AML/CFT Legislative Package

Handbook on the new AML/CFT Regime for Insurance, Credit and Financial Intermediaries

May 2025

FOREWORD: BIPAR

The new EU's legislative package aimed at strengthening the EU framework on anti-money laundering and countering the financing of terrorism (AML/CFT) will apply from July 2027.

The revised EU AML/CFT framework will require in-scope insurance, financial and credit intermediaries to take additional actions to maintain effective compliance.

The intermediary sector takes the anti-money laundering and countering the financing of terrorism seriously. BIPAR commissioned the Brussels office of Steptoe LLP to draw up a handbook which aims to help associations of in-scope intermediaries and the intermediaries themselves to navigate the requirements of the new AML/CFT framework.

Responsibility for compliance with all relevant EU and national legislation rests with individual firms and we hope that this handbook will encourage market participants, and national regulators and supervisory authorities to continue building together a realistic and efficient framework and system of AML/CFT.

This handbook is up to date as per March 2025 and does not yet cover the Level 2 or Level 3 more detailed rules.

We thank the authors, Guy Soussan, Partner, and Algirdas Semeta, Legal Consultant, for their fruitful work and Isabelle Audigier, BIPAR Legal Director, and Rebekka De Nie, EU Policy Manager, who led BIPAR participation in this work.

Nicolas Bohême

Chairman, BIPAR

Nic De Maesschalck

Director, BIPAR

FOREWORD: STEPTOE LLP

With a long-standing presence advising on EU financial services legislation, Steptoe's Brussels office has been a source of guidance to a wide range of financial institutions navigating the diverse regulatory requirements applicable to the sector. A key area of focus for us and the insurance industry is AML/CFT compliance. Given our shared commitment, we are delighted to have worked with BIPAR on this handbook.

The new AML/CFT legislative package marks a significant change. It fully harmonises AML/CFT rules and makes them directly applicable in all Member States. In addition to establishing more thorough rules and procedures in several important areas, the package also clarifies and modifies the existing AML/CFT obligations.

Insurance and financial intermediaries have been subject to AML/CFT requirements for nearly two decades. Current EU AML/CFT rules cover insurance intermediaries involved in life and other investment-related insurance services, though some Member States also apply the requirements to non-life insurance intermediaries. Financial intermediaries that are authorised as investment firms or that operate under the so-called "opt-out" regime of the MiFID II also fall within the scope of the current EU AML/CFT framework. The new AML/CFT legislative package extends the EU-level AML/CFT requirements to certain credit intermediaries. The revised EU AML/CFT framework will require in-scope intermediaries to take additional actions to maintain effective compliance.

We have drafted this handbook to help intermediaries prepare to meet the detailed requirements. With this goal in mind, the handbook:

- summarises the requirements of the new framework;
- draws attention to key changes;
- comments on the main implications for intermediaries.

Who should read this document?

This document will be of interest to insurance brokers, agents, and all other insurance distributors involved in life and other investment-related insurance services. It is also relevant for consumer and mortgage credit intermediaries, as well as financial intermediaries.

Intermediaries subject to AML/CFT rules should read this document to check whether they will need to adapt their operations to ensure that their activities comply with all relevant rules.

After reading this document

This document is not exhaustive and is provided solely for general information purposes. It does not provide legal advice. It is based on the provisions and requirements of the AML/CFT legislative package and other EU law sources.

If, after reading this document, you require further clarification on how the new AML/CFT framework affects your insurance distribution or financial/credit intermediation activities, or if you have any remaining doubts about your obligations, you should seek legal advice tailored to your specific situation.

Guy Soussan

Partner, Steptoe

Algirdas Semeta

Associate, Steptoe

bipar Steptoe

CONTENTS

INTRODUCTION

The new EU's legislative package, aimed at strengthening the EU framework on anti-money laundering and countering the financing of terrorism (AML/CFT), was published in the EU's Official Journal on 19 June 2024. The legislative package comprises:[1]

- The 6th AML/CFT Directive (AMLD6)[2] deals with organisational and institutional aspects of the AML/CFT framework;
- The Single Rulebook Regulation (SRR)[3] sets out the substantive AML/CFT rules and requirements which economic operators must apply to prevent AML/CFT; and
- The AMLA Regulation[4] establishes the EU's Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA).

The AMLD6, the SRR and the AMLA Regulation entered into force on 9 July 2024. The Member States have to adopt national laws implementing the AMLD6 by 10 July 2027.[5] **Similarly, the substantive AML/CFT requirements of the SRR will apply from 10 July 2027**.[6]

The adoption of the SRR marks an important change to the EU's AML/CFT framework. Under the current EU regime, the Member States have a degree of flexibility to decide how to implement the requirements of the AML Directives in their national legal systems. In contrast, the SRR contains a single set of substantive AML/CFT rules which will directly apply in all Member States and do not have to be implemented into national laws. With the adoption of the SRR, economic operators should benefit from a further harmonisation of the current varying national AML/CFT frameworks.

This document provides a brief overview of the **SRR** and the **AMLD6**. Its aim is to guide in-scope insurance/credit/financial intermediaries through the essential elements of the new EU legislation and to help the intermediaries navigate the requirements of the new AML/CFT framework. **This document is not legal advice. For specific questions, readers should take their own advice which considers their particular circumstances**.

The substantive AML/CFT rules in the SRR build on the current EU AML/CFT legislation.[7] However, the SRR goes beyond mere reiteration of the current requirements. It clarifies and

[1] The legislative package also includes the so-called Transfer of Funds Regulation (Regulation (EU) 2023/1113).

[2] Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849.

[3] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[4] Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

[5] The AMLD6 provisions on access to beneficial ownership registers have to be implemented by 10 July 2026 and the rules on single access point to real estate information - by 10 July 2029.

[6] The new framework will apply to football agents and professional football clubs from 10 July 2029.

[7] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended by Directive (EU) 2018/843 (AMLD5).

adapts the existing AML/CFT obligations and, at the same time, establishes more detailed rules and procedures in several key areas.

The SRR and the AMLD6 are so-called Level 1 legal texts which set out the principles and core provisions of the new EU AML/CFT framework. The provisions of the SRR and the AMLD6 will be further detailed in Level 2 (delegated acts, regulatory/implementing technical standards) and Level 3 (guidelines) texts. Annex III to this document lists the Level 2 and 3 measures which are foreseen under the SRR and the AMLD6.

In-scope intermediaries will need to carefully review their existing AML/CFT policies and procedures against the provisions of the SRR in order to identify the necessary changes.

SCOPE

Obliged Entities

The new AML/CFT framework applies to the **obliged entities** listed in Article 3 of the SRR, including:

- Credit institutions;
- Financial institutions.

For the purposes of the SRR, **financial institutions** comprise, among others[8]:

- Insurance undertakings carrying out life or other investment-related insurance activities;
- Insurance intermediaries[9] where they act with respect to life insurance and other investment-related insurance services;
- Investment firms;[10]
- Credit intermediaries;
- Crypto-asset service providers.

Insurance Intermediaries

In line with the current framework, only insurance intermediaries acting with regard to **life insurance and other investment-related insurance services** fall within the scope of the SRR and must comply with the AML/CFT requirements. Insurance intermediaries pursuing insurance distribution in relation to non-life insurance products remain outside the scope of the SRR.

The SRR also maintains the current exemption for insurance intermediaries which engage in the distribution of life-insurance and investment-related insurance products, but: (i) act under the

[8] Article 2(6), SRR.
[9] As defined in Article 2(1)(3) of the IDD.
[10] As defined in Article 4(1) of the MiFID II.

responsibility of one or more insurance undertakings or intermediaries; and (ii) do not collect premiums or amounts intended for the customer.[11]

In sum, the scope of the SRR in relation to insurance intermediaries remains the same. Only the intermediaries, which are subject to the AML/CFT requirements under the current framework, will have to comply with the new AML/CFT requirements of the SRR.

Credit Intermediaries

The SRR introduces AML/CFT requirements for **consumer and mortgage credit intermediaries**.[12] For the purposes of the SRR, a credit intermediary is a natural or legal person, who, in the course of their trade, business, or profession, and for remuneration: (i) presents or offers credit agreements to consumers; (ii) assists consumers by undertaking preparatory work or other pre-contractual administration in respect of credit agreements; or (iii) concludes credit agreements with consumers on behalf of the creditor.[13]

Not all consumer and mortgage credit intermediaries fall within the scope of the SRR:

- Only those that **hold funds** (i.e. banknotes and coins, scriptural money, or electronic money)[14] in connection with credit agreements are subject to the SRR and must comply with the AML/CFT requirements.
- Credit intermediaries **that operate under the responsibility of one or more creditors or other credit intermediaries** are not subject to the SRR.[15]

Implications for credit intermediaries

In-scope consumer and mortgage credit intermediaries will need to prepare to meet the detailed requirements of the SRR. In particular, they will need to establish and implement all necessary AML/CFT internal policies, procedures and controls, as well as conduct customer due diligence on their customers.

Financial Intermediaries

In line with the current framework, the SRR applies to investment firms, as defined in the MiFID II Directive.[16] As a general rule, all financial intermediaries that meet the definition of an

[11] Article 2(6)(c) of the SRR.
[12] Recital 22 of the SRR. Under the current EU regime, credit intermediaries are not subject to the AML/CFT requirements.
[13] Article 4(5) of Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010; Article 3(f) of Directive 2008/48/EC on credit agreements for consumers and repealing Council Directive 87/102/EEC.
[14] Article 4(25) of Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010.
[15] Article 2(6)(h), SRR.
[16] Article 2(6)(d), SRR.

investment firms within the meaning of the MiFID II Directive, including those that pursue activities under the so-called "opt-out" regime[17], are subject to the SRR.

Potentially broader scope in some Member States

Same as under the current EU AML/CFT framework, Article 3 of the AMLD6 allows Member States to apply all or part of the SRR requirements to additional entities in other sectors if the Member States determine that these entities are exposed to ML/TF risks. Some Member States currently extend their national AML/CFT frameworks to non-life/general insurance intermediaries and will maintain the right to do so under the new framework (please see Annex II to this document).

PROPORTIONALITY

Risk-based approach

A fundamental pillar of the new AML/CFT framework is the risk-based approach. It applies to both obliged entities and their supervisors.

For obliged entities

The risk-based approach determines and is reflected in a number of obligations of obliged entities (including intermediaries) under the new AML/CFT framework, including:

- The ability of the Member States to impose additional requirements;
- Exemption of certain economic operators;
- Internal controls framework;
- Outsourcing;
- Composition/staffing of the compliance function;
- Customer due diligence (CDD) measures;
- Oversight of existing business relationships/existing customers;
- The intensity of monitoring of suspicious transactions;
- Transactions/business relations with politically exposed persons (PEPs).

[17] Pursuant to Article 3 of MiFID II, Member States may decide not to apply the Directive to certain persons established in that Member State provided that the activities of those persons are authorised and regulated at national level.

