

Deloitte.

Link'n Learn
19 May 2016

Anti-money
laundering

Speakers



Niall O'Farrell

Senior Manager, Risk Advisory
Deloitte Ireland



Ciara O'Reilly

Manager, Risk Advisory
Deloitte Ireland

Agenda

- 1 The 4th EU Money Laundering Directive
- 2 Expected major effects on Irish legislation
- 3 EU Commission Updates to Directive
- 4 CBI Report on AML in Funds Industry
- 5 How does the CBI conduct an inspection?
- 6 AML Typologies
- 7 Next steps for investment funds and administrators

The 4th EU Anti Money Laundering Directive

Background and context



- The Third EU Anti Money Laundering Directive issued in 2005
- Transposed into local legislation over subsequent number of years, which drastically changed the approach to AML/CFT around the EU
- Elements of the Third Directive regarded as vague and non-prescriptive, making a consistent approach more difficult to achieve
- FATF issued framework recommendations and guidelines in 2012 to strengthen international standards
- Fourth EU AML Directive to be issued in response to this in 2015, with a lead time of 2 years for transposition to local legislation

Objectives of the Fourth EU AML Directive

- In order to remove ambiguities and improve consistency of AML/CFT rules across jurisdictions, Fourth Directive to be issued
- More clearly define obliged entity (designated persons) and competent authority requirements
- Assist in achieving standardised Anti-Money Laundering and Counter Terrorism Financing across EU Member States
- Counteract terrorist financing through improved adherence to obligations
- Increase the focus of obliged entities to threats of AML/CTF

Expected Effects on Irish Legislation

Impact

1. Risk Based Approach

- Member State requirement to evidence that appropriate steps have been taken to identify, assess, understand and mitigate AML/CTF risk
 - National Risk Assessment
- Obligated Entity requirement to evidence risk assessment will be more explicit in new Directive
 - Specific factors to be included e.g. customer, product, geography, channel i.e. bringing these FATF guidelines into legislation

2. CDD and Ongoing Monitoring

CDD:

- Minimum factors for consideration when applying Simplified CDD, and requirement to evidence rationale for applying SCDD
- More prescriptive requirements for applying Enhanced CDD and factors for consideration as higher risk

Ongoing Monitoring:

- More prescriptive requirements for conducting and keeping risk assessments up-to-date
- Requirement to evidence rationale for assignment of risk rating

Impact

3. Beneficial Owners & PEPs

Beneficial Ownership:

- Explicit requirement for legal persons to hold accurate and current information in relation to beneficial ownership of that legal person
- Provision of accurate information to obliged entities and competent authorities on request

PEPs:

- Definition of PEPs to be extended to include domestic PEPs
- Requirement to monitor persons ceasing to be PEPs for additional 6 months, i.e. for a total of at least 18 months

4. Senior Management & Third Party Equivalence

Senior Management:

- Definition of Senior Management to be introduced as employees/officers with specific knowledge of institutions exposure to AML/CTF risk, as well as sufficient seniority
- Clarity that Senior Management definition will not be restricted to members of the Board of Directors

Third Party Equivalence:

- Rescindment of the “white list” of equivalent jurisdictions for AML/CFT jurisdictions outside of the EU.
- Requirement for risk assessment to be conducted on countries outside of EU for AML/CFT purposes

Impact

5. Data Protection & Record Keeping

Data Protection:

- Requirement for consideration of Data Protection requirements for sharing customer information in AML/CFT procedures
- Clarity around application of AML/CFT rules for subsidiaries in third countries where legislation is deficient or non-equivalent

Record Keeping:

- Requirement to delete personal data 5 years after business relationship has come to an end (maximum of 10 years if greater period of retention required by Member State)

Additional Obligations

Competent Authority:

- Incorporate new directive requirements into legislation
- Perform a National Risk Assessment
- Provide guidance for adoption for obliged entities
- Assist with cooperation of Finance Intelligence Units on an international platform

Obligated Entity:

- Review risk classifications
- Maintain records to high quality standard that would stand up under CBI scrutiny
- Update procedures and systems to assist compliance with the new regulation requirements

