AML / CFT NATIONAL RISK ASSESSMENT

RESULTS AND IMPLICATIONS FOR DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

10TH OCTOBER 2018

Agenda

	Topic	Timing
1	**National Risk Assessment: Sector-Specific Findings** *Overview of Process* *DNFBP findings*	14:30 – 14:55
2	**Implications for the private sector** *Stakeholder responsibilities* *Role of Client-level Risk Assessments* *Best Practice Risk Assessment Criteria* *Sources of Guidance for Risk Assessments*	14:55 – 15:15
3	**Questions**	15:15 – 15:25
4	**Concluding Remarks**	15:25 – 15:30

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 DNFBP sector**
  - Sets out methodology for sector-specific risk assessments
  - Presents results of NRA from perspective of the DNFBP 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 risk assessment processes

Objectives of today’s session

Be aware of money laundering / terrorist financing risks and results of the National Risk Assessment

Be prepared to communicate these risks and their implications both internally and externally

Understand what actions can be taken at an institutional level to combat these risks

Part 1 | National Risk Assessment: Sector-Specific Findings

Sectoral risk assessments were conducted to provide a more detailed view of the vulnerabilities and controls associated with six key sectors

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
- **Assessments were aggregated using the World Bank tool** to develop vulnerability and control ratings

The DNFBP sector was rated highest amongst all sectors considered for both inherent and residual risk

	Sectoral vulnerability	
Sector	**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

Inherent risk is led by company service providers, lawyers, trustees and fiduciaries; residual risk remains high due to insufficient controls

Sectoral risk assessment results

Sub-sector	Inherent risk	Controls	Residual risk
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
Overall rating	High		High

Summary outcomes - inherent and residual risk

Inherent risk

- Inherent risk **is high,** led by highest risk sub-sectors of CSPs, lawyers and trustees / fiduciaries

Control environment

- **Private sector awareness of AML / CFT issues is weak,** where individuals often do not have expertise in AML / CFT implications of products
- **Large proportion of DNFBPs lack robust controls**
  - Often small-scale / individual providers
  - Lack expertise and resources of bigger players in implementing effective and robust controls
  - Often have few independent checks and balances to monitor the implementation of AML obligations

Client risk profiles, geographic risk and the nature of services provided drive high levels of risk across the sector

Key inherent risk drivers

1

Large number of risky clients

- Clients who are high net worth individuals, come from risky jurisdictions, PEPs etc
- Corporate clients (shares held on a fiduciary basis)

2

Services provided are risky by nature

- Setting up of corporate structures often complex
- Advice can be misused for ML purposes

3

High level of geographic risk

- Many clients are non-resident, often outside EU
- Some exposure to risky geographies

4

Higher-risk channels are prevalent

- Non-face-to-face service provision is common
- Sometimes provided through intermediaries

Control effectiveness

✓

Some conduct rules / obligations imposed

- Certain providers are subject to ethical standards and warrant procedures
- Some professionals are subject to PMLFTR

✗

Knowledge and awareness is limited

- Small providers often lack AML awareness
- Lack of appropriate investment in controls

✗

Implementation of controls is weak

- AML / CFT obligations sometimes overlooked
- Infrequent reporting of suspicious transactions

Part 2 | Implications for private sector

Supervisory responsibilities
The FIAU and relevant supervisory bodies will support private sector AML / CFT efforts through the supervisory lifecycle

Responsibilities of supervisors

Market entry

- Provide portal for registrations / notifications
- Review licence applications (as relevant)
- Authorise key individuals (as relevant)

Oversight and monitoring

- Share insights gained from risk assessments and 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

