ACCOUNTANCY EUROPE.

BUILDING AN EFFECTIVE ANTI-MONEY LAUNDERING ECOSYSTEM

From reactive to proactive risk management

Position paper

VIEWS.

CORPORATE GOVERNANCE
MAY 2021

HIGHLIGHTS

Money laundering has devastating consequences for economy and society. It is critical to ensure that the fight against money laundering is effective.

This publication presents recommendations on how to build a more effective anti-money laundering/combating the financing of terrorism (AML/CFT) ecosystem across Europe. Our recommendations aim to better implement the existing AML/CFT legislation. This aligns with the European Commission (EC) intentions for its upcoming proposals: to ensure that the current legislative environment works effectively.

To this end, we propose upgrading the role of: i) non-financial obliged entities – including accountants – ii) supervisors and policy makers. Some of our key recommendations are:

- obliged entities need to:
    - change from reactive to proactive AML risk management
    - integrate AML into their governance
- supervisors and policy makers should promote cooperation between Member States and between the public and private sector

CONTENTS

INTRODUCTION

The EC is expected to launch legislative proposals to strengthen the AML framework in the European Union (EU). The EC Executive Vice-President Valdis Dombrovskis himself stressed the importance of this topic in the EC AML Action Plan of 2020, which proposed more stringent supervision and implementation of the rules.

Accountancy Europe supports increased action against money laundering (ML) and terrorist financing (TF) in a smart and collaborative way. We welcome the EC's forthcoming legislation to harmonise the AML rules, enhance AML supervision and establish a coordination and support mechanism for Financial Intelligence Units (FIUs). As we set out in our contribution to the EC's consultation on the AML Action Plan, effective gatekeeping is crucial as a first step but compliance on its own is not enough to ensure effective outcomes in standing up to criminals.

OBJECTIVE

This publication sets out how to build a more effective AML ecosystem. No single part of this ecosystem can defend against ML alone. Cooperation between obliged entities (OEs), supervisors and policy makers is key to achieve effective AML risk mitigation.

The current AML legislation seems to be designed primarily for the financial sector. Its requirements are not adapted to the nature of non-financial OEs' activities. This poses difficulties in interpretation and may cause gaps in its application. AML is part of an ecosystem in which every player has their respective role. It is important to ensure that each actor can play its part appropriately.

This paper proposes recommendations on how:

- OEs can change from reactive to proactive and preventive AML risk management
- OEs can strengthen AML through improved governance and internal controls
- supervisors and policymakers can improve the regulatory and supervisory framework's efficiency

SCOPE

This paper focuses on the role of OEs in the non-financial sector from the accountancy profession's point of view. We look at non-financial entities' responsibilities – including accountants – and consider potential improvements, taking into account their size and business model. The accountancy profession is also expected to support these improvements in action, as part of the non-financial OEs.

WHO ARE THE OBLIGED ENTITIES?

OEs are required by the EU AML legislation to have in place policies, controls and procedures designed to assess and mitigate ML/TF risks. They are also expected to consider risk factors related to e.g. their customers, products, services, transactions, geographic area.

OEs are grouped in financial entities such as banks and insurers and non-financial such as auditors, external accountants and tax advisors, notaries, lawyers and other legal professionals, trust or company service providers, estate agents, providers of gambling services.

OBLIGED ENTITIES NEED TO CHANGE FROM REACTIVE TO PROACTIVE AML RISK MANAGEMENT

A CLOSER LOOK AT THE RISK-BASED APPROACH TO AML

The Financial Action Task Force (FATF) has promoted risk-based principles to fight ML and TF since 2012. The 4th and 5th AML Directives also adopt a risk-based approach to AML and require OEs to implement additional risk management systems and controls. However, recent AML scandals such as Luanda Leaks, FinCEN leaks and the Panama Papers highlighted deficiencies in how AML policies are being implemented. A closer look at the risk-based approach is needed to ensure OEs understand the ML threats and take appropriate action at the right moment.

