AML / CFT NATIONAL RISK ASSESSMENT
RESULTS AND IMPLICATIONS FOR FINANCIAL INSTITUTIONS

OCTOBER 2018

Introductions

DR. ANTON BARTOLO

Head of Enforcement

Malta Financial Services Authority

Agenda

Topic		Duration
1	**National Risk Assessment: Sector-Specific Findings**	**50 mins**
	Overview of Process	
	Banking	
	Securities	
	Insurance	
	Other Financial Institutions	
2	**Implications for the private sector**	**50 mins**
	Stakeholder responsibilities	
	Role of Client-level Risk Assessments	
	Best Practice Risk Assessment Criteria	
3	**Questions**	**10 mins**
4	**Concluding Remarks**	**10 mins**

Context

This session builds on the seminar hosted yesterday, focusing in on the specific implications of the results of the National Risk Assessment

Yesterday

- **Provided a general overview of Malta's ML/TF National Risk Assessment**
  - Introduced context and methodology
  - Presented high-level results
- **Presented response of competent authorities**
  - Communicated National AML / CTF Strategy
  - Highlighted importance of private sector contribution to the national effort

Today

- **Specific focus on ML / TF risks facing the financial sector**
  - Sets out methodology for sector-specific risk assessments
  - Presents results of NRA from perspective of the financial sector
- **Outlines implications of findings and how the private sector can effectively respond**
  - Establishes role of private sector in mitigating ML / TF risks
  - Advises on best practice for client due diligence / risk assessment processes

Objectives of today's session

Be aware of Malta's National AML/CFT effort and findings of the National Risk Assessment

Understand and be prepared to effectively communicate ML/TF threats and vulnerabilities in your respective sectors

Understand how the Private Sector should contribute to the AML/CFT effort

Part 1 | National Risk Assessment: Sector-Specific Findings

Sectoral risk assessments were conducted as part of the National Risk Assessment to provide a more detailed view of the vulnerabilities and controls

Background and purpose

- **National Risk Assessment** conducted to understand ML/TF threats, sectoral vulnerabilities, national combatting ability and emerging risks facing Malta
- Sectoral assessments provide a detailed view of **inherent vulnerabilities and control effectiveness** of key sectors

Approach

- **Working groups for each sector** were formed, comprising representatives of:
  - All relevant Maltese authorities and supervisors
  - A cross-section of private sector firms
- A combination of **data submitted and expert judgement** was used to assess key vulnerability and control criteria

Overarching themes across control environments

Policies and procedures usually in place

- AML / CFT policies and procedures observed to exist
- More mature amongst larger firms

Effectiveness of controls is weak

- AML/CFT processes lack robustness and consistency
- Reporting and monitoring often weak

AML / CFT resourcing requires enhancement

- Many compliance teams under-resourced
- Independent internal audit sometimes not present

AML / CFT awareness is low across sectors

- Staff knowledge is often found to be lacking
- Especially true amongst smaller entities

Relatively high levels of risk were observed across most sectors, particularly banking on inherent risk

Sector	Sectoral vulnerability	
	Inherent risk rating	**Residual risk rating**
Banking	**High**	**Medium-High**
Securities	**Medium-High**	**Medium-High**
Insurance	**Medium**	**Medium**
Other Financial Institutions	**Medium-High**	**Medium-High**
Gaming	Medium-High	Medium-High
DNFBPs	High	High

Focus of this pack

Banking outcomes

The banking sector is considered to have medium-high residual risk, in part due to a more mature control environment

Sectoral risk assessment results

Sub-sector	Inherent risk	Controls	Residual risk
Core domestic banks	High	Medium-low	Medium-high
Non-core domestic and international banks	High	Medium-low	Medium-high
Overall rating	High		Medium-high

Inherent and residual risk

Inherent risk

- Inherent risk **highest of all financial sectors**
  - Primarily due to size of sector (assets ~475% of GDP) and extent of international trade
  - Inherently due to nature of products offered
  - Supported by proportion of high-risk clients (e.g. non-EU residents, PEPs)
  - Further risk due to non-face-to-face clients introduced through intermediaries (e.g. CSPs, trustees)