EU Commission Updates to 4th Directive – February 2016

Key Updates Proposed



- Ensuring a high level of safeguards for financial flows from high risk third countries
- Enhancing the powers of EU Financial Intelligence Units and facilitating their cooperation
- Centralised national bank and payment account registers or central data retrieval systems in all Member States
- Tackling terrorist financing risks linked to virtual currencies
- Tackling risks linked to anonymous pre-paid instruments (e.g. pre-paid cards)

CBI Report on AML/CFT to Irish Funds Sector – November 2015

CBI Key Findings – AML/CFT Report

- 1 Governance
- 2 Risk assessments
- 3 Outsourcing
- 4 Customer Due Diligence
- 5 Suspicious Transaction Reporting
- 6 PEPs
- 7 Policies and Procedures

CBI Inspections – Potential Future Expectations

- 1 On-going Monitoring
- 2 CDD – Take-on of Investors from other administrators
- 3 Remediation of Investor register
- 4 IT Systems – User Access Management and System Interfaces
- 5 Acceptance of subsequent subscriptions and “as soon as practicable”
- 6 Management of Inactive Accounts

Themes



How does the CBI conduct an inspection?

How does the CBI conduct inspections for the Funds industry?



Fund Focused



CBI led inspection

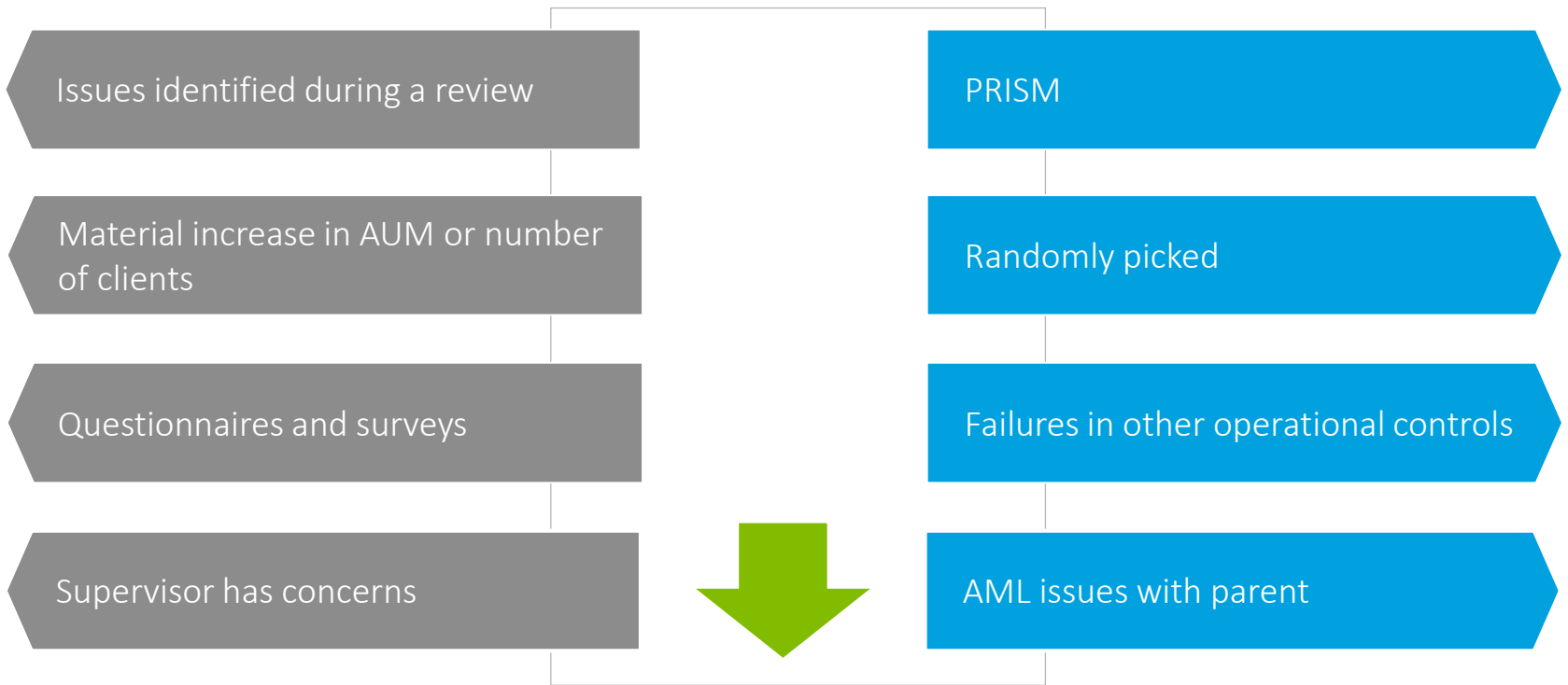


Deep Dive using third party



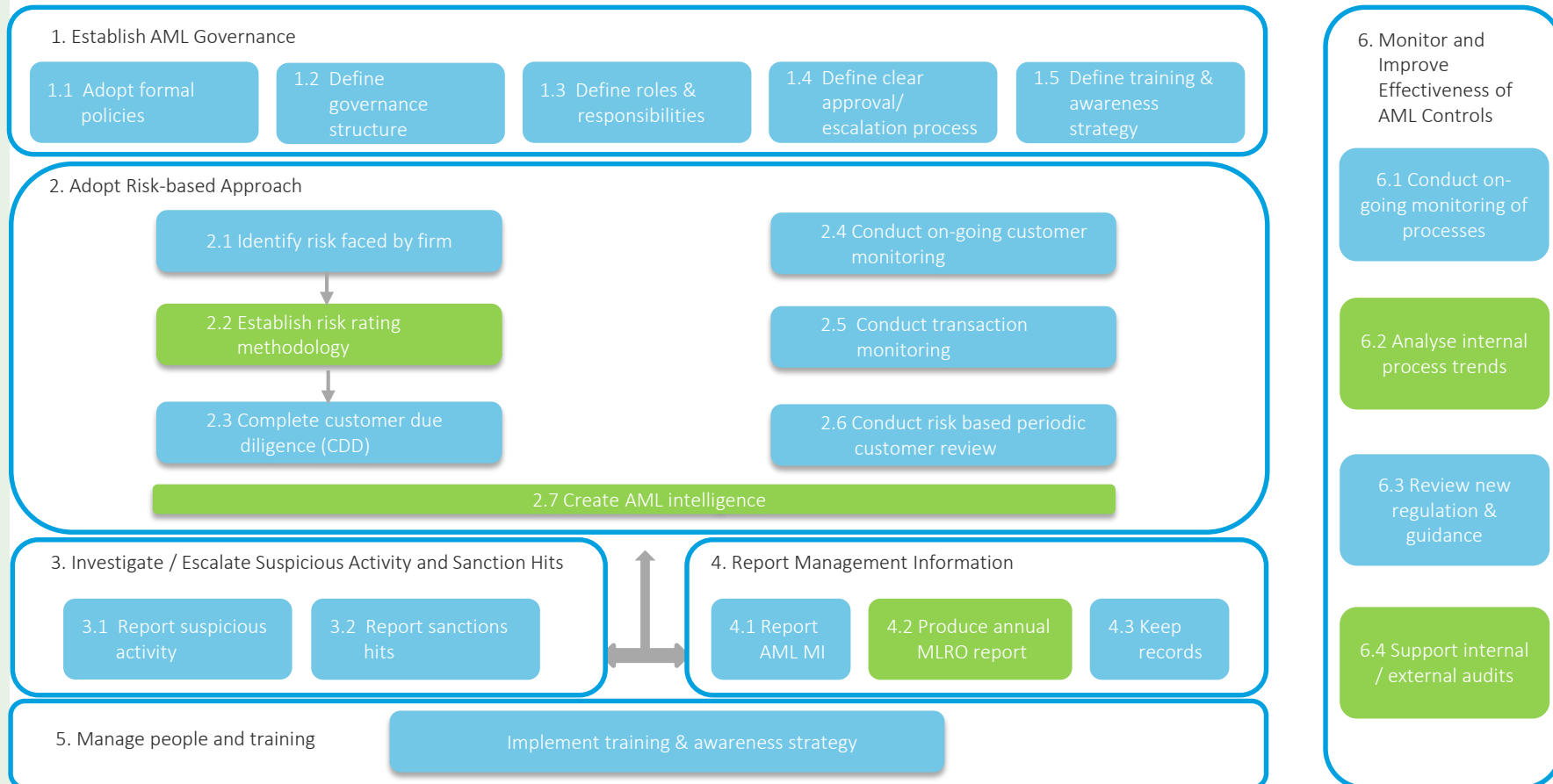
PRISM

Why does the CBI select an entity for inspection?