OEs appear to focus mostly on complying with a list of rules and reporting identified suspicions. Although suspicious activity reporting is an essential part of a risk and control framework, reporting alone is not sufficient to prevent ML. This was showcased by the FinCEN leaks where investigative journalists commented that OEs limited their actions to their legal requirements – i.e. kept reporting suspicious transactions – despite suspicions of illegal activities.

RECOMMENDATIONS FOR OBLIGED ENTITIES

To shift from a reactive to proactive stance, we recommend that OEs :

1. strengthen further their risk-based systems and controls
2. better recognise and mitigate ML risks
3. leverage technology for efficiency

1. STRENGTHEN FURTHER RISK-BASED SYSTEMS AND CONTROLS

The risk assessment should be proportionate to the business' size and allow for developing proportionate control measures.

We outline below three possible ways for OEs to strengthen further risk-based systems and controls.

IMPLEMENT CONTROLS IN PROPORTION WITH THE RISKS

The controls should be more extensive where a business assesses its activities as high risk. If a business does not have the resources to effectively manage that risk, it becomes exposed and could inadvertently facilitate ML. In such cases, it should either obtain the resources or consider whether to restrict that type of activity.

FATF Guidance provides useful insights into identifying AML risks. In addition, the 4th AML Directive sets out three main categories of AML risk factors: (1) customers and entities, (2) product, service, transaction or delivery channel, and (3) countries or geographic areas.[1]

ASSESS THE NEED FOR SIMPLIFIED OR ENHANCED CUSTOMER DUE DILIGENCE

OEs should document their client risk assessment and record the rationale behind each risk assessment. For example, they should explain why the risk is low enough to apply a simplified customer due diligence (CDD). The risk assessment can drive the CDD type and extent and the frequency with which it should be reviewed.

Assessing risks posed by clients is particularly important in relation to politically exposed persons (PEPs). The 4th AML Directive itself sets out criteria as to when to apply an enhanced CDD (ECDD) for PEPs. The CDD's aim is not simply to establish the person's identity or entity's existence but to understand the risks that the client may pose.

[1] For each of these three categories of risk factors the 4th AML Directive (Annex III) provides a more detailed list of factors and types of evidence of potentially higher risk

MANAGE RISK APPETITE IN LINE WITH RISK TOLERANCE

OEs should understand their unique business risk profile, including risk appetite, risk tolerance, and the controls to mitigate those risks. Risk appetite is the risk amount and type an entity is willing to take. Risk tolerance is the entity's readiness to bear the risk, after the application of controls, to achieve its objectives.

Regardless of their size and complexity, OEs need to assess whether they have the capacity to deal with the risks identified before onboarding a client. For example, dealing with face-to-face local clients requires different resources and alert mechanisms levels compared to advising offshore companies. Improving risk governance means that each entity needs to determine its risk profile and adapt its risk and control framework accordingly.

The detail and amount of work OE should undertake to develop this framework will depend on its size and complexity. A small firm may have more informal processes than those that would be expected of a large international business. Limited resources and capacity mean that it is unlikely that SMEs (or small practitioners) will implement detailed and complex risk structures, nor may this be appropriate. Nevertheless, they can adopt systems and controls proportionate to their business' size, nature and risk profile.

2. BETTER RECOGNISE AND MITIGATE MONEY LAUNDERING RISKS

Recognising ML risks requires OEs to sharpen professional judgment and skills. We set out below three possible ways for OEs to do that:

ENSURE AML TRAINING

Effective AML training should provide understanding of the regulatory requirements and their importance to the OE's business. Larger businesses should tailor training to their employees' needs and the relevant risks. For accountants, for example, professional bodies should be able to offer their members opportunities to enhance their knowledge and understand best practice.

UNDERSTAND THE SECTOR SPECIFIC RISKS

Each sector may pose different risks and red flags may vary when dealing with customers and clients. One way to recognise a red flag is to look for inconsistencies with what a typical business model of that type would entail. The inconsistency can be manifested through unusual sources of finance e.g. a traditional SME investing in bitcoin, or through using a complex company structure.