For supervisors

Member States must ensure **effective, impartial and risk-based supervision** of obliged entities[18] based on the following principles:

- Each Member State must take necessary measures to accurately identify, assess, understand, and mitigate its risks related to ML/TF.[19]
- Member States should ensure consistent action at the national level by designating an authority or establishing a mechanism to coordinate the national response to the risks.[20]
- Supervisors should adopt a risk-based approach to their work. They should be able to allocate their tasks and resources effectively towards areas with the highest risks, whilst ensuring that no sector or entity is vulnerable to criminal attempts to launder money or finance terrorism.[21]

National and supra-national risk assessments

Under the risk-based approach, national and EU-wide risk assessments impact the application and the extent of numerous AML/CFT requirements set out in the SRR and AMLD6.

Union-wide risk assessment

The European Commission must conduct an assessment of ML/TF risks at the EU level and in relation to cross-border activities. The Commission is required to publish a report detailing its findings by 10 July 2028. The report has to be updated every four years (the Commission can update parts of the report more frequently).[22]

National risk assessment

Each Member State has to conduct national risk assessments. These assessments must be reviewed and updated at least every four years. The insights gained from the assessments will guide the Member States in refining their national AML/CFT frameworks to effectively address the identified risks.[23]

Risk variables and factors for obliged entities

The purpose of the following section is to provide an overview of the risk variables and factors to consider when conducting risk assessments and risk-based decision-making.

[18] Recital 84 and Article 8(1), AMLD6.
[19] Recital 14, AMLD6.
[20] Recital 19 and Article 8(2), AMLD6.
[21] Recital 88, AMLD6.
[22] Article 7, AMLD6.
[23] Article 8, AMLD6.

A specific expression of the risk-based approach can be found in Annexes I-III of the SRR. The Annexes set out non-exhaustive lists of **risk variables** and **risk factors** which obliged entities need to consider when conducting the business-wide risk assessment and determining the extent of the CDD measures.

Risk variables[24]

Category	Risk variable
Customer risk variables	► Business or professional activity of the customer and beneficial owner ► Reputation of the customer and beneficial owner ► Nature and behaviour of the customer and beneficial owner ► Jurisdictions where the customer and beneficial owner are based ► Main places of business of the customer and beneficial owner ► Relevant personal links of the customer and beneficial owner to certain jurisdictions
Product, service or transaction risk variables	► Purpose of an account or relationship ► Regularity or duration of the business relationship ► Level of assets to be deposited or size of transactions undertaken ► Level of transparency or opaqueness of the product, service or transaction ► Complexity of the product, service, or transaction ► Value or size of the product, service, or transaction
Delivery channel risk variables	► Extent of non-face-to-face business relationships ► Presence and nature of introducers or intermediaries used by the customer
Risk variable for **life and other investment-related insurance**	► Risk level presented by the beneficiary of the insurance policy

[24] A non-exhaustive list of risk variables is set out in Annex I to the SRR.

Annex I, point (d) of the SRR considers the risk level presented by the beneficiary of the insurance policy to be a risk variable for life insurance and other investment-related insurance. The risk level associated with the beneficiary of an insurance policy can vary based on several factors, including but not limited to, the beneficiary's financial history, country of residence, and other relevant considerations.

Lower risk factors[25]

Category	Risk factor
Customer risk factors	▶ Public companies listed on a stock exchange with disclosure requirements ensuring transparency of beneficial ownership ▶ Public administrations or enterprises ▶ Residents in lower risk areas, as specified in geographical risk factors (see below)
Product, service, transaction, or delivery channel risk factors	▶ Life insurance policies with a low premium ▶ Pension scheme insurance policies with no early surrender option and the policy cannot be used as collateral ▶ Pension/superannuation schemes that provide retirement benefits, contributions deducted from wages, no assignment of member's interest ▶ Financial products/services that are defined and limited services to certain customer types for inclusion purposes ▶ Products where ML/TF risks are managed by other factors (purse limits, ownership transparency, etc.)
Geographical risk factors[26]	▶ Member States ▶ Third countries: ■ With effective AML/CFT systems ■ Identified by credible sources as having low levels of corruption or criminal activity ■ Meeting FATF Recommendations and effectively implementing them

[25] A non-exhaustive list of lower risk factors is set out in Annex II to the SRR.
[26] Referring to registration, establishment, or residence of a customer.

Annex II, point (2), subpoints (a) and (b) of the SRR list two **lower risk factors** related to **insurance**:

- Life insurance policies for which the premium is low.
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.

These policies are considered lower risk due to their limited financial investment and liquidity, respectively.

Higher risk factors[27]

Category	Risk factor	Details
Customer risk factors	▶ Unusual circumstances	Business relationships or transactions conducted in unusual circumstances
	▶ High-risk areas	Customers resident in geographical areas of higher risk
	▶ Asset-holding vehicles	Legal persons or arrangements that are personal asset-holding vehicles
	▶ Nominee shareholders	Corporate entities with nominee shareholders or shares in bearer form
	▶ Cash-intensive businesses	High volume of cash transactions
	▶ Complex ownership	Ownership structure appears unusual or excessively complex
	▶ Investment for residence	Third-country nationals applying for residence rights in exchange for investment
	▶ No economic activity	Legal entities or arrangements with no real economic activity or presence
	▶ Indirect ownership	Customers owned by entities or arrangements with no real economic activity
Product, service, transaction, or delivery channel risk factors	▶ Private banking	-
	▶ Anonymity-favouring products	-

[27] A non-exhaustive list of higher risk factors is set out in Annex III to the SRR.

Category	Risk factor	Details
	► Unknown payments	Payments received from unknown or unassociated third parties
	► New products, business practices, or technologies	-
	► High-risk transactions	Transactions related to oil, arms, precious metals, stones, tobacco, cultural artefacts, etc.
Geographical risk factors	► Third countries	Under increased monitoring by the FATF
		Without effective AML/CFT systems
		With significant levels of corruption or criminal activity
		Subject to sanctions, embargos or similar measures
		Providing funding or support for terrorist activities
		Identified as enabling financial secrecy

By 10 July 2026, **AMLA** will issue **guidelines** detailing the risk variables and risk factors that obliged entities should consider when initiating business relationships or carrying out occasional transactions. The future guidelines will be useful for intermediaries in preparing to comply with their CDD obligations under the SRR.

What has changed?

The SRR significantly expands the non-exhaustive list of risk variables in Annex I and clarifies their intended purpose: in addition to determining the extent of the CDD measures to be applied to individual business relationship or occasional transactions (individual risk assessment), the risk variables will have to be used in conducting the business-wide risk assessment. The SRR also adds the risk level presented by the beneficiary of the insurance policy as a new standalone risk variable. These changes should have only a limited impact on obliged entities since the SRR risk variables already appear as risk factors in the current EU AML/CFT regime.[28]

Implications for intermediaries

The SRR provisions on risk variables and lower/higher risk factors should not significantly affect the way in which insurance and financial intermediaries currently conduct business-wide and individual risk assessments or apply the CDD measures. That said, intermediaries will need to ensure that their written AML/CFT policies and other AML/CFT documentation correctly reflect the wording and structure of the relevant SRR provisions (in particular, the transfer of the current risk factors into the category of risk variables).

Credit intermediaries will need to familiarise themselves with the risk variables and risk factors of the SRR and prepare to apply them when conducting business-wide risk assessments and determining the extent of the CDD measures.

REQUIREMENTS FOR OBLIGED ENTITIES

The substantive AML/CFT obligations of obliged entities under the SRR can be divided into two broad categories:

Organisational requirements for obliged entities, including:

- Obligation to put in place internal policies, procedures and controls;
- Conducting business-wide risk assessment;
- Compliance function;
- Outsourcing;
- Requirements for staff of obliged entities, including procedures to prevent and manage conflicts of interest;
- Group-wide requirements.

[28] See Guideline 2 of the ML/TF Risk Factors Guidelines of the European Banking Authority (EBA).

Requirements in relation to customers/business relationships, including:

- CDD measures, including enhanced due diligence and simplified due diligence;
- Reporting of suspicious transactions.

Organisational requirements for obliged entities

Obligation to set up internal policies, procedures and controls

The SRR requires obliged entities to put in place internal policies, procedures and controls to mitigate and manage effectively the ML/TF risks and the risk of non-implementation and evasion of targeted financial sanctions.[29, 30] The SRR requirements build on the current AML/CFT regime, but the content of the requirements has been reinforced and clarified to achieve greater harmonisation.

In line with the risk-based approach, internal policies, procedures and controls have to be proportionate to the nature of the obliged entity's business, including its risks and complexity, and the size of the obliged entity.

The following table outlines the requirements for the internal policies, procedures and controls of obliged entities.

Category	Requirement
Internal policies and procedures	▶ Carrying out a business-wide risk assessment ▶ An entity-level risk management framework ▶ Customer due diligence ▶ Reporting of suspicious transactions ▶ Outsourcing and reliance on customer due diligence performed by other obliged entities ▶ Record retention and policies related to the processing of personal data[31] ▶ Monitoring and managing compliance with internal policies and procedures ▶ Identifying and managing deficiencies ▶ Implementing remedial actions

[29] Chapter II, Section 1 of the SRR.
[30] Pursuant to Article 2(49) of the SRR, "targeted financial sanctions" are defined as "both asset freezing and prohibitions to make funds or other assets available, directly or indirectly, for the benefit of designated persons and entities pursuant to Council Decisions adopted on the basis of Article 29 TEU and Council Regulations adopted on the basis of Article 215 TFEU".
[31] See Articles 76-77 of the SRR.

Category	Requirement
	▶ Verifying the good repute of staff, agents and distributors, proportionate to the risks associated with their tasks and functions ▶ Communication of policies, procedures and controls internally and to agents, distributors and service providers involved in the implementation of entity's AML/CFT policies ▶ Establishing a training policy for employees, agents and distributors in relation to entity's compliance measures[32]
Internal controls and independent audit function	▶ Internal controls and an independent audit function must be in place to test the effectiveness of the internal policies, procedures and controls in place ▶ In the absence of an independent audit function, the testing may be carried out by an external expert
Approval	▶ Internal policies must be approved by the obliged entity's management body in its management function ▶ Internal procedures and controls must be approved at least by the compliance manager
Documentation	▶ Internal policies, procedures and controls must be recorded in writing and kept up-to-date ▶ Internal policies, procedures and controls must be enhanced where weaknesses are identified

By 10 July 2026, **AMLA** will issue **guidelines** on the factors that obliged entities must consider when deciding the extent of their internal policies, procedures and controls, based on the nature of the business, including its risks, complexity, and the size of the obliged entity. In particular, the guidelines should clarify:

- The staffing of the compliance function;
- In which cases internal controls can be organised at the level of the commercial function, of the compliance function and of the audit function;
- When the independent audit function can be carried out by an external expert.

[32] With the SRR, Regulation (EU) 2023/1113, and any administrative acts issued by any supervisor.

What has changed?