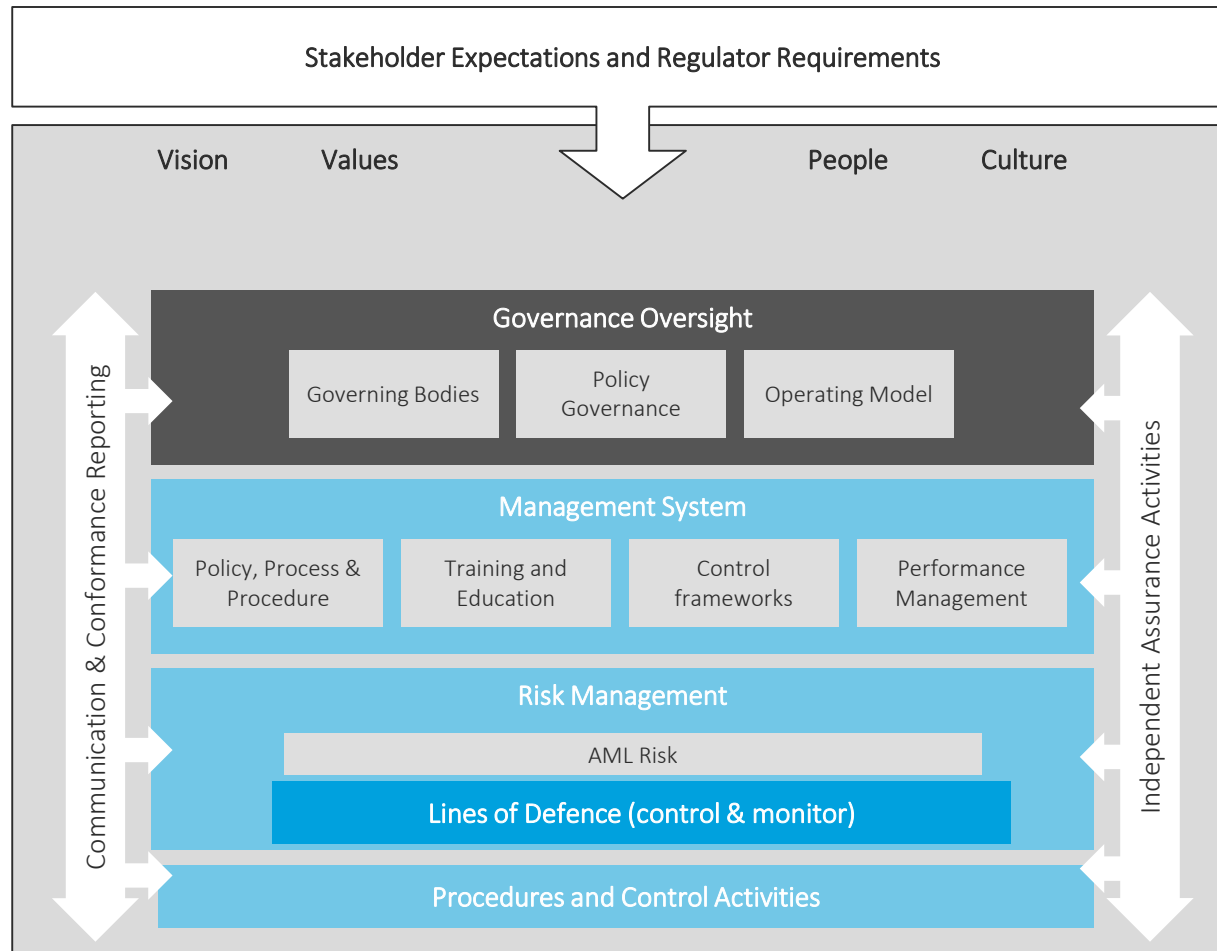


Triggers and reactive measures should be developed in this regard

Central Bank review framework



Governance - AML Risk Framework



Risk Maturity

Low probability high impact events- maturity model

	Tier 1 Aware	Tier 2 Informed	Tier 3 Rehearsed	Tier 4 Prepared	Tier 5 Ready
Anticipate	<ul style="list-style-type: none"> - Current risks are identified by central team - Risk register socialised with business units 	<ul style="list-style-type: none"> - Horizon scanning at enterprise level - Risk modelling at enterprise level 	<ul style="list-style-type: none"> - Risk Model used to highlight business specific Div risks - Central team risk and threat intelligence used to anticipate 	<ul style="list-style-type: none"> - Div risk intelligence and horizon scanning - War Gaming to challenge assumptions and thinking 	<ul style="list-style-type: none"> - Operational staff routinely scan risk and threat - Enterprise wide intelligence - War Gaming considers the worst case - hardening plans
Assess	<ul style="list-style-type: none"> - Risk assessment of current risk and threat at group level only 	<ul style="list-style-type: none"> - Analysis of risk and threat at enterprise level - Enterprise wide impact analysis and gap analysis 	<ul style="list-style-type: none"> - Analysis of Div specific risks and threats - Specific risks and threats drive revised SOPs 	<ul style="list-style-type: none"> - Risk assessments are linked to specific controls - Catastrophic risks analysed at enterprise level 	<ul style="list-style-type: none"> - Catastrophic risks and threat analysed at Div level - Leverage risk analysis, determine governance and level of preparation
Plan	<ul style="list-style-type: none"> - Ad hoc operating plans in place 	<ul style="list-style-type: none"> - Generic enterprise wide SOPs in place - Plans form part of a broader over-arching strategy 	<ul style="list-style-type: none"> - Specific SOPs linked to risk and threat assessment - Detailed mitigation and contingency plans by Div 	<ul style="list-style-type: none"> - Specific response and recovery plans operational - All plans enhanced to mitigate identified risk 	<ul style="list-style-type: none"> - SOPs reflect risk assessment change management - Expanded enterprise plans embedded and agreed