PROMOTE COLLABORATION

OEs can improve their risk awareness through discussion with other actors of the AML ecosystem. These actors can be other OEs, financial services providers, legal enforcement agencies or the FIUs. This collaboration is key to increase awareness of trends, indicators and recent AML developments. A representative example is the *Flag It Up* campaign in the UK where the accountancy, legal and real estate profession partnered with the government to exchange best practice on due diligence and Suspicious Activity Reports (SARs).

3. LEVERAGE TECHNOLOGY FOR EFFICIENCY

As technology advances, the methods money launderers use also become more sophisticated. This trend has accelerated even further as a result of the pandemic. Digitalisation creates new challenges and vulnerabilities that can be exploited for ML. These range from identity verification to new means of disguising funds origin (for example, virtual assets). To meet these challenges, OEs should leverage further available technology to increase AML efficiency and quality. They need to do this in a proportionate manner and in line with the entity's potential. We propose below three ways to achieve this.

USE TECHNOLOGY FOR CLIENT ONBOARDING

Client onboarding remains a mostly manual, time consuming and expensive process. Remote client onboarding has become more common over the last decade and the ongoing coronavirus situation has accelerated further this trend. This has highlighted the need to improve electronic/digital channels for identity verification.

Technology tools available on the market can facilitate the remote client onboarding. A very simple example is the use of a camera to confirm the client's identity. For example, FinTech businesses use this technology as part of their onboarding processes.

USE TECHNOLOGY IN KNOW YOUR CLIENT PROCEDURES

Technology can also streamline ways to collect information on clients (Know Your Client-KYC). Depending on the nature and scale of the OE, some processes can be more automated using workflow management tools. These tools can be integrated into commercial products and create predefined data fields to help standardise the data collection process. OEs can provide access to clients to upload the relevant information.

A further use of technology, subject to data protection provisions, is to create a central secure database for verification of information. Potential clients can upload their information to this database which would be accessible only to those within the regulated sector with a valid reason. Whilst this does not remove the need for due diligence measures, it means that the same documents do not have to be provided to multiple businesses within the regulated sector.

INTEGRATE DIGITAL TOOLS IN EVERYDAY BUSINESS

OEs can make better use of analytical tools in their everyday business activities. For example, accounting firms in some jurisdictions are increasingly using automated bookkeeping tools which scan invoices and assign these to expense categories. Within these tools, it is common to be able to adjust parameters so that certain items may be flagged for review. Some of these tools can set the parameters so transactions outside the norm for that business are flagged to the accountant.

Digital audit tools are also being developed, which may be able to automate analytical review within an audit. Such tools can assist in flagging unusual items, especially as part of large and complex work which may require follow-up. One of the largest global accountancy firms recently announced that it would use artificial intelligence (AI) to assist in the detection of anomalous data in payment flows to assist in combating financial crime.

These recommendations should be considered in a proportionate way and in line with the entity's size and its capabilities.

OBLIGED ENTITIES NEED TO STRENGTHEN AML THROUGH IMPROVED GOVERNANCE

Integrating AML in the governance structures can provide an OE with a better risk overview and management. It can also allow an OE to be proactive on AML risks and ensure ongoing monitoring, reporting and oversight.

Governance procedures vary depending on the business' size and complexity. While larger or complex entities have structured risk management frameworks, smaller organisations are likely to have informal discussions. Each organisation should have the flexibility to manage its risks in a way that is suitable for its business model.

OBLIGED ENTITIES' AML GOVERNANCE REQUIREMENTS

The 4th AML Directive sets a framework for integrating AML into the OE's governance structure. It assigns the OE's board and management the responsibility to oversee and manage ML risks. Nevertheless, we believe there is room for OEs to improve their governance structures and ensure that AML remains high on the board's agenda and management's execution.

We provide below a number of specific recommendations addressed to OEs' board and management. We invite smaller businesses to consider these measures and decide themselves how they best fit their practice.

