registered address or principal place of business • Verification: certificate of incorporation; company registry search; most recent version of M&A (or partnership agreement), recent certificate of good standing (not older than 3 months), or another statutory document • Identify all directors (or partners) (natural and corporate) and in the case of corporate directors obtain: official full name, registration number and registered address or principal place of business • Establish ownership and control structure of the company (or partnership) • Identify and verify all beneficial owners • Other documentation as applicable to be obtained on a risk-sensitive basis: copy of Shareholders' Register; information from independent sources; copy of latest audited financial statements; bank statements (not older than 6 months)

Legal persons: *Verification*

Nature of principal	Identification & verification procedures
Foundation or Association	• Identification: official full name; registration number; date of incorporation or registration; and registered address • Verification: certificate of registration; most recent version of the constitutive document • Identify all persons vested with administration and representation • Establish ownership and control structure • Foundations: identify the founder, any person who has endowed the foundation and any person who has been assigned rights in respect of the foundation
Trust/Trustee	• Identify the trust: full name of the trust, nature of the trust (e.g., discretionary trust, testamentary trust, bare trust) as well as its object and purpose (e.g., wealth management, estate planning), country of administration and applicable law, and registration number if applicable • Verify the existence of the trust by requesting a copy of the trust deed or an extract of same showing the above information • Identify all beneficial owners • Obtain copy of the authorisation of the trustee if regulated

Legal person: *Identification of BOs*

Body corporate or body of persons	i. Any natural person or persons who ultimately own or control that body corporate or body of persons through direct or indirect ownership of more than 25% of the shares or more than 25% of the voting rights or ownership interests in that body corporate or body of persons, including through bearer share holdings, or through control via other means, other than a company that is listed on a regulated market which is subject to disclosure requirements consistent with EU law or equivalent international standards which ensure adequate transparency of ownership information
Trusts, foundations, and other similar legal entities or arrangements	i. Settlor(s) ii. Trustee(s) iii. Protector(s) iv. Determined beneficiaries (or, if not yet determined, class of persons in whose main interest the trust is set up or operates) v. Other natural person(s) exercising ultimate control over the trust