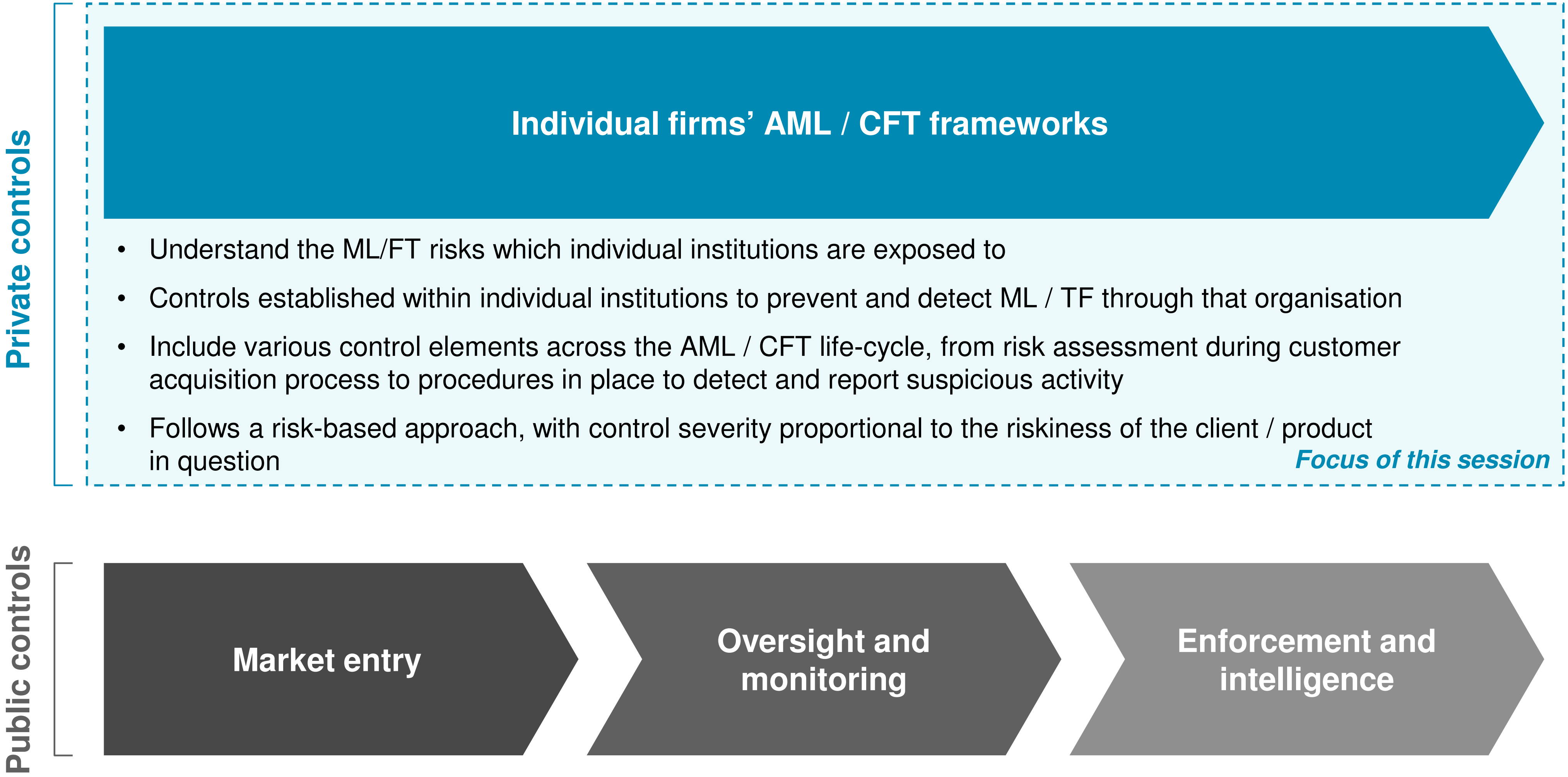
- Investigate ML / TF compliance breaches
- Impose administrative sanctions and penalties on offending firms / persons
- Collect and analyse suspicious transaction reports

+

Ongoing co-operation with private sector through the Joint Committee, involvement of professional bodies, ad hoc expert working groups and by means of consultations

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

- Understand the ML/FT risks which individual institutions are exposed to
- Controls established within individual institutions 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

AML/CFT controls framework

FATF recommendations establish expectations across AML/CFT capabilities which should be referred to while designing AML/CFT controls

Relevant FATF Recommendations

○ FATF recommendation number

10

Conduct **customer risk assessments** when establishing new relationships and carrying out transactions over €15K
[Regulation 5 of the PMLFTR]

11

Maintain records of transactions, CDD measures, account files and correspondence for 5 years after the end of the relationship
[Regulation 13 of the PMLFTR]

12

Establish **strong risk-management systems** **(**including enhanced authorisation, assessment and monitoring programmes) for PEPs
[Regulation 11 of the PMLFTR]

15

Proactively **identify and assess ML / TF risk** arising from new products, business practices or technologies
[Regulation 5 of the PMLFTR]

18

Implement **internal control programmes** against ML / TF, at a group-wide level if applicable
[Regulation 5 and Regulation 6 of the PMLFTR]

19

Apply **enhanced due diligence** / assessment measures to transactions involving clients from high-risk jurisdictions
[Regulation 11 of the PMLFTR]