Compared to the current EU AML/CFT framework, the SRR lays down more detailed rules on internal policies, procedures and controls. It introduces new requirements regarding internal policies and procedures on outsourcing and reliance on CDD performed by other obliged entities; verification of good repute of the obliged entities' agents and distributors; communication of internal AML/CFT policies, procedures and controls to obliged entities' agents and distributors, and to service providers involved in AML/CFT compliance; training of agents and distributors; etc.

The SRR also changes the process of approving AML/CFT policies, procedures and controls. The SRR mandates that internal policies be approved by the obliged entity's management body in its management function while internal procedures and controls should be approved at least by the compliance manager. The current EU AML/CFT regime requires senior management approval for all policies, procedures and controls.

Implications for intermediaries

Insurance and financial intermediaries will need to review carefully their existing internal AML/CFT policies and procedures against the more detailed requirements of the SRR. Credit intermediaries will need to adopt and put in place the necessary internal policies, procedures and controls to ensure compliance with the SRR requirements.

The exact requirements/ arrangements for the AML/CFT internal policies, procedures and controls, including the compliance function, will only be known when the AMLA publishes the guidelines on the extent of internal policies, procedures and controls.

Obligation to conduct a business-wide risk assessment

Obliged entities must conduct a business-wide risk assessment that is proportionate to the nature of the obliged entity's business, including its risks and complexity, and the size of the obliged entity.[33]

[33] Article 10(1), SRR.

The table below outlines the SRR requirements for the business-wide risk assessment.[34]

Category	Description
Purpose	▶ Identify and assess ML/TF risks to which an entity is exposed ▶ Identify and assess risks of non-implementation and evasion of targeted financial sanctions
Criteria/ Information sources	▶ Risk variables and risk factors set out in the SRR ▶ Union-level risk assessment findings ▶ National risk assessments conducted by the Member States ▶ Relevant publications by international standard setters, the Commission or the AMLA ▶ Information on AML/TF risks from competent authorities ▶ Information on customer base
Timing	▶ Before launching new products, services or business practices ▶ Before using new delivery channels and new or developing technologies for new or pre-existing products/services ▶ Before starting to provide an existing service or product to a new customer segment or in a new geographical area
Performance	▶ Compliance officer must be responsible for drawing up the business-wide risk assessment ▶ Management body (in its management function) must approve the business-wide risk assessment ▶ In case of two-tier management system (dual boards), the management board/body must communicate the approval to the supervisory board/body
Documentation	▶ Documented in writing ▶ Kept up-to-date ▶ Regularly reviewed, especially after significant internal or external events

[34] Article 10, SRR.

What has changed?

A high-level requirement to conduct business-wide risk assessments exists under the current EU AML/CFT framework.[35] However, the details of the requirement are currently scattered across several EBA Guidelines which are not legally binding and are subject to the so-called "comply or explain" approach. The SRR consolidates the current rules in a single legally binding provision.

The Regulation also clarifies and updates certain existing rules, including an express requirement to cover risks of non-implementation and evasion of targeted financial sanctions in business-wide risk assessments, and an express requirement to have business-wide risk assessments approved by the management body in its management function.

Implications for intermediaries

Insurance and financial intermediaries will be already familiar with the SRR rules on business-wide risk assessments. The SRR should not significantly change the way in which intermediaries conduct the assessments. However, intermediaries may have to conduct and update their business-wide risk assessments more frequently due to the SRR's extended list of instances in which such assessments should be performed.

Credit intermediaries will need to thoroughly prepare for conducting and regularly reviewing business-wide risk assessments.

Setting up compliance functions

Obliged entities are required to appoint a **compliance manager** and a **compliance officer.**[36]

- The **compliance manager** is a member of the management body of the obliged entity.
- The **compliance officer** is appointed by the management body of the obliged entity and has to be sufficiently high in the hierarchical structure of the entity.

[35] Article 8(1), AMLD5.
[36] Article 11, SRR.

The table below outlines the SRR requirements for compliance function.[37]

Role	Responsibilities
Compliance manager	► Ensuring compliance with the SRR, the Transfer of Funds Regulation and any administrative acts issued by any supervisor ► Ensuring internal policies, procedures and controls are consistent with the entity's risk exposure and are implemented ► Ensuring allocation of sufficient resources ► Receiving information on significant/material weaknesses in policies, procedures and controls ► Assisting and advising the management body ► Submitting annual report on the implementation of internal policies, procedures and controls to the management body
Compliance officer	► Responsible for policies, procedures and controls in day-to-day operation ► Drawing up business-wide risk assessment ► Implementing targeted financial sanctions ► Reporting suspicious transactions to the FIU ► Point of contact for competent authorities ► Drawing up annual report on the implementation of internal policies, procedures and controls

Proportionality

In line with the risk-based approach, obliged entities can have a single person performing the functions of the compliance manager and the compliance officer, or combine the compliance functions with other functions where the nature of the business (including its risks and complexity) and the size of the entity justify such arrangement.

[37] Article 11, SRR.

Resources for the compliance function

Obliged entities must provide the compliance function with adequate resources, including staff and technology, that are proportionate to the size, nature and risks of the obliged entity for the effective performance of its tasks.

Protection of compliance officer

The compliance officer can only be removed from their position with a prior notification to the management body in its management function and the removal must be notified to the supervisor. Obliged entities must take measures to ensure that the compliance officer is protected against retaliation, discrimination and any other unfair treatment. In addition, decisions of the compliance officer must not be undermined or unduly influenced by the commercial interests of the obliged entity.

Outsourcing of compliance function

The SRR does not prevent obliged entities from outsourcing the (majority of) tasks of the compliance officer.[38] The tasks of the compliance manager cannot be outsourced since the compliance manager must be a member of the management body of the obliged entity.

What has changed?

The current EU AML/CFT framework contains high-level provisions regarding the identification of the member of the management body responsible for AML/CFT and the appointment of the AML/CFT compliance officer.[39] However, the detailed rules on this matter are currently set out in non-legally binding EBA Guidelines.[40] The SRR transfers a number of the detailed provisions of the EBA Guidelines into a legally binding Regulation.

The SRR introduces new rules on the protection of the compliance officer. It aslo clarifies the division of responsibility for reporting to the management body on the implementation of internal policies, procedures and controls.

[38] The wording of Article 10(2), read together with Article 18(3)(a), of the SRR creates uncertainty whether the compliance officer's task of drawing up the business-wide risk assessment can be outsourced.
[39] Articles 8(4)(a) and 46(4) of the AMLD5.
[40] EBA Guidelines on the role, tasks and responsibilities AML/CFT compliance officers.

Implications for intermediaries

For insurance and financial intermediaries, the impact of the SRR requirements on compliance functions will largely depend on the size and the nature of the business of the intermediary. Smaller intermediaries and intermediaries engaged in non-complex business with low ML/TF risks may only need to clarify or assign additional tasks to members of their management bodies/staff. Larger intermediaries and intermediaries conducting complex business with higher ML/TF risks might have to make more extensive changes in their internal organisation to meet the SRR requirements.

In addition to the size and complexity of the business, the impact on financial intermediaries may also vary depending on whether a financial intermediary is an authorised investment firm or operates under the MiFID II opt-out regime. The latter financial intermediaries might have to make more significant adjustments to comply with the SRR requirements.

Credit intermediaries will need to make new internal governance arrangements in line with the SRR requirements on compliance functions.

The exact requirements/arrangements for the AML/CFT compliance function will only be known when the AMLA publishes the Guidelines on the extent of internal policies, procedures and controls.

Outsourcing

Obliged entities may outsource tasks related to the AML/CFT requirements of the SRR to third-party service providers.[41]

How to outsource AML/CFT tasks?

Obliged entities considering outsourcing should:

- Ensure that the service provider is sufficiently qualified and applies the policies, procedures and controls of the obliged entity;
- Conclude written agreements with service providers which set out the conditions for the performance of outsourced tasks;
- Notify the supervisor about the outsourcing arrangement before the service provider starts carrying out the outsourced task;

41 Article 18, SRR.

- Be able to demonstrate to the supervisor that the obliged entity understands the rationale of the measures undertaken by the service provider and that such measures mitigate the identified ML/TF risks;
- Ensure that the outsourcing arrangement does not materially impair the quality of the obliged entity's internal AML/CFT policies, procedures and controls;
- Only outsource to non-EU service providers if they are part of the same group as the obliged entity and additional SRR conditions are met.

Oversight of outsourced AML/CFT tasks

In the case of outsourcing, **obliged entities** remain **fully liable** for any action performed by the service provider related to the outsourced task. Obliged entities must regularly control that service providers effectively implement the obliged entity's AML/CFT policies and procedures when performing outsourced tasks. The frequency of the controls should correspond to the critical nature of the outsourced tasks.

Prohibited outsourcing

Certain tasks under the SRR **cannot** be outsourced, including:

- Proposal and approval of the business-wide risk assessment;[42]
- Approval of internal AML/CFT policies, procedures and controls;[43]
- Decision on the risk profile of a customer;
- Decision to enter into a business relationship or carry out an occasional transaction with a client;
- Reporting of suspicious activities to FIUs;[44]
- Approval of the criteria for the detection of suspicious or unusual transactions.

What has changed?

The current EU AML/CFT framework does not regulate the outsourcing of AML/CFT-related tasks, except for a high-level principle that, in the case of outsourcing, the obliged entity remains primarily responsible for complying with the AML/CFT requirements,[45] and the specific rules on outsourcing of operational functions of the AML/CFT compliance officer.[46]

The SRR sets out detailed new rules regarding outsourcing, including on conditions for outsourcing, requirements for service providers, notifications to supervisors, obliged entities'

[42] See Article 10(2), SRR.
[43] See Article 9, SRR.
[44] See Article 69, SRR.
[45] Recital 36, AMLD5.
[46] EBA Guidelines on the role, tasks and responsibilities AML/CFT compliance officers.

oversight of outsourcing arrangements, and restrictions on outsourcing to third-country service providers.

Implications for intermediaries

Insurance intermediaries are not subject to requirements on outsourcing under the Insurance Distribution Directive. Similarly, the Mortgage Credit Directive and the Directive on Consumer Credit Agreements do not impose any specific rules on outsourcing for credit intermediaries. Therefore, the new SRR rules on outsourcing will likely affect insurance and credit intermediaries more than the other financial institutions (for example, insurers), which already must comply with sector-specific rules on outsourcing.

Financial intermediaries authorised as MiFID II investment firms are already subject to the MiFID II rules on outsourcing. These financial intermediaries will likely have to make only limited changes to their existing outsourcing policies and procedures, and the existing outsourcing arrangements. The new SRR rules might have a greater impact on financial intermediaries that operate under the MiFID II opt-out regime depending on whether and to what extent the relevant national rules impose requirements on outsourcing for such financial intermediaries.

Intermediaries, which currently rely on third parties for compliance with the AML/CFT obligations, will need to review their outsourcing arrangements closely to ensure that the latter meet the conditions for outsourcing under the SRR. This includes at least the internal policies and procedures, the credentials of service providers and the content of written agreements with providers. Intermediaries will also have to notify the outsourcing arrangements to supervisors and secure their approval.