BOARDS AND MANAGEMENT ROLE IN EFFECTIVE AML RISK MANAGEMENT

1. RECOMMENDATIONS FOR THE BOARD

BUILD A STRONG AML CULTURE

Boards need to understand better their ML risk exposure and key vulnerabilities. The first step is to ensure that OEs make AML risk management a recurring item of the board's agenda to ensure management oversight.

The board should set the tone on AML measures and communicate this proactively within the organisation. Board members need to challenge the policies and procedures to ensure they are commensurate with the inherent risks posed by the business activities. The board should ensure that the controls can effectively mitigate the ML risks in line with the agreed risk appetite. Its members should also foster a culture that supports appropriate AML risk awareness, behaviours and judgments about risk and provide appropriate escalation mechanisms.

CREATE AN ESCALATION PROCESS

Each OE should have a clear escalation process to allow employee reporting non-compliance with AML regulation.

A useful tool is to create a speaking-up mechanism. Boards can encourage reporting illegal activities through an anonymous whistleblowing channel. This may provide useful insights into potentially questionable practices and shed light onto new areas of risk. The EU Whistleblowing Directive contains specific provisions about protecting whistleblowers in relation to compliance with AML legislation.

ENSURE PROPORTIONATE AML RISK MANAGEMENT

All OEs, regardless of size, must implement appropriate AML risk controls. For proportionality, smaller entities may define duties division less sharply. Those that are charged with governance should nonetheless oversee and actively monitor their entity's AML risks and ensure that these are considered as part of the business strategy.

2. RECOMMENDATIONS FOR MANAGEMENT

In line with the board's guidance, management's role is to implement effective risk management and risk reporting obligations. Management should be able to recognise AML risks, monitor these on an ongoing basis and allocate adequate resources to establish a control framework that can manage and mitigate those risks.

To do that, management should regularly review the effectiveness of their policies and procedures via self-assessment or with the help of third parties to ensure that any established structures work properly. Establishing key performance indicators (KPIs) to measure the system quality and benchmarking the performance will help to estimate where the entity can position itself on the risk spectrum.

We believe entities should establish three lines of defence to coordinate this effectively and ensure sound ML/TF risk management.

1ST LINE OF DEFENCE: BUSINESS OPERATIONS

As a first line of defence, management should ensure that those engaged in the business operations understand their ML/TF risks and their obligations to manage these risks. This can be reinforced through objective setting and performance reviews.

Creating a risk reporting obligation and risk register can flag up areas of concern. Risk reporting obligations assist in making the entity more aware of potential ML/TF risks. The assigned compliance officer should include these risks in a risk register, indicating mitigating measures and most importantly report key risks and actions

to the board on a regular and timely basis (see 2nd line of defence). There also should be a feedback loop - so information gathered about risks and clients feeds back into the assessment process and control framework.

2ND LINE OF DEFENCE: RISKS CONTROLS AND COMPLIANCE

A compliance officer can be appointed in specific cases, according to the 4th AML Directive. As part of their day-to-day tasks, the compliance officer is expected to ensure that there is a cohesive prevention system in place and that any vulnerabilities or issues are flagged promptly. The aim is to ensure that those charged with governance are alert to their ML risks and take concrete steps to manage them.

OEs should build further on these legal requirements and establish a process for regular communication and reporting to the board on AML issues. The AML compliance officer should have access to the board to be able to communicate potential red flags as part of a compliance and risk management system.

Management should report to the board on a recurring basis. Depending on the organisation's size, reporting can take a form of regular meetings between managers and those who are in the governance position. In larger organisations, a formal slot at either board or risk committee meetings is recommended.

Management regularly needs to reassess whether the control processes are efficient and effective to manage ML risk. This also includes keeping up to date with the external AML developments which impact the day-to-day evolvement of the entity's business.

3RD LINE OF DEFENCE: INTERNAL AUDIT

Internal audit, the third line of defence, plays an important role in evaluating the risk management and controls including the AML officer's functioning. The internal audit function should provide the audit committee (or a similar oversight body) with periodic evaluations of compliance with AML/CFT policies and procedures.