Control environment

- Controls considered **more mature in banking** than majority of other financial sectors
  - AML / CFT frameworks, policies and procedures observed to be in place
  - Developed and enhanced over a period of time
- However **overall controls remain insufficient** as recent inspections demonstrate, particularly on
  - Resourcing of bank compliance staff
  - Quality of bank operations with regards to AML/CFT

Securities outcomes

The securities sector was found to have medium-high residual risk, driven by relatively weak execution of private sector controls

Sectoral risk assessment results

Sub-sector	Inherent risk	Controls	Residual risk
Collective investment schemes	Medium-high	Low	Medium-high
Custodians	Medium-high	Low	Medium-high
Foreign exchange traders	Medium-high	Low	Medium-high
Fund administrators	Medium-high	Low	Medium-high
Fund managers (and investment/asset managers)	Medium-high	Low	Medium-high
Stockbrokers	Medium	Low	Medium
Overall rating	Medium-high		Medium-high

Inherent and residual risk

Inherent risk

- Inherent risk considered **relatively high** for most sectors
  - Risk driven by nature of activities, volume and speed of transactions
  - Links to foreign jurisdictions, prevalence of non-face-to-face channels are additional factors
  - Exposure to non-EU residents, PEPs and high net worth individuals also drive risk

Control environment

- **Level of controls is found to be weak**
  - Enforcement of AML / CFT obligations is severely lacking
  - Staff knowledge, awareness and AML monitoring are poor, especially across smaller firms
  - Resourcing of compliance teams sometimes lacking
  - Some firms lack an independent internal audit function

Insurance outcomes
The insurance sector was found to have the lowest risk of all financial sectors, due to its small size and adequate control environment

Sectoral risk assessment results

Sub-sector	Inherent risk	Controls	Residual risk
Insurance	Medium	Medium-low	Medium
Overall rating	**Medium**		**Medium**

Inherent and residual risk

Inherent risk

- Inherent risk **lower than most other financial sectors**
  - Relatively small sector compared to e.g. banking
  - Most clients fairly low-risk, with exception of pensions
- **Inherent risk is driven by pensions** products:
  - Deposit features facilitate placement / layering
  - Product has strong links to tax evasion

Control environment

- **Some good effectiveness of controls observed**, particularly around
  - Adherence to AML / CFT requirements
  - Commitment towards good corporate governance
  - Robust and comprehensive AML/CFT legislative framework firms operate within
- **Some areas exist for improvement**
  - Knowledge and awareness of staff should be boosted through good quality training
  - Internal policies and procedures could be strengthened
  - Independent audit functions required

Other financial institutions outcomes

Other financial institutions vary significantly in terms of risk, with an overall residual rating of medium-high

Sectoral risk assessment results

Sub-sector	Inherent risk	Controls	Residual risk
Payment services	High	Medium-low	Medium-high
Lending	Medium-low	Medium-low	Medium-low
Other activities	Medium	Low	Medium
Overall rating	Medium-high		Medium-high

Inherent and residual risk

Inherent risk

- Inherent risk **varies significantly by sub-sector**
  - Payment, remittance and e-money services high risk due to high volume, nature of activity and international nature
  - Cash-intensive services (e.g. remittance and foreign currency) also drive risk
  - Risk from lending is low: some risk if funds gained through fraud

Control environment

- **Control framework reasonable** across sector
  - Regulations and guidelines in place
  - Market-entry authorisation appears effective
- However, **private sector controls implementation could be improved**
  - STR reporting infrequent and lower than expected
  - Extent of responsibilities not always fully understood
  - Knowledge and understanding of AML / CFT risks could be enhanced

Part 2 | Implications for private sector

Supervisory responsibilities

The FIAU and MFSA will support private sector AML / CFT efforts through their responsibilities across the supervisory lifecycle

Responsibilities of the supervisors

Market entry

- Provide portal for firm registrations / notifications
- Review licence applications
- Authorise key individuals across supervised firms