Staff of obliged entities

Obliged entities are required to ensure that their **staff involved in the implementation of AML/CFT measures** is aware of the applicable AML/CFT requirements and the obliged entity's business-wide risk assessment, internal policies, procedures and controls, including through specific ongoing training programmes.[47]

Obliged entities' **staff assigned with tasks related to the obliged entity's compliance with AML/CFT requirements**:

- Must undergo a proportionate assessment (the content of which must be approved by the compliance officer) of their skills, knowledge, expertise, good repute, honesty, and integrity;[48]

[47] Article 12, SRR.
[48] Article 13(1), SRR.

- Disclose any potential conflicts of interest with the obliged entity's (prospective) customers.[49]

The above awareness and fit & proper requirements also apply to agents and distributors of obliged entities.

Staff must have access to internal channels for the reporting of breaches of AML/CFT requirements and be protected from retaliation when doing so in accordance with the EU Whistleblowing Directive[50] [51].

What has changed?

The SRR expands the requirements in relation to awareness and training of staff members who are involved in the implementation of AML/CFT policies and procedures. The SRR also introduces express professional and integrity standards for staff members involved in AML/CFT compliance tasks and requires that these individuals undergo an assessment approved by the compliance officer. In addition, the more detailed awareness and integrity requirements apply to agents and distributors of obliged entities.

Implications for intermediaries

Insurance and financial intermediaries need to check whether any additional staff members and the intermediaries' agents/distributors might have to be assessed for their fitness and propriety. Insurance and financial Intermediaries should also review their existing conflicts-of-interest policies and training programmes to ensure that they properly reflect the SRR requirements.

Credit intermediaries will need to assess fitness and propriety of the relevant staff members and the intermediaries' agents/distributors, review their existing conflicts-of-interest policies and put in place or update training programmes in line with the SRR awareness requirements. Credit intermediaries might have to provide extensive additional training to their current staff or even hire new personnel with AML/CFT compliance experience.

[49] Article 13(2)-(3), SRR.
[50] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.
[51] Article 14, SRR.

Record retention[52]

Obliged entities must **retain certain documents and information**, including:

- Copies of documents and information obtained as part of CDD;
- Records of assessments undertaken, including the results, regardless of whether a suspicious transaction report was made;
- Supporting evidence and records of transactions, necessary to identify transactions;
- Copies of documents and information obtained in partnerships for information sharing and records of all instances of information sharing.

These documents, information and records **must not be redacted**.

Obliged entities may replace the retention of copies of the information with **references to such information** if they are able to provide the information immediately to competent authorities and ensure that the information is not modified or altered. Obliged entities are required to document this decision in their internal procedures.[53]

The information must be retained for a **period of five years** from the date of termination of the business relationship or the date of the occasional transaction. Personal data has to be deleted upon expiry of the five-year period.

What has changed?

The SRR broadens record retention obligations to include a wider variety of documents. It introduces the flexibility to retain references to such information instead of copies, on the condition that the information can be provided to competent authorities immediately and remains unaltered.

Implications for intermediaries

Insurance and financial intermediaries will have to review their record-keeping policies to ensure that they retain all documents and information required under the SRR. Credit intermediaries will have to implement specific record-keeping policies to comply with the requirements of the SRR.

[52] Article 77, SRR.
[53] Article 77(2), SRR.

Group-wide requirements

The SRR establishes specific compliance expectations for groups.[54]

Parent undertakings[55] have the following obligations:

- Ensure that the requirements on internal procedures, risk assessment and staff apply in all branches and subsidiaries:
  - Established in the Member States; and
  - Established outside the EU in the case of groups whose head office is located in the EU;
- Conduct a group-wide risk assessment that considers the business-wide risk assessments performed by branches and subsidiaries;
- Establish group-wide internal AML/CFT policies, procedures and controls;
- Put in place policies, procedures and controls on information sharing within the group for AML/CFT purposes, which:
  - Require obliged entities within the group to exchange relevant information when such sharing is relevant for CDD and ML/TF risk management;
  - Ensure that the exchanged information is subject to sufficient guarantees in terms of confidentiality, data protection and the use of information;
- Establish the **compliance function at the group level**. The group-level function should include a compliance manager and, where justified by the group's activities, a compliance officer;
- Require that non-EU branches and subsidiaries comply with the SRR requirements when the minimum AML/CFT requirements in a third country are less strict;
- If compliance with the SRR is not permitted under relevant third-country laws, take additional measures to ensure that non-EU branches and subsidiaries effectively handle the ML/TF risks, and inform the supervisors of their home Member State about such measures.[56]

By 10 July 2026, AMLA must develop draft regulatory technical standards that specify the minimum requirements for group-wide policies, procedures, and controls, including minimum standards for information sharing within the group and other group-wide requirements.

[54] Section 2 of Chapter II, SRR.
[55] As defined in Article 2(1)(42), SRR.
[56] Articles 16-17, SRR.

What has changed?

Group-wide AML/CFT requirements exist under the current EU AML/CFT framework but are in part set out in non-legally binding EBA Guidelines.[57] The SRR incorporates a number of provisions of the EBA Guidelines. The SRR also clarifies which entity is responsible for group-wide AML/CFT requirements and sets more detailed rules on group-wide employee awareness and outsourcing.

Implications for intermediaries

Parent undertakings of insurance/credit/financial intermediary groups will need to review the existing group-wide policies and procedures against the more detailed SRR requirements. The exact requirements/arrangements for group-wide AML/CFT policies, procedures and controls, including regarding the compliance function, will only be known when the AMLA publishes the regulatory technical standards on group-wide policies, procedures and controls.

Requirements relating to customers/business relationships

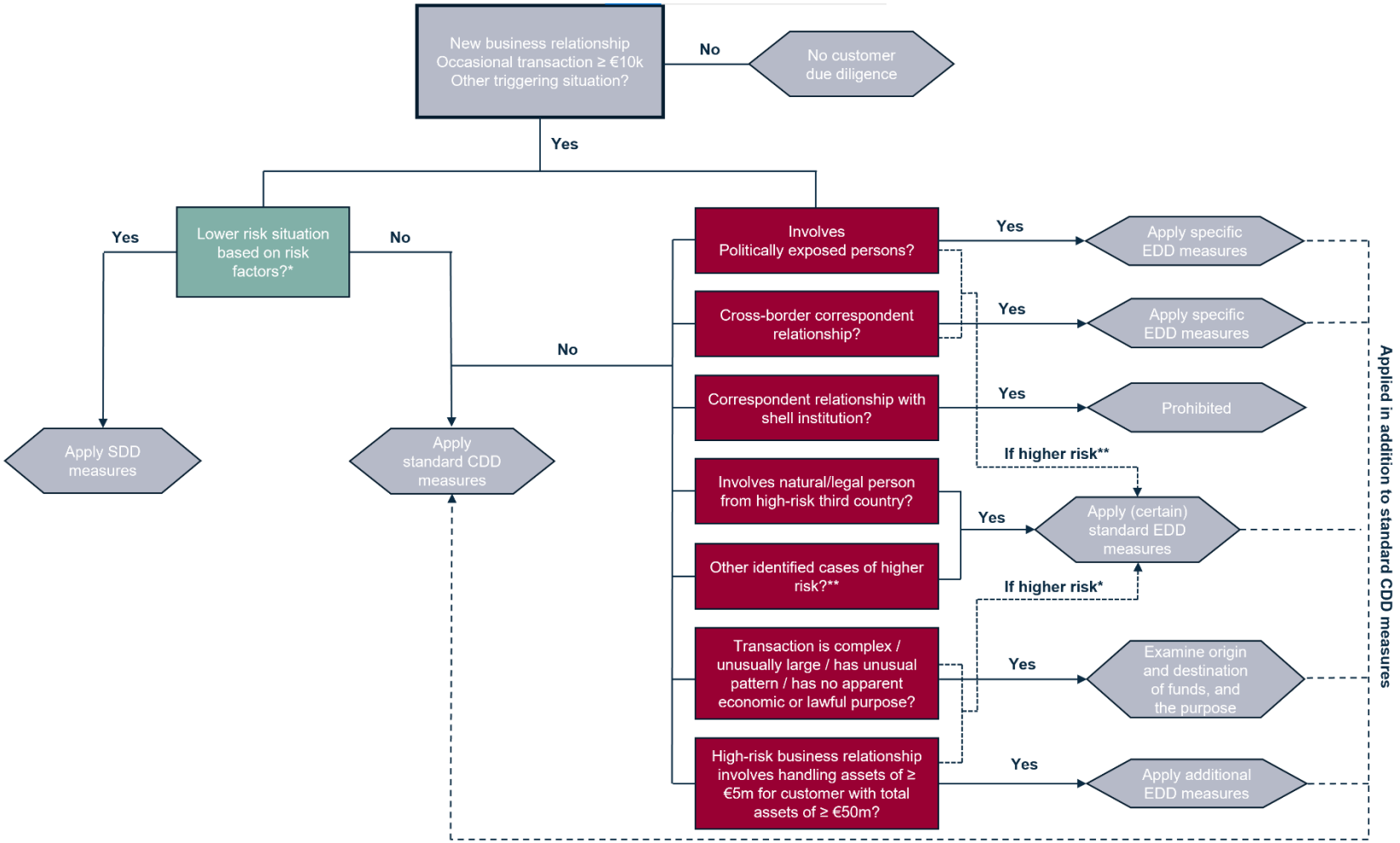
Customer due diligence (CDD)[58]

The SRR establishes the CDD requirements for obliged entities. The SRR further specifies the CDD measures already mandated by AMLD5, including adjusted thresholds (for example, transactions previously set at a minimum of €15,000 are now reduced to €10,000). Additionally, certain exemptions, previously allowed in the performance of CDD measures, have been eliminated from the AML/CFT framework.

The flowchart on the next page provides a highly simplified decision tree for the selection of appropriate CDD measures and is intended to facilitate the reading of the sections below.

[57] EBA Guidelines on the role, tasks and responsibilities AML/CFT compliance officers.
[58] Chapter III, SRR.

Flowchart on the choice of appropriate CDD measures



* The degree of ML/TF risk should be assessed on the basis of the lower/higher risk factors set out in Annexes II and III to the SRR.

** The ML/TF risks posed by a business relationship or occasional transaction should be determined on the basis of: the higher risk factors in Annex III to the SRR; the AMLA Guidelines on money laundering and terrorist financing risks, trends and methods; any other indicators of higher risk, such as notifications issued by the FIU and findings of the business-wide risk assessment.

When to perform CDD measures?

Intermediaries, as obliged entities, **must apply CDD measures** in the following circumstances:[59]

- When establishing a business relationship;
- If an occasional transaction exceeds €10,000 (or a lower threshold chosen by the relevant Member States);
- When participating in the creation of a legal entity or the setting up of a legal arrangement;
- If there is a suspicion of ML/TF;
- If there are doubts about the veracity/adequacy of previously obtained customer information;
- If there are doubts that the person they interact with is the customer or the person authorised to act on their behalf;
- When initiating or executing a transaction of at least €1,000 (through single operation or linked transactions) that constitutes a transfer of funds as defined in Article 3(9) of the Transfers of Funds Regulation;
- If an occasional transaction in cash exceeds €3,000 (at least identifying the customer and verifying their identity).