Risk assessments

The Risk-Based Approach

Inherent Risk

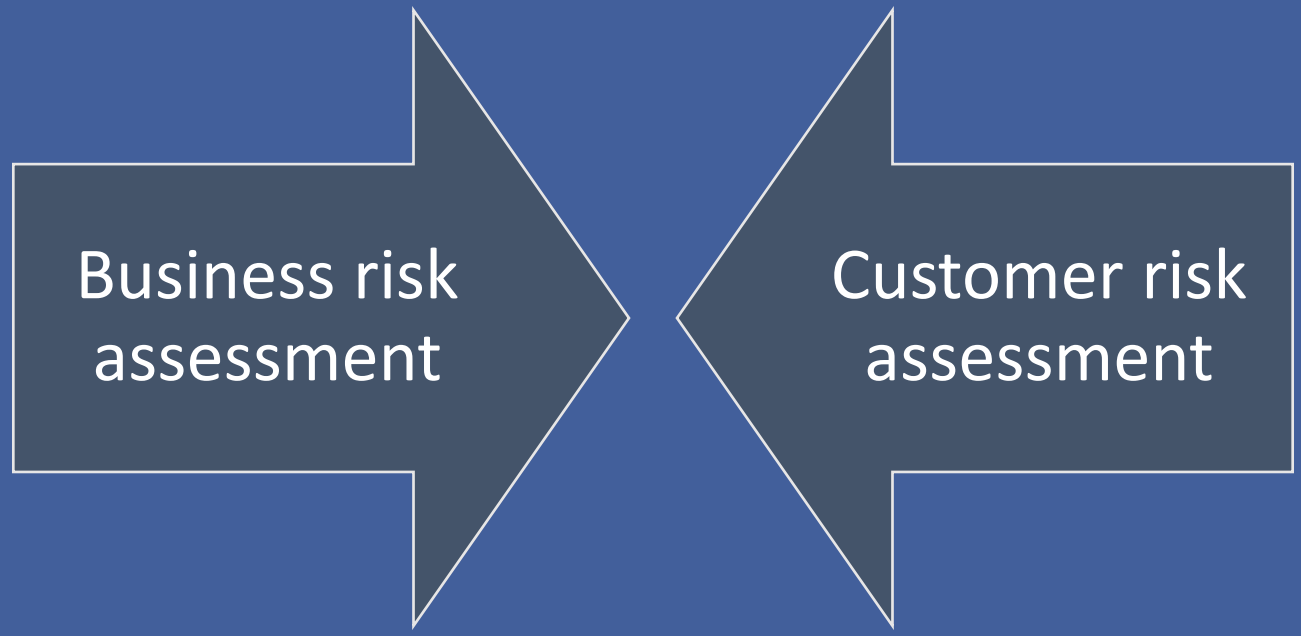
–

Mitigating Measures

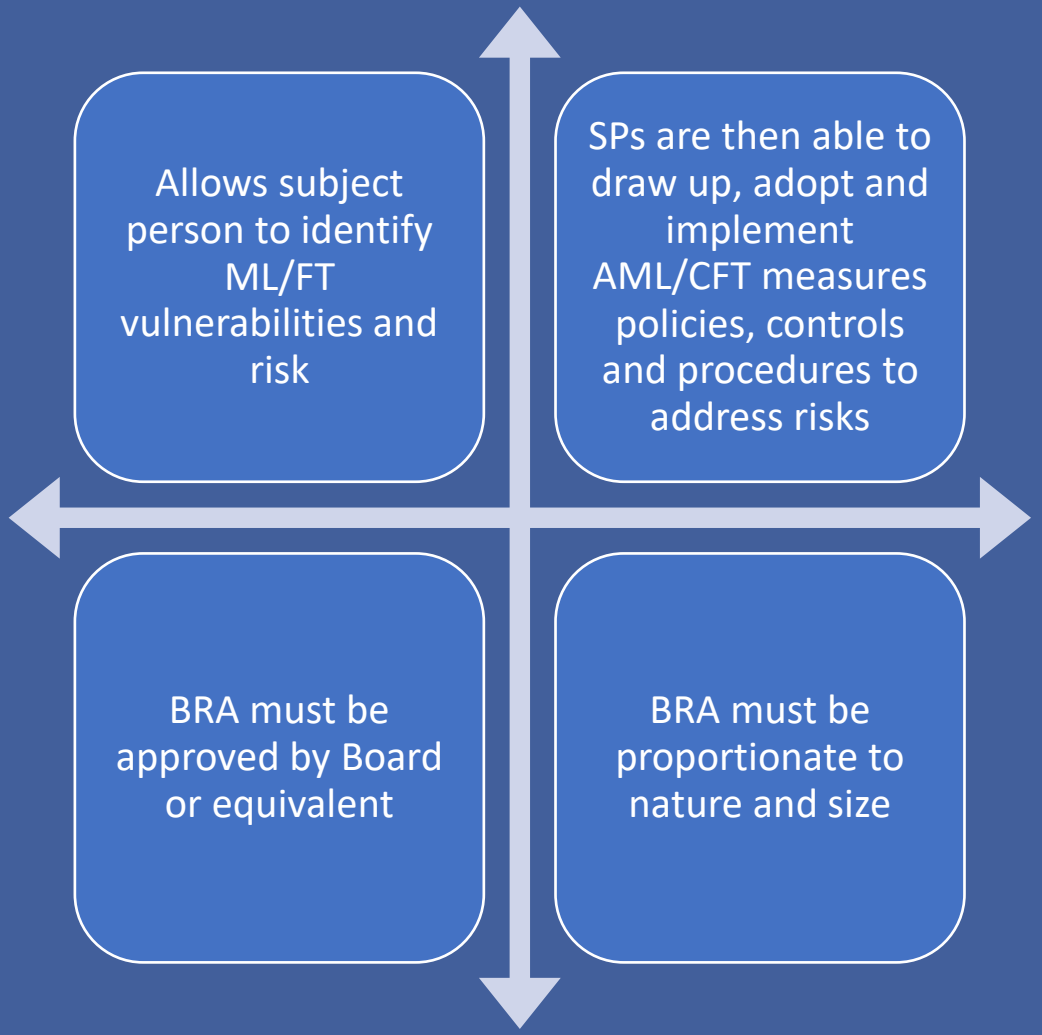
=

Residual Risk

Entity-level risk assessment

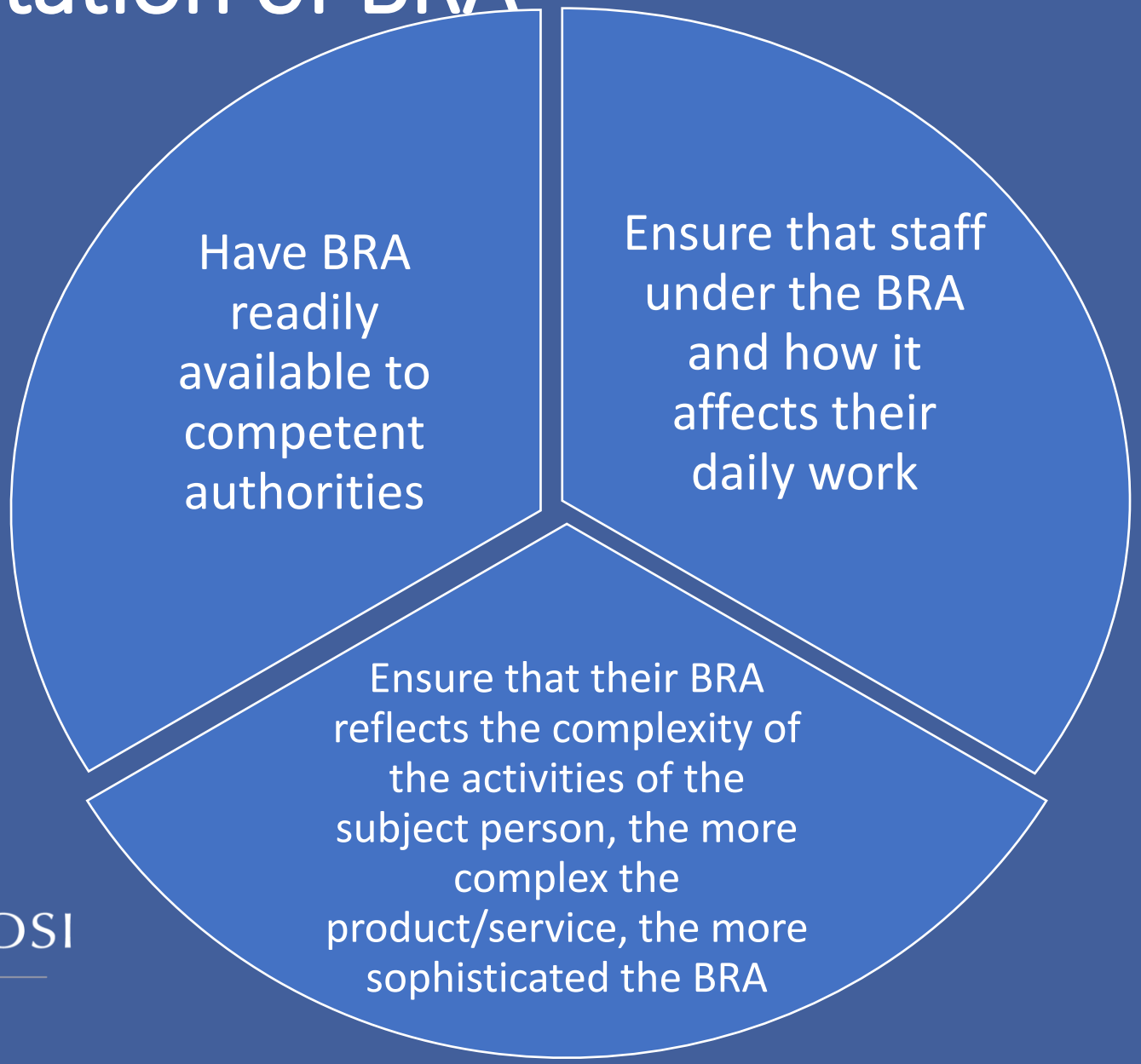


Business risk assessment



Implementation of BRA

Firms should:



CAMILLERI PREZIOSI
ADVOCATES

Business risk assessment

1. Risk identification

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

2. Risk assessment / measurement

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

3. Risk 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

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

CAMILLERI PREZIOSI
ADVOCATES

Mitigating Measures, Policies, Controls & Procedures

- 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.

Customer Acceptance Policy

- Description of high risk customers
- Risk indicators that will lead to low, medium or high risk rating
- Level of CDD measures which should be applied to each risk rating
- Under what circumstances service should be declined

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.

Risk Factors

- Reputation
  - Subject to adverse reports or media
  - Reliable sources
  - Guidelines or procedures to allow employees to discern what is as reliable media reports
  - Impact of adverse media can at times also depend on how remote in time it is. The longer the passage of time from the date of the media item (or the date of the adverse activity reported on in the media item), the less likely it is that the facts reported on will have an ML/FT impact
  - consider what is known about a (prospective) customer and its beneficial owner through official means (e.g., criminal convictions, asset seizures, sanctions, etc.), as well as internally through previous dealings with the same.