20

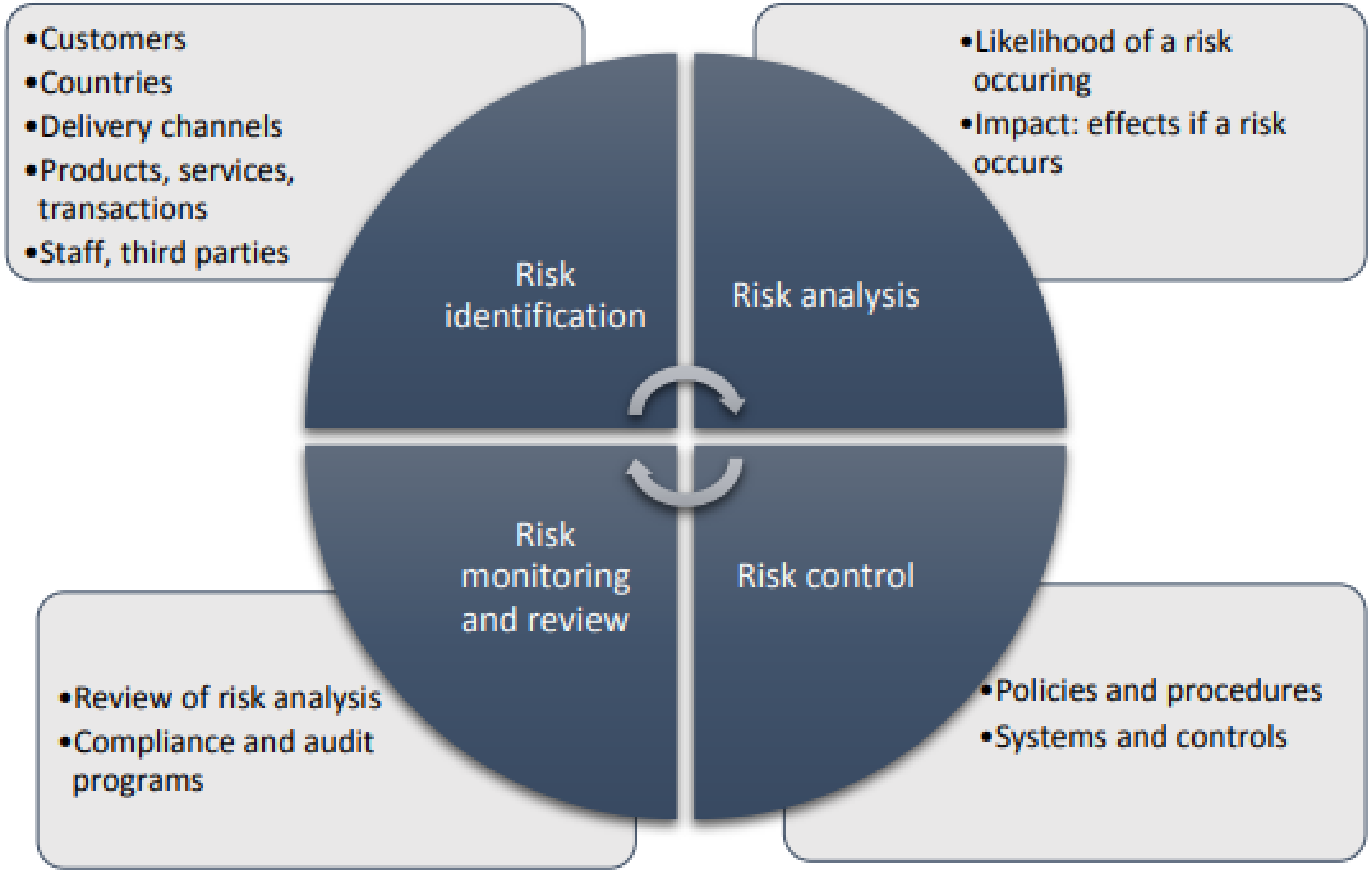
Report suspicious transactions to the FIAU, in accordance with the situations outlined in FATF recommendations 22 and 23
[Regulation 15 of the PMLFTR]

21

Not disclose the submission of an STR or related information to the FIAU to the subject or associates
[Regulation 16(1) of the PMLFTR]

Understanding ML/TF risk exposure

AML/CFT controls have to be commensurate to the ML/FT risks the individual institution is exposed to and effectively mitigate the same



Risk identification

- Customers
- Countries
- Delivery channels
- Products, services, transactions
- Staff, third parties