Management should ensure that audit functions are allocated to staff who are knowledgeable and have the appropriate expertise to conduct such audits. They should be independent of the compliance team who design and implement the procedures. Management should also ensure that the audit scope and methodology are appropriate to the risk profile and that the frequency of such audits is also based on risk.

RECOMMENDATIONS FOR SUPERVISORS AND POLICYMAKERS TO REINFORCE THE REGULATORY AND SUPERVISORY FRAMEWORK

To ensure proper functioning of this AML ecosystem, supervision and regulation need to be modernised as well. We welcome the EC commitment to take action in this area. To further reinforce the regulatory and supervisory framework we recommend to:

1. enhance cooperation amongst Member States
2. facilitate collaboration between the private and public sector
3. review the interaction between AML and the General Data Protection Regulation (GDPR)
4. consider sector specific divergencies

1. ENHANCE COOPERATION BETWEEN MEMBER STATES

Criminal activity does not stop at borders. Information and knowledge sharing between national supervisory authorities is critical for the AML system to be effective. This includes sharing insights on risks within the relevant supervised population and best practice in addressing supervisory obligations.

There are existing channels for sharing information on suspicious activity. However, sharing of typologies, emerging threats and other analyses more widely may assist smaller authorities with fewer resources.

Member States should also ensure OEs have sufficient access to information. This could be achieved through data sharing and inter-operable systems, especially in respect of national registers of beneficial ownership. FIUs

and supervisors should remain open to dialogue, so that the supervised population is better informed, and proceed with pro-active action against ML risks.

EU SUPERVISOR ROLE

We believe cooperation amongst national authorities can be further enhanced with the creation of an EU supervisor. The EC has already indicated its intentions to proceed with this initiative. An EU supervisor should have a mix of direct and indirect powers. National authorities should focus on the local supervision and with supranational oversight of the supervisor. This will allow to consider factors which are specific to the relevant jurisdiction at the national level.

The direct and indirect powers combination can enable the future EU supervisor to effectively exchange best practices e.g. on the use of latest technologies, cross border aspects and analysis of business models. It will also facilitate communication and collaboration within the AML ecosystem.

In developing this model, the EC should retain the sector specific knowledge of the differing non-financial OEs which has been gained by national supervisors. The EU level supervisor should also replicate this understanding using staff who are sector experts. There are national examples of relevant supervisors that can provide references for the creation of an EU supervisor, such the Office for Professional Body AML Supervision (OPBAS).

Creating an EU supervisor will also provide an opportunity for Member States to review their existing supervisory structures and consider whether these are still fit for purpose. In some jurisdictions, the supervisory landscape is fragmented, focusing only on specific business areas.

2. FACILITATE COLLABORATION BETWEEN THE PRIVATE AND PUBLIC SECTOR

Public-private partnerships (PPPs) can play an important role in strengthening the AML ecosystem. Enhanced cooperation between OEs and authorities can better inform and improve understanding of the common threats. This should also lead to further collaboration with the FIUs and OEs in the financial and non-financial sector.

National actors should overcome the ‘taboo’ of cooperating with the private sector to combat financial crime. Although this practice seems to be more established in the financial sector, we note that this is not the case for OEs in other sectors and especially the non-financial sector. PPPs with other regulated sectors need to be established i.e. accountants, lawyers, real estate as well as banking and gaming sector.

PPPs can facilitate better use of financial intelligence through information sharing e.g. data and typologies which then can update revised ML risk assessments. Working together to understand better how criminals use the non-financial regulated sector will result in better risk management.

These partnerships should be cross-sector, involving financial institutions as well as other private-sector organisations and law enforcement agencies. It is important to also recognise that the role each plays in the AML ecosystem differs as do the resources available. Their mechanisms should be accountable and transparent while its governance should be reviewed by authorities at recurring stages.

COOPERATION BETWEEN FIUS AND OBLIGED ENTITIES

FIUs have a crucial role in assessing trends in ML and TF across the EU to identify common elements and typologies of ML. They receive significant amounts of information about incidents and suspicious cases. Cooperation with the OEs and real-time information exchange would help spot trends and identify typologies.

