

Governance and Compliance

Risk Assessment

- Firms undertake and document a Money Laundering/Terrorist Financing risk assessment of their business, to include all risk categories (such as geographic risk, product/service risk, investor risk and channel/distribution risk).
- The underlying methodology, assumptions and risk ratings used are documented.
- Appropriate controls are devised to mitigate any risks identified and that these controls are aligned to and embedded in operational procedures.

Outsourcing

- Firms have appropriate oversight of outsourced service providers carrying out AML/CFT functions, notwithstanding whether the outsourced service provider is a related group entity or comes from outside the group.
- Oversight of outsourced service providers would include the review of the outsourced service provider's policies and procedures and appropriate assurance testing of any AML/CFT functions performed e.g. transaction monitoring processes, suspicious transaction reporting processes and processes to ensure appropriate approval of high risk investors.
- Suitable quantitative and qualitative data is reported to the Board of the Firm by the outsourced service provider to allow an informed view of risks and trends, including reports on the functions carried out by the outsourced service provider and regular MI.
- Firms ensure that all staff undertaking AML/CFT roles on behalf of the Firm are instructed on the law relating to Money Laundering/Terrorist Financing and are provided with on-going training.
- AML/CFT functions are appropriately resourced to perform their roles efficiently and effectively and are subject to regular monitoring and review, for example by Internal Audit.

Roles and Responsibilities

- A Firm's Board can demonstrate active engagement in the monitoring and management of Money Laundering/Terrorist Financing risk, including involvement in the completion of a Money Laundering/Terrorist Financing risk assessment and continuing consideration of industry developments that may impact the business.
- A Firm has access to the necessary capabilities to ensure the appropriate oversight of service providers carrying out AML/CFT functions, including the review of policies and procedures and assurance testing of the AML/CFT functions performed.
- MI and MLRO Reports provided to the Board, include suitable quantitative and qualitative data to provide (i) an informed view on the performance of the functions carried out by service providers and (ii) an understanding of risks and trends

Governance and Compliance

Policies and Procedures

When developing AML/CFT policies and procedures;

- Have a clearly defined process in place for the formal review and approval, at least annually, of the policies and procedures at appropriate levels.
- Risk assessments are reviewed on a frequent basis, at least annually, and are actively used to inform the Firm's risk-based approach and the design of AML/CFT controls.
- Policies and procedures demonstrably comply with all legal and regulatory requirements.
- Have appropriate procedures and controls in place to ensure compliance with all aspects of Section 33(8) of the CJA 2010 for investors that have failed to provide adequate CDD documentation or information.
- Have effective policies and procedures in place for the management of PEPs, including procedures for carrying out EDD and for obtaining senior management sign off of PEP relationships. The policies and procedures should also outline timelines for senior management sign off and indicate the seniority of sign off required.

Training

- Firms ensure that all persons involved in the conduct of the business (including staff at outsourced service providers) are instructed on the law relating to Money Laundering/Terrorist Financing and are provided with on-going training.
- Adequate training records for all staff are retained.

On- Boarding of Customer

- Policies and procedures are to set out additional CDD as a result of increasing or heightened risk.
- Investor and beneficial owner ID & Verification procedures should be embedded within the Firm and detailed operational requirements for on-boarding established.
- Evidence to support the application of SCDD to be contained on the investor file.
- Firms to ensure that they have effective policies and procedures in place for the management of PEPs, including senior management sign off of the PEP relationship.
- Firms, when scrutinising the SOF, to seek to discover the origin and the means of transfer of the funds that are involved in the transaction (for example, occupation, business activities, proceeds of sale, corporate dividends) and when scrutinising the SOW, to seek to discover the activities that have generated the total net worth of the investor (that is, the activities that produced the investor's funds and property).
- Policies and procedures set out the circumstances under which the Firm would cease to provide services or would discontinue an existing business relationship due to an investor's failure to provide the required or updated CDD documentation or information.
- The policies and procedures should outline the process and timeline for ceasing the provision of services.