The **verification of the identity of the customer and the beneficial owner must be performed <u>before</u>** the establishment of a business relationship or the carrying out of an occasional transaction, except when lower risk justifies a postponement. An exception to this rule permits completing the identity verification **<u>during</u>** the establishment of the business relationship when it is necessary to avoid disrupting the usual course of business and there is a **low risk of ML/TF**.[60]

What has changed?

The SRR introduces several new instances in which CDD measures should be applied, including when: participating in the creation of a legal entity; carrying out an occasional transaction in cash that exceeds €3,000 (at least identifying the customer and verifying their identity); and there are doubts about the veracity/adequacy of previously obtained customer information.

[59] Article 19, SRR.
[60] Article 23, SRR.

How to perform CDD measures?

Intermediaries, as obliged entities, are **required to carry out the following CDD measures**:[61]

- **Identify the customer** and verify their identity. This can be done through the submission of identity documents and, where relevant, through the use of electronic identification means;[62]
- **Identify the beneficial owner** and take reasonable measures to verify their identity;[63]
- Assess and understand the **purpose and intended nature** of the business relationship or the occasional transactions. This can include obtaining information on the purpose and economic rationale, the estimated amount, as well as the source and destination of funds.[64]
- Verify whether the customer or the beneficial owner are subject to **targeted financial sanctions**;
- Assess and obtain information on the **nature of the customer's business**;
- Conduct **ongoing monitoring** of the business relationship. This includes scrutiny of the transactions undertaken to ensure that the transactions are consistent with the customer's business activity and risk profile;[65]
- Determine whether the customer or the beneficial owner is a "**politically exposed person**", or a family member or a person known to be a close associate of a politically exposed person;
- Identify and verify the identity of **natural persons benefiting from a transaction/activity** where it is conducted on behalf or for the benefit of a natural person other than the customer;
- Confirm the authorisation of any **person claiming to act on behalf of the customer**, and identify and verify their identity.

In line with the risk-based approach of the AML/CFT framework, obliged entities must determine the extent of the CDD measures based on an **individual analysis of the ML/TF risks associated with the specific customer**.

[61] Article 20, SRR.
[62] See Articles 22-23, SRR.
[63] Ibid.
[64] See Article 25, SRR.
[65] See Article 26, SRR.

What has changed?

The SRR adds new CDD measures, such as identifying and verifying the identity of natural persons - other than the customer - benefiting from a transaction/activity. The Regulation incorporates several CDD measures which are currently set out in non-legally binding EBA Guideline[66] (assessing the nature of the customer's business; verifying whether the customer or the beneficial owners are subject to targeted financial sanctions).

The SRR also sets out more detailed rules on identifying and verifying the identity of customers and beneficial owners, identifying the purpose and intended nature of a business relationship/occasional transaction, and ongoing monitoring requirements.

What happens when the obliged entity is unable to comply with CDD requirements?

If an obliged entity is unable to comply with CDD requirements, it must:[67]

- Refrain from entering into a business relationship;
- Terminate an existing business relationship:
  - In the case of life insurance, when necessary and as an alternative to terminating the contract, insurers and insurance intermediaries shall refrain from performing transactions for the customer (including pay-outs to beneficiaries) until CDD measures are complied with;
- Refrain from carrying out an occasional transaction;
- Consider filing a suspicious transaction report to the FIU.

In addition, when no natural person can be identified as a beneficial owner or doubts remain as to the identity of the beneficial owner, obliged entities **must record these findings** and **identify all the natural persons holding the positions of senior managing officials** in the corporate or legal entity and verify their identities.[68]

What has changed?

The general consequences of the inability to apply CDD measures remain broadly the same as under the current EU AML/CFT framework. However, the SRR introduces a specific rule for life insurance.

[66] EBA Guidelines on ML/TF risk factors and EBA Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures.
[67] Article 21, SRR.
[68] Article 22(2), SRR.

Enhanced due diligence (EDD)[69]

Under certain circumstances, obliged entities are expected to apply EDD measures.

When to perform EDD measures?

Obliged entities must apply EDD measures in the case of:

- Business relationships and transactions involving **natural or legal persons located in third countries presenting increased ML/TF risks;**[70]
- **Cross-border correspondent relationships** and **correspondent relationships with shell institutions;**[71]
- Transactions with **self-hosted wallets**;[72]
- **Politically exposed persons,** including their **family members and close associates;**[73]
- Any other cases identified as **higher risk** based on the business-wide risk assessment, the risk variables and risk factors, or any other indicators, such as notifications from the FIU.

How to perform EDD measures?

As under the AMLD5, the SRR requires obliged entities to examine the **source and destination of funds**, as well as the **purpose of all transactions** that fulfil **at least one** of the following conditions:

- The transaction is complex;
- The transaction is unusually large;
- The transactions are conducted in an unusual pattern;
- The transactions do not have an apparent economic or lawful purpose.[74]

The SRR specifies that, in **higher-risk situations**, obliged entities must apply EDD measures which are **proportionate** to the identified higher risks and **may** include:[75]

- Obtaining **additional information** on the:
  - Customer and the beneficial owner(s);
  - Intended nature of the business relationship;
  - Source of funds and wealth of the customer and beneficial owner(s);

[69] Section 4, Chapter III, SRR.
[70] Articles 29-31, SRR.
[71] Specific EDD measures are set out in Articles 36-39, SRR.
[72] Specific EDD measures are set out in Article 40, SRR.
[73] Specific EDD measures are set out in Articles 42-46, SRR.
[74] Article 34(2), SRR.
[75] Article 34(4), SRR.

- The reasons for the intended or performed transactions and their consistency with the business relationship;

- Obtaining the **approval of senior management** for establishing or continuing the business relationship;
- Conducting **enhanced monitoring** of the business relationship by:
  - Increasing the number and timing of controls;
  - Selecting patterns of transactions that need further examination;
- **Requiring the first payment** to be carried out through an account held in the customer's name at a credit institution, which adheres to the CDD standards that are no less stringent than those specified by the SRR.

The SRR contains specific EDD measures to be applied when a higher-risk business relationship **involves the handling of assets of at least €5 million** through personalised services for a customer holding total assets of at least €50 million.[76]

What has changed?

Under the current EU AML/CFT framework, the list of possible EDD measures for cases of higher risk is set out in non-legally binding EBA Guidelines[77]. The SRR integrates the list of possible measures in a legally-binding Regulation. The SRR also adds a new EDD requirement for higher-risk business relationships which involve the handling of assets of at least €5 million.

Specific enhanced due diligence measures for politically exposed persons

The SRR sets out specific EDD measures which must be applied to politically exposed persons, including their family members and close associates. Same as under the current EU AML/CFT regime, Member States also have to draw up and maintain lists of "prominent public functions" at the national level.[78]

When a politically exposed person is involved, obliged entities must apply the following measures **in addition to the standard CDD measures**[79]:

- Obtain senior management approval for carrying out occasional transactions or for establishing or continuing a business relationship;
- Take adequate measures to establish the source of wealth and funds involved;
- Conduct enhanced ongoing monitoring of the business relationship.

In the case of **life or other investment-related insurance policies**, obliged entities must take reasonable measures to determine if the beneficiary or beneficial owner of the beneficiary is a politically exposed person. The assessment must be conducted **no later than at the time of pay-**

[76] Article 34(5), SRR.
[77] EBA Guidelines on ML/TF risk factors.
[78] Article 43, SRR.
[79] Article 42, SRR.

out under or assignment of the policy. If that is the case, obliged entities must apply the following **measures in addition to the standard CDD measures**[80]:

- Inform senior management before pay-out;
- Conduct enhanced scrutiny of the entire business relationship.

Simplified due diligence (SDD)[81]

Obliged entities can apply SDD measures when the risk factors indicate a low degree of risk in the business relationship or transaction.

SDD measures **may** include the following:[82]

- Verifying the identity of the customer or beneficial owner **after the establishment of the business relationship**, but, in any case, no later than 60 days after the establishment;
- Reducing the **frequency of customer identification** updates;
- Reducing the **amount of information collected** to identify the purpose and intended nature of the business relationship or transaction, or inferring it from the type of transactions or business relationship established;
- Reducing the **frequency or degree of scrutiny** of transactions;
- Applying any other measure identified by AMLA through regulatory technical standards.

Obliged entities have to check on a regular basis that the conditions for the application of SDD measures are still met. In addition, they should **refrain from applying SDD measures** in the following situations:[83]

- There are doubts about information veracity/accuracy;
- Factors indicating lower risk are no longer present;
- The monitoring of customer transactions and collected information suggest a higher risk scenario;
- There is suspicion of ML/TF;
- There is suspicion that the customer or the person acting on their behalf is attempting to circumvent or evade targeted financial sanctions.

By 10 July 2026, AMLA is required to develop draft regulatory technical standards which further specify the SDD measures, including measures for specific categories of obliged entities and products/services.[84]

[80] Article 44, SRR.
[81] Section 3, Chapter III, SRR.
[82] Article 33, SRR.
[83] Article 33(5), SRR.
[84] Article 28(1)(b), SRR.

What has changed?

AMLD4[85] introduced the concept of simplified due diligence (SDD). However, AMLD5 did not further specify the application of these measures and the current detailed rules on SDD are set out in non-legally binding EBA Guidelines[86]. The SRR addresses this gap by fully harmonising and clarifying the content and the application of the SDD measures.

The SRR list of SDD measures is broadly in line with the current EBA Guidelines. In contrast, the SRR sets out a more detailed list of situations in which obliged entities should refrain from applying SDD measures.

Specific CDD measures for life and other investment-related insurance[87]

Obliged entities must take the following **additional CDD measures on the beneficiaries** of life insurance and other investment-related insurance policies as soon as the beneficiaries are identified or designated:

- If the beneficiaries are identified as specifically named persons or legal arrangements, **recording the name of the person or arrangement**;
- If the beneficiaries are designated by characteristics or class, **obtaining sufficient information concerning the beneficiaries** so the obliged entity is able to establish the identity of the beneficiary at the time of pay-out.

Reporting suspicious transactions

Same as under the current framework, obliged entities must report to and cooperate with Financial Intelligence Units (FIUs) **when they have knowledge, suspicion, or reasonable grounds to suspect that funds or activities are proceeds of criminal activities or relate to TF**.[88] The SRR set out clearer rules on how suspicious transactions are to be identified.[89]

Obliged entities must provide FIUs with any requested information. As a general rule, obliged entities must respond to information requests from the FIUs **within 5 working days**. In justified and urgent cases, FIUs may shorten this deadline, including to less than 24 hours.

The **compliance officer** of each obliged entity is responsible for transmitting information on suspicious transactions to the FIU of the Member State in which the obliged entity is established.[90]

---

[85] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.
[86] EBA Guidelines on ML/TF risk factors.
[87] Article 47, SRR.
[88] Article 69(1), SRR.
[89] Article 69(2), SRR.
[90] Article 69(6), SRR.