Currently, there is very limited feedback from FIUs to the regulated sector. This contributes to limited understanding by OEs whether and how their reports are used. This allows weaknesses in the system that criminals can exploit. In appropriate cases that intelligence needs to be shared with OEs, even if this is done anonymously. Information about trends and typologies will allow to raise red flags on matters that otherwise may have not appeared concerning. Information and intelligence sharing by FIUs can also significantly contribute to the EU AML supervisor’s work.

3. REVIEW THE INTERACTION BETWEEN AML AND THE GENERAL DATA PROTECTION REGULATION

The GDPR's impact on the AML legislation needs to be reviewed. There is a perceived inherent conflict of interest between preventing ML/TF and data protection linked to the GDPR. AML and CFT rules encourage to gather and analyse as much data as possible to identify patterns and criminals, whereas the GDPR aims to restrict the use of personal data on a large scale.

There needs to be a data exchange system whereby OEs, competent authorities and other institutions can exchange information in a safe way.

OEs in financial and non-financial sector have pointed to the need for additional rules to facilitate data use and exchange. Currently, data exchange is limited due to different interpretations of the GDPR. Data protection authorities need to provide a clear guidance to ensure that data protection rules do not inadvertently prevent information exchange or making use of technology.

The rules should be suitable for balancing key issues such as the relationship between the duty of confidentiality and data protection and the AML/CFT duties. This should apply on an equal basis to all parties that are subject to a duty of confidentiality.

4. CONSIDER SECTOR SPECIFIC DIVERGENCIES

The legislation needs to be better adapted for OEs in the non-financial sector, as the definition of OE extends beyond the financial sector. The rules should acknowledge there are different types of OEs and identify and target the factors to consider.

A concrete example how the future AML legislation should consider the specificities of the non-financial sector relates to the 'transaction' concept. The definition and monitoring of a 'transaction' does not map easily across to the accountancy profession or other parts of the non-financial sector. This means that each sector has to produce guidance to interpret and implement this requirement. The value of ongoing monitoring of client relationships is undoubted, but clearer and more tailored legislation as is currently the case in the financial sector may allow more effective use of resources by OEs and their supervisors.

In addition, non-financial OEs are often required to perform AML checks for financial transactions similar to the ones financial OEs carry out. It is important to avoid duplication between the financial and non-financial OEs' activities. As the financial OEs have direct exposure to AML risks resulting from financial transactions, they can take the lead in checking this for the purposes of AML.

CONCLUSIONS

ML has devastating consequences for the economy and society. It is critical to ensure that the fight against ML is effective and efficient. The upcoming EC AML reforms focus on consistent implementation of the AML rules and more stringent supervision. However, the enhanced EU action against ML is only a part of the solution.

AML is part of an ecosystem in which every player has a respective role. It is important to ensure that each actor plays its part appropriately.

OEs themselves should improve their proactive action on AML. This includes further strengthening their risk-based systems, better recognising and mitigating ML risks and leveraging the use of technology.

The governance's role is indispensable to fight ML. AML needs to be integrated in the OE's governance structures and its risk management. Boards need to understand better their ML risk exposure and key vulnerabilities. Management should be able to better recognise AML risks, monitor these on an ongoing basis and allocate adequate resources to establish a control framework that can manage and mitigate those risks.

Supervision and regulation also need to be modernised to ensure proper functioning of the AML ecosystem. Enhancing cooperation between OEs, supervisors and policy makers is crucial to achieve effective AML risk mitigation.

Avenue d'Auderghem 22-28, 1040 Brussels

+32(0)2 893 33 60

www.accountancyeurope.eu

@AccountancyEU

Accountancy Europe

ABOUT ACCOUNTANCY EUROPE

Accountancy Europe unites 50 professional organisations from 35 countries that represent close to **1 million** professional accountants, auditors and advisors. They make numbers work for people. Accountancy Europe translates their daily experience to inform the public policy debate in Europe and beyond.

Accountancy Europe is in the EU Transparency Register (No 4713568401-18).