Risk Factors

- Nature and Behaviour

  - Reluctance to provide CDD without a legitimate reason
  - CDD that gives rise to doubts on veracity or authenticity
  - Structures that include bearer shares or nominee shareholders
  - Material changes to a customer's ownership and control structure without legitimate rationale
  - Transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without economic or lawful purpose or sound commercial rationale
  - Request from client for unnecessary levels of secrecy
  - No sound economic and/or lawful reason for customer seeking services or products in the subject person's jurisdiction

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 • Complex structure • Unregulated virtual currency exchanges • Non-profit organisations sending funds to non-reputable jurisdictions	• Transfers to a high-risk jurisdictions with no apparent connections • Links to high-risk jurisdictions • Links to countries subject to sanctions or embargos	• Large financial transactions with no apparent economic rationale • No justification for the transactions being proposed • ML/FT risk presented by the product/service itself • Services intended to render the customer anonymous	• 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 • 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

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.**

Jurisdictional Risk Assessment

- 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
- A JRA should take into consideration the customer activity, including business activities, SOW and SOF to determine the SP's geographical risk exposure and whether any of these are linked to a country which may expose it to ML/FT risks.

Record-keeping

Record-keeping

Category	Detail	Retention period
Actions taken to adopt and implement the RBA	• Copy of BRA, changes thereto, decisions taken with respect to the BRA • Copy of most recent controls, policies, measures and procedures	5 years
CDD information & documents obtained for ID&V	• Copy of each CRA • ID&V documents • Results of commercial electronic database searches • Video conferencing records • Document ensuring that an agent is duly authorised in writing to act obo the principal	5 years from termination of relationship or transaction is completed (last transaction)
Records containing details relating to business relationship or transaction	• Information on purpose and intended nature of relationship • All business correspondence • Details on transactions	5 years from termination of relationship or transaction is completed (last transaction)

Record-keeping (cont.)

Category	Detail	Retention period
Reporting	• Internal reports • External reports • Justification why no STR was made	5 years from later date when STR was submitted or date when business relationship end or transaction is carried out
Other	• Training • Employee screening • Reliance agreement • Outsourcing agreement • Other reports which may be useful for FIAU, e.g. internal audit reports	• 5 years from when training took place • 5 years from when employment relationship ends • 5 years from when outsourcing and reliance agreements end • Other: 5 years from when adopted or the subject person ceases relevant activity

Organisation and categorisation of records

Subject persons are to maintain a list of their current business relationships setting out:

- The name of the customer and/or customer reference number;
- The risk categorization of the business relationship (risk rating or risk score);
- The type of service being provided or product being offered;
- Whether the customer is a natural person, legal person, a trust or other legal arrangements;
- The date of commencement of the business relationship and, where applicable, the date on which it ceased;
- A list of all the jurisdictions that the customer deals with;
- Whether the customer or ultimate beneficial owner is a PEP, or an immediate family member or a close associate of a PEP; and
- Whether reliance has been exercised with respect to the particular business relationship.

What about personal data retention?

- Inform a customer that the collection of personal data is necessary to comply with its obligations under Maltese AML laws
- Inform a customer that the his/her personal data will be used for AML purposes
- Where a necessary measure such as CDD is required for the prevention, investigation and prosecution of criminal offences, including measures to combat money laundering, the provisions of the restriction of the data protection (obligations and rights) regulations issued under the Data Protection Act, are restricted in application
- The risk based approach allows subject persons to understand what information it should obtain to carry out its CDD measures, which are commensurate and appropriate

Suspicious Transaction Reporting

- transactions that are not commensurate with the stated business type and/or that are unusual and unexpected
- unusually large numbers and/or volumes of wire transfers and/or repetitive wire transfer patterns;
- unusually complex series of transactions indicative of layering activity involving multiple accounts, banks, parties, jurisdictions;
- transactions being conducted in bursts of activities within a short period of time, especially in previously dormant accounts;
- transactions and/or volumes of aggregate activity inconsistent with the expected purpose of the account and expected levels and types of account activity provided at onboarding;
- parties and businesses that do not meet the standards of routinely initiated due diligence and anti-money laundering oversight programs (e.g., unregistered/unlicensed businesses);
- transactions seemingly designed to, or attempting to avoid reporting and recordkeeping requirements

How to report?