By 10 July 2027, AMLA will issue guidelines on indicators of suspicious activity/behaviour.

Transaction restrictions

Obliged entities must **refrain from carrying out transactions** they suspect to be related to criminal activity or TF until they have submitted a report and complied with any instructions from the FIU. If it is not feasible to refrain from executing a transaction, obliged entities must **notify the FIU immediately after the transaction is completed**.[91]

Prohibition of disclosure

Obliged entities **may not disclose to the relevant customer** that transactions or activities are being assessed, that information is being, will be or has been transmitted to a FIU, or that an analysis related to ML/TF is being or may be conducted. Some derogations from the prohibition are available, including disclosure to competent authorities and to entities within the same group.[92]

What has changed?

The SRR introduces more comprehensive requirements for reporting suspicious transactions, including a requirement to report suspicions arising from inability to conduct CDD and more detailed rules on identifying suspicious transactions/activities. The SRR also contains express deadlines for reporting a suspicious transaction/activity to FIUs and responding to FIUs' requests. Obliged entities will be also required to report using a common template developed by the AMLA.

Implications for intermediaries

Insurance and financial intermediaries will need to ensure that their officers and employees are aware of the updated rules on suspicious transaction reporting, including the more detailed indicators of suspicious activity/behaviour. Intermediaries should also integrate the express deadlines for communicating with the FIUs into their internal policies and procedures. Credit intermediaries will need to make internal arrangements to comply with the SRR's suspicious transaction reporting requirements and ensure that their officers and employees understand their roles in relation to these requirements.

[91] Article 71, SRR
[92] Article 73, SRR.

BENEFICIAL OWNERSHIP TRANSPARENCY

CDD and Reporting of Beneficial Ownership

The SRR provisions on beneficial ownership information build on the current AML/CFT framework.

Beneficial owners of legal entities are natural persons who either:

- Have a direct or indirect **ownership interest** in the corporate entity; or
- **Control** the corporate/other legal entity directly or indirectly through ownership interest or other means.[93]

The SRR defines an **ownership interest** as the **direct or indirect ownership of 25% or more of the shares or voting rights** or other ownership interest in the corporate entity.[94] This is in line with the current AMLD5 threshold.

However, should Member States recognise particular risks linked to certain legal entities, they are required to inform the Commission, which may then determine a lower threshold to be appropriate. The Commission may set the ownership interest **threshold at a maximum of 15%.**

Legal entities (and trustees of express trusts, persons holding similar positions in similar legal arrangements) must maintain **beneficial ownership information that is adequate, accurate and up-to-date.** The SRR also sets out in detail the content of the beneficial ownership information.[95] These obligations, currently part of the AMLD5, have been expanded to encompass various legal arrangements.

Legal entities must **provide beneficial ownership information to obliged entities for CDD purposes** and report beneficial ownership information to **central beneficial ownership registers** of the Member State where the legal entity is created.[96]

The **obligation to disclose beneficial ownership information** applies to non-EU legal entities and arrangements when they:

- Enter into business relationships with obliged entities in the EU;
- Acquire real estate in the EU;
- Acquire certain high-value goods in the EU;
- Are awarded public procurement contracts by a contracting authority in the EU.[97]

[93] Article 51, SRR.
[94] Article 52, SRR.
[95] Article 62, SRR.
[96] Article 63, SRR.
[97] Article 67, SRR.

Obliged entities must **report to the central registers any discrepancies** they find between the information available in the central beneficial ownership registers and the information that obliged entities collect in the course of CDD.[98]

Central beneficial ownership registers[99]

The AMLD6 requires Member States to establish **central registers for beneficial ownership information** reported under the SRR. Member States must also designate an entity in charge of the register and ensure that it can request information from legal entities, necessary to identify and verify the identities of beneficial owners.

The entity in charge of the central register:

- Has to keep the information accurate and up-to-date and is empowered to carry out checks, such as on-site inspections of legal entities, to verify the identity of beneficial owners;
- Must be able to withhold or refuse to issue a certificate of proof of registration when there are inconsistencies or errors in the information reported;
- Can impose sanctions for failure to comply with reporting requirements.

Central registers have to be interconnected through a **European Central Platform.**[100]

Who can access beneficial ownership information?[101]

The following entities should always have direct access to beneficial ownership information contained in the central beneficial ownership registers:

- Competent authorities;
- Other relevant national authorities;
- AMLA;
- Other relevant European authorities (OLAF, EPPO, Europol, Eurojust);
- **Obliged entities when applying CDD measures**.

Access for persons with legitimate interest[102]

Persons who do not fit in the above categories, but can demonstrate a **legitimate interest**, should be granted access to certain information contained in the beneficial ownership registers.[103]

---

[98] Article 24, SRR.
[99] Article 10, AMLD6.
[100] Article 10(19), AMLD6. The European Central platform was established by Article 22(1) of Directive (EU) 2017/1132.
[101] Article 11, AMLD6.
[102] Article 12, AMLD6.
[103] Specifically, the information includes: (i) the name of the beneficial owner; (ii) the month and year of birth of the beneficial owner; (iii) the country of residence and nationality or nationalities of the beneficial owner; (iv) for beneficial owners of legal entities, the nature and extent of the beneficial interest held; (v) for beneficial owners of express trusts or similar legal arrangements, the nature of the beneficial interest (Article 12(1), AMLD6).

Certain persons will always be considered to have a legitimate interest, such as journalists, civil society organisations (connected with AML/CFT activities), natural and legal persons likely to enter into business with a legal entity, etc. Access to beneficial ownership information should also be granted to any other person who can show a legitimate interest.

What has changed?

The SRR and the AMLD6 significantly elaborate and update the rules on beneficial ownership information and transparency. The SRR clarifies the thresholds and criteria of beneficial ownership of legal entities through ownership interest and control. It also lays down detailed rules on the identification of beneficial owners of express/discretionary trusts, other similar legal arrangements and collective investment undertakings.

The SRR further details the beneficial ownership information that legal entities/legal arrangements must hold and lays down new obligations of non-EU legal entities/legal arrangements in relation to beneficial ownership information.

Meantime, the AMLD6 sets out a more detailed list of authorities which should always have access to beneficial ownership information contained in the central beneficial ownership registers and specific access rules for persons with legitimate interest, including a detailed list of persons who are deemed to have legitimate interest, and the procedure to confirm legitimate interest.

Implications for intermediaries

Although the SRR and the AMLD6 significantly modify the EU rules on beneficial ownership transparency, the changes should have limited operational implications for insurance and financial intermediaries. However, intermediaries will need to keep in mind the new express obligation in the SRR to report discrepancies in beneficial ownership information to central beneficial ownership registers.

Credit intermediaries will need to adjust to the beneficial ownership transparency requirements of the SRR. In particular, they will need to start collecting beneficial ownership information as part of CDD and report to the central registers any discrepancies between the collected information and the information available on the registers.

OTHER RELEVANT PROVISIONS

Information sharing[104]

Obliged entities may form and participate in partnerships for information sharing. These partnerships facilitate the exchange of information that is strictly necessary for fulfilling the CDD requirements and the obligations related to reporting suspicious transactions.

[104] Article 75, SRR.

How to participate in information sharing partnerships?

Obliged entities intending to join such partnerships must:

- Notify their respective supervisors of their intention to participate;
- Ensure that the exchange of information is limited to the specific categories outlined in the SRR, which include details regarding the customer's identity, the purpose and nature of a business relationship/transaction, customer transactions, risk factors, and suspicions.

The sharing of information can be carried out **only in relation to certain customers**:

- Their behaviour or transaction activities are associated with higher ML/TF risks, as identified under EU-level and national risk assessments;
- Customers are based/established in non-EU countries, which have been identified as high-risk third countries, countries with compliance weaknesses in their national AML/CFT regimes, or countries posing a specific and serious threat to the EU's financial system;
- A customer is party to a cross-border correspondent relationship;
- Politically exposed persons, including family members and close associates;
- Customers for whom the obliged entities need to collect additional information in order to determine whether they are associated with a higher level of ML/TF risk.

Several **conditions** apply to the sharing of information within the context of a partnership for information sharing, including:

- Recording all instances of information sharing;
- Duty to conduct own assessment of transactions and avoid relying solely on the shared information;
- Implementing appropriate technical and organisational measures.

Obliged entities participating in partnerships for information sharing must define **policies and procedures for the sharing of information** in their internal policies and procedures.

Implications for intermediaries

Partnerships for information sharing is a new mechanism introduced by the SRR. They might be a useful tool for all in-scope intermediaries and facilitate the information-gathering activities for compliance with the AML/CFT requirements.

Data protection[105]

The SRR sets out rules on processing of personal data to ensure the new framework is compliant with the GDPR.[106]

If it is **strictly necessary for the prevention of ML/TF**, obliged entities may process:

- Special categories of personal data specified in Article 9(1) of the GDPR;[107]
- Personal data concerning criminal convictions and offenses, as referred to in Article 10 of the GDPR.

Obliged entities may adopt decisions resulting from **automated processes**, including: profiling, as defined in Article 4(4) of the GDPR, or from processes involving AI systems, as specified in Article 3(1) of the AI Act[108], under certain conditions:

- Limiting the data processed by automated processes to data obtained for CDD purposes;
- Ensuring meaningful human intervention in decision-making; and
- Allowing the customer to obtain an explanation of the decision and challenge it, except in relation to suspicious transaction reports.

What to keep in mind when processing personal data?

Obliged entities must observe the SRR safeguards when processing personal data:

- Inform their customers or prospective customers;
- Ensure the data is accurate and up-to-date, avoid decisions that could lead to biased and discriminatory outcomes, and adopt high-level security measures;
- For personal data relating to criminal convictions and offenses, ensure that the data relates to ML/FT and have procedures in place that allow distinguishing between allegations, investigations, proceedings, and convictions.

Restrictions

Personal data must only be processed for the purpose of preventing ML/TF and must not be processed further in a manner that is not compatible with these purposes. The processing of personal data for commercial purposes is prohibited.

---

[105] Article 76, SRR.

[106] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[107] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[108] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

What has changed?

The SRR sets out more detailed rules on the processing of personal data, including conditions for the processing of personal data covered by Articles 9 and 10 of the GDPR, and the use of automated processes and AI systems in AML/CFT compliance activities.

Anonymous accounts and large cash payments

In light of the risks associated with ML/TF that stem from **anonymous accounts**, the SRR further clarifies the restrictions on their use.[109] The SRR also establishes a new EU-wide limit to **large cash payments** for persons trading in goods or providing services. The limit is fixed at **€10,000**, with the possibility for Member States to adopt lower limits, following a consultation with the European Central Bank.[110]

SUPERVISION AND SANCTIONS

Supervision

Supervisors must adopt a **risk-based approach** to supervising the obliged entities' compliance with AML/CFT requirements.[111]

Financial intelligence Units (FIUs)

FIUs are central national units established by Member States. Their primary responsibility is to **receive, analyse, and process reports of suspicious activities and other relevant information related to ML/TF.** [112] FIUs are expected to function autonomously and independently, equipped with adequate resources to perform their duties effectively.