Risk analysis

- Likelihood of a risk occuring
- Impact: effects if a risk occurs

Risk control

- Policies and procedures
- Systems and controls

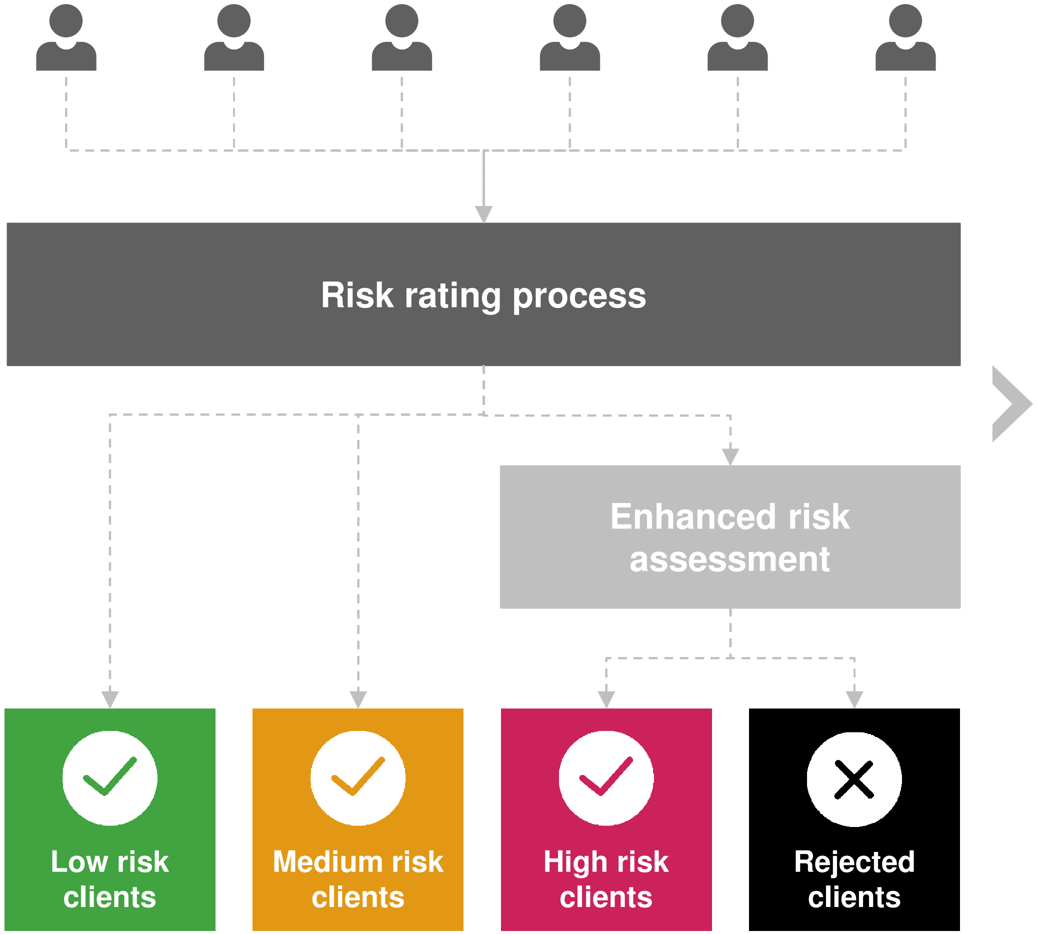
Risk monitoring and review

- Review of risk analysis
- Compliance and audit programs

Customer risk assessment

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

Illustrative approach



Usage

Onboarding

- Initial risk assessment and 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

Example indicators of high risk (1/2)

Internal risk assessments aim to qualify the level of risk posed by each client through consideration of key risk indicators

Customer risk

- ★ ❑ Are they sanctioned?
- ★ ❑ Do they engage in high-risk activities? (e.g. arms manufacturing, dealing)
- ❑ Are they a politically-exposed person (PEP)?
- ❑ Is their business cash-intense?
- ❑ Is their identity / beneficial ownership unclear, or masked by a complex structure?
- ❑ Are they an NPO?
- ❑ Is the source of funds unclear or illegitimate?

Product / service risk

- ★ ❑ Does the service provided appear to be an effort to conceal activities / identity from authorities?
- ❑ Does the service / transaction relate to high-risk commodities (e.g. crude oil)?
- ❑ Does the service / transaction relate to high-value materials (e.g. precious metals)
- ❑ Does the service / transaction relate to property in a high-risk area?
- ❑ Does the service / transaction relate to complex transactions or company structuring?

★ Indicates extremely high risk

Example indicators of high risk (2/2)

Internal risk assessments aim to qualify the level of risk posed by each client through consideration of key risk indicators

Geographic risk

- ★ ❑ Is the country sanctioned?
- ★ ❑ Is the country listed as non-cooperative in AML matters by FATF?
- ★ ❑ Does the country provide funding / support for terrorism according to the World Bank?
- ★ ❑ Is there a high level of corruption or criminal activity in the country?
- ❑ Is the shadow economy of the country large?
- ❑ Is the country politically unstable?
- ❑ Are terrorist organisations present within the country?

n.b. consideration should be given to the country of the client, but also all countries they transact / have links with

Channel risk

- ★ ❑ Is the product / service provided to a third party who has full discretionary authority for the client?
- ❑ Is the product / service provided through an agent or intermediary?
- ❑ Is the product / service provided remotely through a channel with little means of verifying the client's identity?

★ Indicates extremely high 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 • Issues reports on ML / TF trends and typologies
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

Part 3 | Questions

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 intelligence, 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