- Internal external reporting procedures to report any knowledge or suspicion of ML/FT, allowing MLRO to report where necessary

- The four main functions of an MLRO are to:
  - receive reports from employees;
  - consider these reports to determine whether knowledge or suspicion of ML/FT subsists;
  - report to the FIAU; and
  - respond promptly to any request for information made by the FIAU.

Preparing an STR

1. Introduction:

- Explain the suspicion
- Make reference to any previous STRs
- Summary of the suspected violations

2. Body:

- Provide details of the review/investigation carried out by the reporting entity;
- State the facts in a clear and concise manner
- Rationale must be clearly identified
- State who the person is (individual or group of persons)

3. Conclusion

- Provide a summary of the suspicion, location/s, as well as identification and any follow up the reporting institution is taking.

Example 1: Incomplete STR

- Mr X was the originator of five transfers totalling EUR175,000. All of the wires were remitted to a Qatar based company. During the same period, Mr X deposited large sums of cash and cheques into his account.

- This STR fails to provide specific details on the application of the suspects funds (the name, bank, and account number of the beneficiary, if identifiable). The financial institution fails to provide any information concerning the relationship, if any, between the FI and the customer. Also, no specific transaction data is provided that identifies the dates and amounts of each wire transfer.

Example 2: Insufficient STR

- Account was opened in 2002. Assets were transferred in by wire. 50 checks for $250 were deposited, securities were liquidated and money was paid out in May 2003.

- This narrative provides no information to support the reason the broker-dealer submitted the STR. Although some general transaction information is included, it fails to provide dates or amounts of the incoming credits to the account, i.e., the dates, amounts, originator, and source of the wire transfers, the issuer or issuers of the 50 checks, and the beneficiary of the funds closing the account in May. Also, no information is given concerning the owner of the account.

Example 3: Sufficient STR

- This STR is being filed to summarize suspicious cash deposits and wire transfer activity conducted by John Doe, account #12345678910. John Doe has been a bank customer since April 2000. Mr. Doe is a college student and employed part-time at Quickie Car Wash.
- Cash deposits to Mr. Doe's personal checking account are structured to possibly circumvent federal reporting requirements. The deposits are followed by immediate wire transfers to Aussie Bank in Sydney, Australia to a single beneficiary, Jennifer Doe, account #981012345, with an address located in Australia. Specifically the following activity has been observed: cash deposits (dates followed by amounts): 03/15/02 $9,950.00; 03/17/02 $9,700.00; 03/18/02 $10,000; total: $29,650. Wire transfers out (dates followed by amounts): 03/16/02 $9,900.00, 03/18/02 $9,700.00, 03/19/02 $9,900.00.
- The volume and frequency of the deposits is not consistent with previous banking transactions conducted by Mr. Doe. The amounts of currency do not appear consistent with the customer's stated employment. Also, the relationship between the customer and Jennifer Doe and the purpose for the wire activity is unknown.
- Therefore, due to the structured cash deposits by the customer on almost consecutive days into the account, and the immediate wire transfer of the funds out of the account to Jennifer Doe, Aussie bank, account #891012345, Sydney Australia, this STR is being filed.

Example 4: Complete STR

- On June 27, 2003, Jane Smith came up to the third main cage and cashed out $5,000 in chips. She proceeded to hold purple chips (looked to be about $5,200) stating that she was going to keep those chips until later. While waiting in line, Ms. Smith was talking to another patron about the currency transaction reporting (CTR) process and basically telling him how to avoid a CTR. She was explaining how the cage, table games, and slots compare their amounts and fill out a CTR when someone gets over $10,000. Ms. Smith told the other patron that's why she pulls some of her chips back so she will not have to pay taxes. She and the other gentleman then walked out together.
- Ms. Smith has visited our casino over the last month, usually once a week. Her winnings were minimal until last week when on June 20, 2003 she cashed out $5,000 in chips one day. She returned the following day and cashed out an additional $5,000 in chips. We have maintained a copy of Ms. Smith's winnings over the last month and also a copy of her driver's license.
- Today, Ms. Smith was informed that she was barred from our casino after she was overheard instructing another patron on how to avoid a CTR

goAML System

The FIAU has replaced the STR submission system and implemented the goAML software solution.

The use of goAML

- effective
- efficient
- Improves communication

About goAML

- Built system made for FIUs by UNODC
- Consists of online report data entry forms
- Possibility to upload reports in the form of XML
- Helps subject persons improve report data quality
- Notification and messaging system to inform about report status and feedback
- Supports submitting bank account history electronically
- History of reporting and statistics

How it works?