FIUs must have access to the information required to fulfil their tasks and may solicit data from obliged entities.[113] Additionally, FIUs should provide relevant information to supervisors.[114] FIUs may take **urgent actions**, such as suspending or withholding consent to a transaction that presents suspicions of ML/TF.[115]

In the case of cross-border ML/TF threats, FIUs are strongly encouraged to cooperate among themselves.

[109] Article 79, SRR.
[110] Article 80, SRR.
[111] Article 40, AMLD6.
[112] Article 19, AMLD6.
[113] Article 21, AMLD6
[114] Article 23, AMLD6.
[115] Article 24, AMLD6.

National supervisors

Member States must designate a national supervisor to monitor the implementation of the AML/CFT framework.[116]

The tasks of national supervisors include:

- Distributing pertinent information to obliged entities;
- Verifying the adequacy and implementation of internal policies, controls and procedures;
- Monitoring and evaluating ML/TF risks;
- Conducting off-site investigations and on-site inspections, and additional investigations as required;
- Taking appropriate supervisory measures to rectify violations;
- Enforcing administrative measures and imposing pecuniary sanctions.

Supervisors of financial institutions, including insurance/credit/financial intermediaries, have at least the following powers in performing the abovementioned tasks[117]:

- Compelling obliged entities to submit information;
- Examining the books and records of the obliged entity and taking copies or extracts from such books and records;
- Obtaining access to any software, databases, IT tools, or other electronic means of recording information used by the obliged entity;
- Obtaining written or oral information from any person responsible for AML/CFT internal policies, procedures and controls, and from service providers under outsourcing arrangements;
- Interviewing any other person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation.

The new AML/CFT framework also sets out detailed rules on supervision of obliged entities carrying out cross-border activities[118], cooperation in the context of group supervision[119] and AML/CFT supervisory colleges in the financial sector.[120]

AMLA

AMLA is the new Frankfurt-based EU agency which is tasked with preventing the use of the EU's financial system for the purpose of ML/TF.[121] AMLA's **objectives** include:

- Contributing to identifying and assessing risks and threats across the EU;

[116] Article 37, AMLD6.
[117] Article 37(6)-(7), AMLD6.
[118] Article 47, AMLD6.
[119] Article 46, AMLD6.
[120] Article 49, AMLD6.
[121] For further reference, see the AMLA Regulation.

- Ensuring proper supervision in the area of AML/CFT within the internal market;
- Contributing to supervisory convergence in the area of AML/CFT and to the harmonisation of practices in the detection of suspicious transactions/activities; and
- Supporting and coordinating the exchange of information between FIUs and other competent authorities.[122]

AMLA has extensive tasks with respect to ML/TF risks facing the internal market, "selected obliged entities" (please see immediately below), financial and non-financial supervisors, and FIUs.[123]

AMLA will **directly supervise selected obliged entities in the financial sector**. In order to identify the selected obliged entities for direct supervision, AMLA will periodically assess the inherent and residual risk profiles of financial institutions and their groups that operate on a cross-border basis in at least six Member States. By 1 January 2026, AMLA has to develop separate methodologies for classifying inherent and residual risk profiles of different types of financial institutions, including life insurance intermediaries.[124]

Financial institutions and groups with a high residual risk profile will qualify as **selected obliged entities**. AMLA must start the first selection process of selected obliged entities by 1 July 2027 and has to conclude it within six months from the start date.[125] National financial supervisors may also request AMLA to assume direct supervision over non-selected obliged entities.[126]

AMLA will have **direct supervisory powers** over the selected obliged entities which are equivalent to the supervisory powers of national supervisors, including[127]:

- The right to request information from any selected obliged entity, their employees, affiliated legal persons, and third parties to whom they have outsourced functions;
- The power to conduct necessary investigations and on-site inspections of selected obliged entities;
- The right to apply dissuasive administrative measures to ensure compliance with AML/CFT legislation; and
- The power to impose pecuniary sanctions and periodic penalty payments on selected obliged entities for breaches or non-compliance.

In addition, AMLA will have **indirect supervisory powers** over non-selected obliged entities in the financial sector, including[128]:

- Periodic assessments of the activities of national financial supervisors;
- Coordinating and facilitating the work of the AML/CFT supervisory colleges in the financial sector;

[122] Article 1, AMLA Regulation.
[123] Article 5, AMLA Regulation.
[124] Article 12, AMLA Regulation.
[125] Article 13, AMLA Regulation.
[126] Article 14, AMLA Regulation.
[127] Articles 17-23, AMLA Regulation.
[128] Articles 30-34, AMLA Regulation.

- Requesting national financial supervisors to act in exceptional circumstances following indications of serious, repeated or systematic breaches;
- Settling disagreements between financial supervisors in cross-border situations;
- Investigating potential breaches of the applicable EU law by financial supervisors.

To fund its operations, the AMLA will collect **annual supervisory fees** from selected and non-selected obliged entities in the financial sector. The fees will be determined by the Commission through a delegated act, taking into consideration factors such as total annual turnover and risk profiles.[129]

What has changed?

The AML/CFT legislative package significantly overhauls the system of AML/CFT supervision in the EU. The key changes include the more detailed and extensive powers of FIUs and national (financial) supervisors; new rules on the supervision of cross-border activities, group supervision and AML/CFT supervisory colleges in the financial sector; direct and indirect supervision carried out by the AMLA.

Implications for intermediaries

The impact of the overhaul of the AML/CFT supervisory system on insurance and financial intermediaries depends on the size and nature of the business of a particular intermediary. Micro and small insurance intermediaries, which conduct no or limited cross-border activities, will likely not experience a significant change in the supervision of their compliance with the AML/CFT requirements. Meantime, large intermediaries with significant cross-border business and intermediary groups will have to adapt to the new elements of the AML/CFT supervisory system, ranging from the enhanced supervision of cross-border activities and establishment of AML/CFT supervisory colleges to, potentially, direct AML/CFT supervision by the AMLA.

Credit intermediaries will need to prepare for the supervision of their compliance with the AML/CFT requirements.

[129] Article 77, AMLA Regulation.

Sanctions

Breaches of the SRR and the Transfer of Funds Regulation

Member States must:

- Ensure that obliged entities can be held liable for any breach of the SRR and the Transfer of Funds Regulation;
- Establish pecuniary sanctions and administrative measures with respect to these breaches.[130]

AMLD6 also specifies thresholds for **pecuniary sanctions** and outlines the **administrative measures** that supervisors in Member States can apply to obliged entities.[131]

Breaches of beneficial ownership transparency requirements

Member States are required to set penalties for violations of beneficial ownership transparency requirements. Member States had to inform the Commission about their penalty rules and legal basis by 10 January 2025.[132]

REVIEW OF THE NEW AML/CFT FRAMEWORK

By 10 July 2032, and every 3 years thereafter, the Commission is mandated to evaluate the implementation of the SRR and the AMLD6, and to present a report to the European Parliament and the Council.[133]

The Commission must also draw up a report 6 years after the date of application of the SRR to assess the need and proportionality of:

- Lowering the 25% threshold for the identification of beneficial ownership;
- Extending the scope of high-value goods referred in Annex IV of the SRR;
- Adjusting the limit for large cash payments.[134]

[130] Article 53, AMLD6.
[131] Articles 55-56. AMLD6.
[132] Article 58, SRR.
[133] Article 87, SRR; Article 76, AMLD6.
[134] Article 88, SRR.

ANNEX I – Selected acronyms and definitions in the AML/CFT comprehensive framework

AML	Anti-money laundering
AMLA	Anti-Money Laundering and Countering the Financing of Terrorism Authority
AML/CFT supervisory college	A permanent structure for cooperation and information sharing for the purposes of supervising a group or entity that operates in a host Member State or third country[135]
Business relationship	A business, professional or commercial relationship connected with the professional activities of an obliged entity, which is set up between an obliged entity and a customer, including in the absence of a written contract, and which is expected to have, at the time when the contact is established, or which subsequently acquires, an element of repetition or duration[136]
Beneficial owner	Any natural person who ultimately owns or controls a legal entity, an express trust or similar legal arrangement[137]
Central beneficial ownership registers	A centralised database maintained by Member States, containing beneficial ownership information, statements and information on nominee arrangements of legal entities and trustees of express trusts or similar legal arrangements [138]
CFT	Countering the Financing of Terrorism
EPPO	European Public Prosecutor's Office
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation

[135] As defined in Article 2(8), AMLD6
[136] As defined in Article 2(19, SRR.
[137] As defined in Article 2(28), SRR.
[138] For further reference, see Article 10, AMLD6.

Group	A group of undertakings which consists of a parent undertaking, its subsidiaries, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU[140]
ML/TF	Money laundering and terrorist financing
OLAF	European Anti-Fraud Office
FIUs	Financial Intelligence Units are central national units responsible for receiving and analysing reports of suspicious activities and any other relevant information relating to AML/CFT
FIU.net	A system for the exchange of information between FIUs of Member States[139]

[139] See Article 30, AMLD6.
[140] As defined in Article 2(41), SRR.

ANNEX II – Member States which currently extend AML/CFT rules to non-life insurance intermediaries[141]

Member State	Extension to non-life/general insurance
Austria	✗
Belgium	✗
Bulgaria	✗
Croatia	✗
Cyprus	✗
Czech Republic	✗
Denmark	✗
Estonia	✗
Finland	✓
France	✓
Germany	✓
Greece	✗
Hungary	✗
Ireland	✗
Italy	✗
Latvia	✗
Lithuania	✗
Luxembourg	✗
Malta	✓
Netherlands	✗
Poland	✗
Portugal	✗
Romania	✓
Slovakia	✗
Slovenia	✗
Spain	✗
Sweden	✗

[141] The list is based on the information published online by national authorities of each Member State.

ANNEX III – List of Level 2 and 3 measures under the SRR and the AMLD6

Level 2 measures of the SRR

Type	Measure	Deadline
Delegated act	Regulatory Technical Standards (RTS) on group-wide policies, procedures, and controls, including information sharing within the group, criteria for identifying the parent undertaking, and conditions for applying group-wide requirements to entities with common ownership, management, or compliance control[142]	By 10 July 2026, AMLA must develop and submit draft RTS to the Commission for adoption
Delegated act	RTS on additional measures for branches and subsidiaries in third countries where local laws do not permit compliance with AML/CFT requirements, including minimum actions and additional supervisory actions[143]	
Delegated act	RTS on customer due diligence measures, specifying obliged entities, sectors, or transactions with higher ML/TF risk, related occasional transaction values, and criteria for identifying occasional and linked transactions[144]	
Delegated act	RTS on information necessary for customer due diligence, specifying requirements for standard, simplified, and enhanced due diligence, simplified due diligence measures[145]	
Delegated act(s)	Defining categories of breaches subject to penalties, indicators to classify the level of gravity of breaches and criteria for setting the level of penalties[146]	The Commission must adopt by 10 July 2026
Delegated act(s)	Identifying third countries with significant strategic deficiencies or weaknesses in their AML/CFT regimes and designate them as high-risk third countries, specifying countermeasures to mitigate risks[147]	The Commission may adopt the delegated acts within 20 calendar days of ascertaining criteria are met
Delegated act(s)	Identifying third countries with compliance weaknesses in their AML/CFT regimes and	

[142] Article 16(4)-(5), SRR.
[143] Article 17(3)-(4), SRR.
[144] Article 19(9)-(10), SRR.
[145] Article 28(1), SRR. On 6 March 2025, the European Banking Authority (EBA) launched a public consultation on the draft RTS.
[146] Article 68(2), SRR.
[147] Article 29, SRR.