Control	<ul style="list-style-type: none"> - Generic crisis management structure in place with defined escalation criteria 	<ul style="list-style-type: none"> - Specific escalation procedures to reflect identified risk and threat - Div level control mechanisms identified 	<ul style="list-style-type: none"> - Practiced escalation procedures at Div level - Clearly understood procedure to escalate to group level 	<ul style="list-style-type: none"> - Accountability and decision making level escalations reflect the risk profile - Command and control enhanced to reflect specific risk 	<ul style="list-style-type: none"> - Specific controls mechanisms exercised in context with horizon (War Game) - Enterprise and expanded enterprise control mechanisms active
Test & Evaluate	<ul style="list-style-type: none"> - Generic risk management and threat awareness campaigns to all Div and functions 	<ul style="list-style-type: none"> - Specific targeted campaigns to all staff of identified risk and threat - Executive level risk management training 	<ul style="list-style-type: none"> - Senior management assessed against risk management criteria - Enterprise wide risk training - Crisis awards for all Div 	<ul style="list-style-type: none"> - Risk management metrics used to evaluate management performance - Regular training through simulation and War Gaming 	<ul style="list-style-type: none"> - Risk metrics embedded in appraisal process at all levels - Simulation and War Gaming for staff and expanded enterprise in ad hoc and re-building

Increasing Maturity →

US FinCEN Recent Awards

SAR Review Task Force – IRS Criminal Investigation

Transnational Organised Crime - FBI

Transnational Security Threat – US Customs and Border Protection National Targeting Center

Third Party Money Laundering – IRS Criminal Investigation

Significant Fraud – Immigration and Customs Enforcement – Homeland Security Investigations

What should we do now?

Next Steps for investment funds and administrators

Review existing investor books and practices for regulatory expectations and legislative requirements

Revisit and expand risk assessments to incorporate financial sanctions as well as AML/CFT

Perform an impact assessment for the transposition of the 4th EU AML Directive into local legislation

Q&A





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/ie/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

With nearly 2,000 people in Ireland, Deloitte provide audit, tax, consulting, and corporate finance to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. With over 210,000 professionals globally, Deloitte is committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, Deloitte Global Services Limited, Deloitte Global Services Holdings Limited, the Deloitte Touche Tohmatsu Verein, any of their member firms, or any of the foregoing's affiliates (collectively the "Deloitte Network") are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.