Customer Due Diligence

On- Boarding of Customer

- Policies and procedures are to set out additional CDD as a result of increasing or heightened risk.
- Investor and beneficial owner ID & Verification procedures should be embedded within the Firm and detailed operational requirements for on-boarding established.
- Evidence to support the application of SCDD to be contained on the investor file.
- Firms to ensure that they have effective policies and procedures in place for the management of PEPs, including senior management sign off of the PEP relationship.
- Firms, when scrutinising the SOF, to seek to discover the origin and the means of transfer of the funds that are involved in the transaction (for example, occupation, business activities, proceeds of sale, corporate dividends) and when scrutinising the SOW, to seek to discover the activities that have generated the total net worth of the investor (that is, the activities that produced the investor's funds and property).
- Policies and procedures set out the circumstances under which the Firm would cease to provide services or would discontinue an existing business relationship due to an investor's failure to provide the required or updated CDD documentation or information.
- The policies and procedures should outline the process and timeline for ceasing the provision of services.

On – Going Monitoring

- Firms ensure they have effective on-going monitoring policies and procedures in place including full review and consideration of all trigger events associated with their underlying investors.
- Investors re-categorised as PEPs are subject to senior management approval and the completion of EDD.

Reliance on Third Parties

- There is a signed agreement in place between the Firm and the relevant third party, where the third party has formally consented to being relied on and will, without any restriction, provide the Firm with the underlying CDD documents or information, in a timely manner, upon request.
- The signed agreement must not contain any conditional language, whether explicit or implied, which may result in the inability of the relevant third party to provide the underlying CDD documentation or information upon request. Examples of such conditional language include (but are not limited to) terms such as 'to the extent permissible by law', 'subject to regulatory request' etc.
- Policies and procedures set out an approach with regard to the identification, assessment, selection and monitoring of third party relationships, including the frequency of testing performed on such third parties.
- The Firm only relies on the relevant third party to carry out CDD measures required by Section 33 and 35(1).

Identification and Escalation of Suspicious Transactions

Suspicious Transaction Reporting

- Firms review and validate any monitoring systems and/or reports to ensure that they are meaningful and effective, in particular where transaction monitoring systems generate low levels of alerts.
- Policies and procedures contain an adequate description for directors and/or employees of the Firm of their obligations to report a suspicious transaction, as well as guidance on how to complete and submit such reports.
- If the suspicion is not reported, the outcome and reasons for not doing so should be documented and retained.
- Firms have policies and procedures in relation to reporting suspicions that may arise as a result of a failure on the part of the investor to provide the required or updated CDD documentation or information.
- In situations where there a “suspicious” or “unusual” transaction has been identified, the firm may not know if there is an predicate underlying predicate offence. However, where the underlying offence is identified, (in addition to the STR), that offence should be reported separately to An Garda Síochána.

Terrorist Financing & EU Financial Sanctions

Terrorist Financing

- Firms take measures to prevent Terrorist Financing and adopt measures to prevent Terrorist Financing commensurate with the risk. The preventative measure for anti-money laundering and combating the financing of terrorism are the same but will be applied at times in different ways.
- Firms take measures to prevent the financing of terrorism such as carrying out customer due diligence, on-going monitoring, reporting of suspicious transactions, training and have in place effective policies and procedures.
- If a Firm has knowledge or a suspicion of Terrorist Financing, it must immediately file an STR.
- In the event that an investor is matched to either the EU terrorist lists or UN terrorist lists, the Firm should file an STR immediately with the Financial Intelligence Unit in the Garda Bureau of Fraud Investigation and not carry out any service or transaction in respect of the account until the report has been made. When the report is made, the Gardaí can then take steps and/or give directions to the Firm in respect of the account as appropriate under the CJA 2005 and/or CJA 2010. Where a person or entity is listed in an EU Council Regulation relating to terrorism, there is a legal obligation to immediately freeze that person or entity's account.

EU Financial Sanctions

- Firms will devise and implement policies, procedures, systems and controls, to facilitate adherence to their obligations in relation to FS Regulations, for example the implementation of appropriate FS screening mechanisms and procedures for the escalation and management of any potential FS matches.