Type	Measure	Deadline
	designate specific enhanced due diligence measures to mitigate risks[148]	
Delegated act(s)	Identifying third countries posing a specific and serious threat to the Union's financial system and designate specific countermeasures or enhanced due diligence measures to mitigate risks[149]	The Commission may adopt delegated acts where AMLA or the Commission identifies a specific and serious threat to the Union's financial system that cannot be mitigated under Articles 29 and 30 of the SRR
Delegated act(s)	Supplementing the list of prominent public functions[150]	The Commission may adopt delegated acts if the lists notified by Member States identify additional categories of prominent public functions relevant to the Union
Delegated act(s)	Amending the SRR by identifying categories of corporate entities with higher ML/TF risks and setting lower ownership thresholds[151]	The Commission may adopt delegated acts if, in its risk assessment to be completed by 10 July 2029, it concludes that a lower threshold is appropriate to mitigate risks
Implementing act	Implementing Technical Standards (ITS) specifying the format to be used for the reporting of suspicions[152]	By 10 July 2026, AMLA must develop and submit draft ITS to the Commission for adoption
Implementing act	ITS specifying the format to be used by FIUs for reporting information to the EPPO[153]	By 10 July 2026, AMLA, in collaboration with the EPPO, must develop and submit draft ITS to the Commission for adoption
Implementing act	Setting out the methodology for identifying third countries posing a specific and serious threat to the Union's financial system[154]	The Commission may decide if and when to adopt, in accordance

[148] Article 30, SRR.
[149] Article 31, SRR.
[150] Article 43(3), SRR.
[151] Article 52, SRR.
[152] Article 69(3)-(4), SRR.
[153] Article 81(1), SRR.
[154] Article 31(9), SRR.

Type	Measure	Deadline
Implementing act	Setting out the format for the establishment and communication of Member States' lists of prominent public functions[155]	with the examination procedure referred to in Article 86(2) of the SRR
Implementing act	Listing the types of legal entities governed by Member States' laws subject to the requirements of Article 57 of the SRR[156]	
Implementing act	Listing the types of legal arrangements governed under the law of Member States subject to the same beneficial ownership transparency requirements as express trusts, and a description of those legal arrangements[157]	

Level 3 measures of the SRR

Measure	Deadline
Guidelines determining the scope of internal policies, procedures, and controls, including when to organize internal controls across functions and when to use an external expert for independent audits[158]	AMLA must issue guidelines by 10 July 2026
Guidelines on the minimum content requirements and additional information sources for business-wide risk assessments[159]	
Guidelines on risk variables and factors for obliged entities when entering business relationships or conducting occasional transactions[160]	
Guidelines on ongoing monitoring of business relationships and their associated transactions	
Guidelines on establishing and governing outsourcing relationships, including monitoring critical functions by service providers, defining roles and responsibilities within outsourcing agreements, supervisory approaches and expectations for outsourcing critical functions[161]	AMLA must issue guidelines by 10 July 2027
Guidelines defining ML/TF risks, trends, and methods for non-EU geographical areas, considering Annex III risk factors[162]	
Guidelines on measures for credit institutions, financial institutions, and trust or company service providers to establish whether a customer holds total assets of at least EUR 50,000,000 (or	

[155] Article 43(2)
[156] Article 57(4), SRR.
[157] As determined in Article 58(5), SRR.
[158] Article 9(4), SRR.
[159] Article 10(4), SRR.
[160] Article 20(3), SRR.
[161] Article 18(8), SRR.
[162] If higher-risk situations are identified, the guidelines are to include EDD measures for obliged entities.

Measure	Deadline
equivalent in other currencies) in financial, investable, or real estate assets, and how to determine that value[163]	
Guidelines specifying criteria and elements for crypto-asset service providers to conduct assessments and implement risk mitigation measures, including minimum actions when identifying unregistered or unlicensed respondent entities[164]	
Guidelines specifying the measures for crypto-asset service providers to identify, assess, and mitigate ML/TF risks associated with transactions involving self-hosted addresses[165]	
Guidelines on the criteria for identifying close associates and assessing the risk levels of politically exposed persons (PEPs), their family members, and close associates, including those no longer in prominent public functions[166]	
Guidelines on the acceptable conditions for relying on information collected by another obliged entity, including for remote customer due diligence; roles and responsibilities of entities involved in such reliance; supervisory approaches to reliance on other obliged entities[167]	
Guidelines on indicators of suspicious activity or behaviours	
Joint guidelines with the European Banking Authority (EBA) on measures for credit and financial institutions to ensure AML/CFT compliance when implementing Directive 2014/92/EU,[168][169]	AMLA and EBA must issue joint guidelines by 10 July 2027

Level 2 measures of AMLD6

Type	Measure	Deadline
Delegated act	Regulatory Technical Standards (RTS) on the relevance and selection criteria when determining whether a report submitted to the FIU concerns another Member State[170]	By 10 July 2026, AMLA must develop and submit draft RTS to the Commission for adoption
Delegated act	RTS on the benchmarks and methodology for assessing and classifying the risk profile of obliged entities, including the frequency of risk profile reviews[171]	
Delegated act	RTS on criteria for determining when appointing a central contact point is	

[163] Article 34(5), SRR.
[164] Article 37(3), SRR.
[165] Article 40, SRR.
[166] Article 42(2), SRR.
[167] Article 50, SRR.
[168] Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.
[169] Article 21(4), SRR.
[170] Article 31(3), AMLD6.
[171] Article 40(2), AMLD6. On 6 March 2025, the EBA launched a public consultation which addresses this draft RTS.

Type	Measure	Deadline
	appropriate and the functions of the central contact points[172]	
Delegated act	RTS on the respective duties of home and host supervisors and the modalities of their cooperation[173]	
Delegated act(s)	RTS on the general conditions for AML/CFT supervisory colleges in the non-financial sector	
Delegated act(s)	RTS on indicators to classify the gravity of breaches, criteria for setting pecuniary sanctions or applying administrative measures, and a methodology for imposing periodic penalty payments, including their frequency[174]	
Implementing act	Implementing Technical Standards (ITS) on the format to be used for the exchange of information between FIUs[175]	By 10 July 2026, AMLA must develop and submit draft ITS to the Commission for adoption
Implementing act	ITS on the template to be used for the conclusion of cooperation agreements with supervisors of third countries[176]	By 10 July 2029, AMLA must develop and submit draft ITS to the Commission for adoption
Implementing act(s)	Laying down the methodology for collecting statistics and the arrangements for their transmission to the Commission and AMLA [177]	The Commission may decide if and when to adopt, in accordance with the examination procedure referred to in Article 72(2) of AMLD6
Implementing act(s)	Establishing the format for the submission of beneficial ownership information[178]	
Implementing act(s)	Defining the technical specifications and procedures for access to central registers based on legitimate interest[179]	
Implementing act(s)	Establishing the format for submitting information to the centralized automated mechanisms[180]	
Implementing act(s)	Setting out the technical specifications and procedures for the connection of Member States' centralised automated mechanisms to BARIS[181]	

[172] Article 41(2), AMLD6.
[173] Article 46(4), AMLD6.
[174] Article 53(10), AMLD6. On 6 March 2025, the EBA launched a public consultation on draft RTS.
[175] Article 31(2), AMLD6.
[176] Article 51(4), AMLD6.
[177] Article 9(5), AMLD6.
[178] Article 10(6), AMLD6.
[179] Article 14(1)-(2), AMLD6.
[180] Article 16(40, AMLD6.
[181] Article 16(6), AMLD6.

Type	Measure	Deadline
Implementing act(s)	Setting out the technical specifications and procedures for interconnecting Member States' central registers[182]	

Level 3 measures of AMLD6

Measure	Deadline
Guidelines on base amounts for pecuniary sanctions relative to turnover, categorized by type of breach and obliged entity[183]	AMLA must issue guidelines by 10 July 2026
Guidelines for FIUs on preserving autonomy and independence, operational and strategic analysis, cross-checking information, and practices for suspending transactions and monitoring accounts[184]	AMLA must issue guidelines by 10 July 2028
Guidelines for FIUs on procedures for forwarding and receiving reports concerning another Member State under Article 69(1)(a) of the SRR, and the follow-up actions required[185]	
Guidelines for supervisors on the characteristics of a risk-based approach to supervision, measures to ensure effective supervision and staff training, and steps for conducting risk-sensitive supervision[186]	
Guidelines on criteria to assess good repute, honesty, and integrity, knowledge, expertise, and the consistent application by supervisors of their entrusted powers[187]	AMLA must issue guidelines by 10 July 2029
Guidelines on cooperation between financial supervisors and the authorities competent for the supervision of credit institutions or financial institutions[188]	AMLA, in consultation with EBA, must issue guidelines by 10 July 2029
Guidelines on cooperation between competent authorities and central register entities to prevent ML/TF, and procedures for supervisory authorities to consider these concerns under other Union legal acts	AMLA, in cooperation with the ECB, the European Supervisory Authorities, Europol, Eurojust, and EPPO, must issue guidelines by 10 July 2029
Opinion on the methodology for the collection of statistics[189]	AMLA must issue opinion by 10 July 2029
Opinion on the functioning of AML/CFT supervisory colleges in the non-financial sector[190]	AMLA must issue opinion by 10 July 2029 and every 2 years thereafter

[182] Article 17(1)-(3), AMLD6
[183] Article 53(11), AMLD6.
[184] Article 19(10), AMLD6.
[185] Article 31(4), AMLD6
[186] Article 40(3), AMLD6.
[187] Article 6(8), AMLD6
[188] Article 64(6), AMLD6.
[189] Article 9(4), AMLD6.
[190] Articles 49(14) 50(14), AMLD6.

Measure	Deadline
Opinion on the risks of ML/TF affecting the Union[191]	AMLA must issue opinion by 10 July 2030 and every 2 years thereafter
Opinion on supervisory cooperation regarding obliged entities carrying out cross-border activities[192]	Within 1 month of request by supervisors, in the situations referred to in Article 47(3) of AMLD6
Opinion on the matter of disagreement between members of an AML/CFT supervisory college[193]	Within 2 months of request by members of a college
Opinion on the matter of disagreement between supervisors of the home and host Member States[194]	Within 1 month of request by supervisors

[191] Article 7(5)-(6), AMLD6.
[192] Article 47(3), AMLD6.
[193] Article 50(12), AMLD6.
[194] Article 54(5), AMLD6.