Oversight and monitoring

- Share insights gained from sectoral risk assessments and firms' annual compliance reports
- Provide targeted feedback from desk-based / onsite compliance reviews
- Issue formal regulations / guidelines
- Provide guidance to support private sector understanding

Enforcement and intelligence

- Investigate ML / TF compliance breaches
- Impose administrative sanctions and penalties on offending firms
- Collect and investigate suspicious transaction reports

+

Regular engagement with private sector

Private sector responsibilities

To combat ML / TF risk, firms must develop effective AML / CFT controls across the board

Private controls

Individual firms' AML / CFT frameworks

- Controls established within individual firms to prevent and detect ML / TF through that organisation
- Include various control elements across the AML / CFT life-cycle, from risk assessment during customer acquisition process to procedures in place to detect and report suspicious activity
- Follows a risk-based approach, with control severity proportional to the riskiness of the client / product in question

Focus of this session

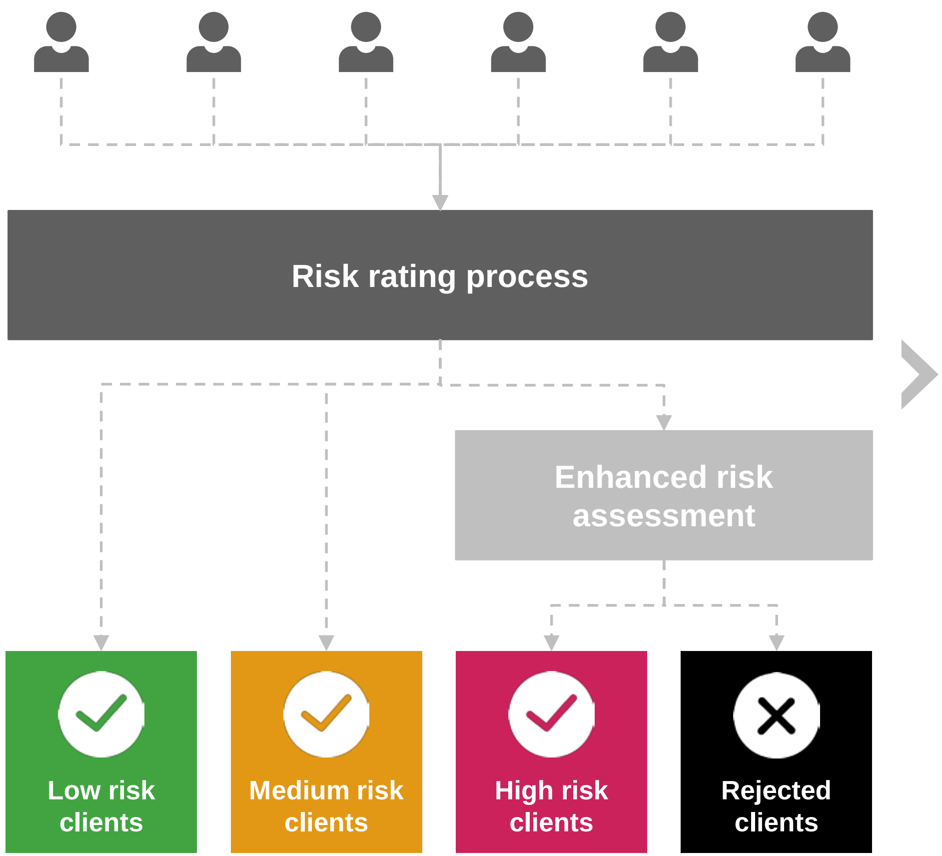
Public controls

Market entry → **Oversight and monitoring** → **Enforcement and intelligence**

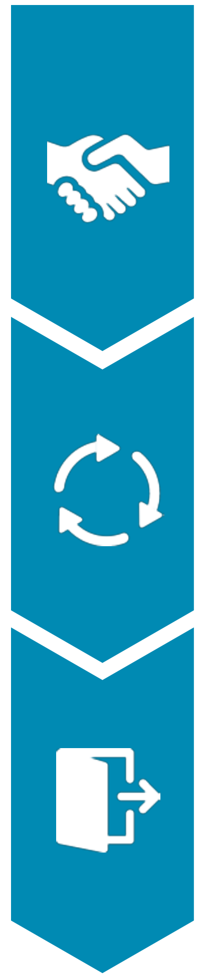
Customer risk assessment approach

A risk-based approach to management is employed to ensure the severity of controls triggered is proportional to the risk posed by the client