Step 1: Registration in goAML

This new platform must be used by all subject persons when submitting an STR.

Step 2: Choose type of New Reports

The user has the option to choose between SML upload or Web Reports when entering documentation and information.

Step 3: Choose the TYPE of report to use

The FIAU differentiated between the type of reports submitted and each entity must classify under the correct category

- STR (Suspicious transaction report)
- SAR (Suspicious activity report)
- TFR (Terrorism financing report)
- PEPR (Politically exposed person report)

Step 3: Submit and Await Feedback

Once submitted the reporting entity will receive feedback on the success of the submission. If rejected, the entity would need to amend accordingly.

Types of Reports – STR

- STR consists of a transaction or series of transactions which are deemed to be suspicious due to not being in line with the customer's known or expected transactional profile.
- Ex 1. Customer deposits a onetime cash payment of EUR20K which is not observed to be in line with their known profile and offers no reasonable explanation for such deposit. All other transactions made by the customer are in line with their expected activity. In this case, SP should report only the suspicious transaction to the FIAU by submitting an STR regarding the EUR20K transaction. The remaining transactions should be submitted as an AIF.

Types of Reports – SAR

- An SAR consists of transactional activity which is in line with the known or expected profile, but the customer displays behaviours which raise suspicion.

- Examples of this include but are not necessarily limited to:

  - adverse information through open sources,
  - refusal to provide requested documentation;
  - uncooperative behaviour;
  - becoming uncommunicative.

Types of Reports – TFR & TFTR

- Terrorism Financing Reports, TFRs, are to be submitted when there is suspicion of terrorist financing activities. This report is predominantly activity based and the suspicion does not arise from the actual transaction(s). This report type does not allow for the inclusion of suspicious transaction reporting.

- Terrorist Financing Transaction Reports, TFTRs, are to be submitted when there is a clear suspicion of terrorist financing, however the suspicion emanated from a transaction or series of transactions carried out by the reported natural or legal persons.

FIAU Guidance Note on submitting STRs by remote gaming licencees

- On 4th April 2019, the FIAU issues a guidance note to assist remote gaming licensees in identifying the information and documentation that should be provided to the FIAU when submitting a STR.
- The FIAU noted that the following information, among others, should be provided:
  - Status of account (whether it is active, suspended/blocked, closed) including the balance held in the gaming account as at date of submission of the STR.
  - Value and volume of withdrawals and deposits effected on a yearly basis over at least the five years immediately preceding the submission of the STR;
  - Identification, to the extent possible of unusual and/or significant increases in the value and/or frequency of deposits during a particular timeframe; or any gaming activity which is not commensurate with the volume and/or value of deposits;
  - The IP addresses used to log on to the gaming account;
  - Copies of due diligence documents.

Awareness, training and employee screening

Training

A subject person is required to take appropriate and proportionate measures from time to time to:

- ensure that employees are aware of relevant AML/CFT legislation (and any updates) and data protection requirements, as well as of the subject person's AML/CFT measures, policies, controls and procedures and any ML/FT risks particular to subject person; and

- provide training in relation to the recognition and handling of operations and transactions which may be related to proceeds of criminal activity, money laundering or the funding of terrorism.

Training

Tailored Training	The Unit must tailor training for employees that fulfil roles with higher financial crime risk exposure – those being staff that are client facing.
Practical Dimension	Training carried out should have a strong practical dimension to it and includes case studies and the regular testing of staff, in order to ensure that the staff understand their responsibilities. The training must not unduly dwell on legislation and regulations, as this may prove to be monotonous for the staff and lead to disinterest and not give the staff necessary tools in real life scenarios. Thus, for example, if computerised training is used, this should conclude with a test at the end.
Training Follow-Ups	Completion of training must be documented and monitored through appropriate management information metrics, and non-completion of training must be taken seriously through appropriate consequence management.
External Training	External training carried out by third parties as well as relevant conferences/seminars should also be recommended for employees.

Employee screening

Subject persons shall also have in place appropriate employee screening policies and procedures when hiring employees, which may include;

- obtaining a Police conduct certificate or equivalent documentation;
- documentation being refreshed on an ongoing basis.

Any questions?

Thank you

Technical Excellence, Practical Solutions

CAMILLERI PREZIOSI
ADVOCATES

INTERLAW.
An International Association of Independent Law Firms