Illustrative approach



Usage



Onboarding

- Initial risk assessmentand onboarding process varies by risk type
- Higher-risk clients required to submit more extensive documentation, and more checks conducted to verify document authenticity
- Low risk clients have streamlined process

Ongoing monitoring

- Client activities monitored against “expected” profile, often by automated systems
- Response severity to abnormal activity dictated by risk level
- Risk assessments refreshed on regular basis; more frequently for high-risk clients

Exits

- Customer exits occur when risk level of client goes beyond tolerated level
- “Room for manoeuvre” often more limited with higher risk clients
- Suspicious activity amongst high-risk clients often sufficient to trigger an exit

Customer risk assessment approach

Internal risk assessments aim to qualify the level of risk posed by each client through consideration of a number of risk drivers

Risk drivers observed		Assessment criteria	Example considerations	Rationale
1	**Customer risk**	Customer activity	• Sectors of operation • Nature of activities	Some sectors / activities more frequently associated with ML / TF
		Customer reputation	• Official investigations / procedures • Media reports and accusations	Previous conduct can inform expected future risk
		Customer nature	• Ownership and identity verification • Company structure	ML / TF offenders typically try to obscure identity
2	**Geographic risk**	Geographic operations	• Location of company headquarters • Geographies transacted with	Crime level, presence of terrorist groups etc makes ML / TF more common in some jurisdictions
		Geographic links	• Links to other risky geographies	
3	**Product risk**	Product nature	• Transparency of product • Complexity of transactions	Complexity attractive as ML / TF harder to detect
		Product value	• Value of assets involved	ML / TF often requires movement of large sums
4	**Channel risk**	Degree of separation	• Level of face-to face activity • Use of intermediaries	ML / TF criminals often look to avoid directly revealing identity

Sources: Joint Money Laundering Steering Group, UK Financial Conduct Authority, Joint Committee of the European Supervisory Authorities

1

Customer risk: activity

The client's stated purpose, activities and operations should be examined for features raising risk, such as political exposure or excessive cash use

Background of customer

- Is background **consistent with stated activities**?
- Is value of **assets**, **income** and **transaction volumes** reasonable for stated activities?

Sectors covered

- Are **sectors / sector links** at high risk of ML / TF?
- Is sector **indirectly linked** to ML / TF, e.g. higher risk of corruption, significant cash volumes, NPO

Political exposure

- Does client have connections to **public / political figures**?
- If client is public / political figure, is there a risk of **bribes being laundered** through account?

Business activities

- Do **activities and purpose** pose a risk?
- Would **day-to-day activities carried out** increase risk of client coming into contact with ML / TF (e.g. raising money for overseas development)?

Business-specific controls

- Is client **supervised / regulated**?
- Is client **subject to public scrutiny** (e.g. publicly traded company)?

Sources: Joint Money Laundering Steering Group, UK Financial Conduct Authority, Joint Committee of the European Supervisory Authorities, World Bank Tool for Assessment of Money Laundering and Terrorist Financing Risk

1 Customer risk: reputation

The reputation of the client should be considered, taking into account both official documents and reports from other credible sources

Official investigations and procedures

- ❑ Has client **previously been subject to ML / TF investigations**?
- ❑ Has client / associates had **assets frozen** or **legal proceedings** made against them?
- ❑ Has client / associates been subject to **historical sanctions**?

Media reports and exposes

- ❑ Has client been subject of **adverse media / investigatory reports**?
- ❑ If so, are allegations **sufficiently credible** to take into account? (Credibility factors include quality, independence and persistence of reporting)

In-house information

- ❑ Does any **first-hand** information gained through long-term relationships indicate the level of risk?
- ❑ Does diligence corroborate that perception is **still accurate**, especially following **break in business relationship** or **change in client management**?

Sources: Joint Money Laundering Steering Group, UK Financial Conduct Authority, Joint Committee of the European Supervisory Authorities, World Bank Tool for Assessment of Money Laundering and Terrorist Financing Risk

1 Customer risk: nature

The client's identity, interactions and nature should be examined for clues regarding their intentions

Customer identity

- ❑ Is client and beneficial owner's identity verifiably **accurate** and **sound**?
- ❑ Have there been any recent **changes in ownership** or **control**?
- ❑ Does the client use **bearer shares / nominee shareholders**?

Corporate structure

- ❑ Does the client have a **complex / opaque structure** without a clear business rationale?
- ❑ If so, is the complex structure spread across **multiple jurisdictions**?
- ❑ Is the client an **NPO**?

Business motivation

- ❑ Is the **rationale** of the client in obtaining the service **clear**?
- ❑ If the client is a non-resident, are their **reasons for choosing Malta** clear?
- ❑ Could the clients' needs could be **better serviced elsewhere**?

Source of funds

- ❑ Is the client's wealth / source of funds **legitimate** and **transparent**?
- ❑ Are they **consistent** with the client's stated **occupation**, **inheritance** or **investments**?
- ❑ Is the **country of origin** high-risk?

Transaction nature

- ❑ Does client request **unusual secrecy** levels / **complex transactions**?
- ❑ If so, does this appear to be an attempt to **evade reporting thresholds**?
- ❑ Does the client **avoid relationships** (e.g. many one-off transactions)?

Activity profile

- ❑ Can the **expected use** of services be established given the client's profile?
- ❑ Is the client's use of services **consistent with expectations** once onboarded?

Sources: Joint Money Laundering Steering Group, UK Financial Conduct Authority, Joint Committee of the European Supervisory Authorities, World Bank Tool for Assessment of Money Laundering and Terrorist Financing Risk

2

Geographic risk

Firms should form an internal list of high-risk jurisdictions based on available data sources, and consider all geographies the client is linked to

Geographic and contextual factors

ML risk considerations:

- Is there a lack of **political stability**?
- Is **corruption prevalent**?
- Is there a lot of **criminal activity**, especially those associated with money laundering (e.g. illegal drugs, trafficking)
- Is the **shadow economy** relatively large?

TF risk considerations:

- Are any international **sanctions or embargoes** in place?
- Do **proscribed terrorist groups** (e.g. identified by Malta, EU or Interpol) operate within the country?
- Are there allegations of **terrorist organisation funding / support** against the country (e.g. by the World Bank)?

Group membership

- Is the country a **member of regional groups / unions** (e.g. European Union) with **minimum AML / CFT requirements**?
- Is the country a member of **supranational organisations** (e.g. MONEYVAL) with similar standards?

AML / CFT implementation standards

- Is the extent and quality of the **AML / CFT control framework** established by competent authorities adequate?
- Are **market entry** controls, scope and quality of **supervision**, and effectiveness of **detection** and **prosecution** by authorities adequate?

Sources: Joint Money Laundering Steering Group, UK Financial Conduct Authority, Joint Committee of the European Supervisory Authorities, World Bank Tool for Assessment of Money Laundering and Terrorist Financing Risk

2

Geographic risk

Firms should form an internal list of high-risk jurisdictions based on available data sources, and consider all geographies the client is linked to

Official evaluations and assessments

- ❑ Do **official assessments / evaluations** (e.g. by Moneyval) exist, and do they highlight strong controls?
- ❑ Do published **National Risk Assessments** highlight a strong control environment?

Expert body opinions

- ❑ Have expert bodies (e.g. World Bank) published **warnings** about the country?
- ❑ Is the country on FATF's **list of high-risk jurisdictions**?

International perception

- ❑ Have **other governments** made public statements or comments on the ML / TF environment of the country?
- ❑ Have **internationally-active private companies** (e.g. global banks) made statements on the country?

Bilateral trade

- ❑ Is there a high level of **bilateral trade** / **strong relationship** between relevant jurisdictions and Malta?
- ❑ If client is **active across multiple foreign countries**, is there a high level of bilateral trade between those?

Sources: Joint Money Laundering Steering Group, UK Financial Conduct Authority, Joint Committee of the European Supervisory Authorities, World Bank Tool for Assessment of Money Laundering and Terrorist Financing Risk

3 Product risk

Many financial products are complex and opaque, making detection of ML harder; clients' use of such products will raise their risk level

Transparency

- ❑ Does the product / service allow the **user to remain anonymous**, or for **third parties to instruct its use**?
- ❑ Does the product / service allow **source or destination** of value to be traced?

Complexity

- ❑ Do transactions / services involve **multiple parties** or **multiple jurisdictions**?
- ❑ Does the **inherent complexity** of product / service make **detection of suspicious behaviour** difficult?

Transaction size

- ❑ Is the products / services generally associated with **higher-value transactions**?
- ❑ Does the product /service have transaction **value limits or caps**?
- ❑ Is the product / service **cash-intensive**?

Sources: Joint Money Laundering Steering Group, UK Financial Conduct Authority, Joint Committee of the European Supervisory Authorities, World Bank Tool for Assessment of Money Laundering and Terrorist Financing Risk

4

Channel risk

Delivery channels with a high degree of separation between provider and client are generally higher risk, as clients cannot be verified as easily

Degree of removal

Onboarding channel considerations:

- ❑ Is **client physically present for identification** during initial due diligence?
- ❑ If not, has **strong and reliable non-face to face due diligence** been carried out to mitigate risk of identity fraud?

Day-to-day business channel considerations:

- ❑ Does the channel through which business is conducted provide a **reasonable degree of verification** (e.g. videoconference or telephone call)?

Use of intermediaries

Referral considerations:

- ❑ Has the client been introduced by a **trusted source** (e.g. another regulated / supervised institution)?
- ❑ Has the client been referred through an **agent without direct client contact**?

Intermediary considerations:

- ❑ If an intermediary is used, is it **regulated or supervised** for AML / CFT matters?
- ❑ Does the **location, reputation and history** of the intermediary raise any concerns?

Sources: Joint Money Laundering Steering Group, UK Financial Conduct Authority, Joint Committee of the European Supervisory Authorities, World Bank Tool for Assessment of Money Laundering and Terrorist Financing Risk

Customer risk assessment sources

A variety of sources exist which can complement domestic authorities' guidance in assessing risk of potential clients

International bodies

Entity	Role
FATF	• Provides and monitors adoption of AML / CFT standards • Publishes list of high-risk and monitored ML / TF jurisdictions
THE WORLD BANK	• Provides guidance on ML / TF assessment processes • Analyses countries' financial integrity • Publishes a list of countries linked with terrorist financing / support
INTERPOL	• Publishes reports and guidance on Money Laundering • Provides information on terrorist organisations and activities
	• Imposes various trade sanctions on countries and individuals
	• Imposes various trade sanctions on countries and individuals

Q&A

?

Part 4 | Concluding remarks

To effectively combat ML / TF, it is critical that the private sector embraces its responsibilities and acts proactively in implementing robust controls

What you can do

Review organisational governance to clarify internal responsibilities, enhance policies and procedures, and update risk appetite

Review processes and procedures to ensure up-to-date risk assessments are maintained, and used to inform business decisions

Enhance resourcing of compliance teams where necessary, and ensure these are independent from audit functions

Conduct regular staff training programmes to ensure all business representatives are aware of ML / TF risks

What we will do

Work alongside private sector to gather insights, and use this to inform policy enhancements

Augment resources of supervisors to conduct on-site investigations and enhanced monitoring

Continue to provide guidance and training to private sector on implementing controls