Luxembourg's Insurance sector must embrace AML/CTF compliance

By Nicolas MARINIER, Partner and Emilie RUBAYIZA, Senior Manager at Deloitte Luxembourg

Due to fewer transactions, some might mistakenly assume that the insurance sector bears a lower money laundering and terrorist financing (ML/TF) risk than banks and investment funds. But the insurance sector is not immune to ML/TF, and this misperception is dangerous:

1. Criminals may target the insurance industry to commit their fraud or transgress Targeted Financial Sanctions (TFS). While TFS violation and fraud are now clearly identified by Luxembourg Penal Code (art. 506-1) as *primary* ML offenses, "classic" ML/TF risks, like drug trafficking, prostitution, tax crime or corruption should not be forgotten or overlooked.
2. Money launderers aim to outsmart "lines of defense" by having a diverse "investment" strategy/portfolio, and subscribing to multiple insurance products. These may include products that offer high premiums, cash-outs and/or investment values. Or they may subscribe to an insurance contract with unlawful funds in order to receive regular returns to put back into legitimate monetary streams. Others may even transfer the ownership of their fraudulent products via an insurance contract.
3. Criminals are IT and cyber savvy and adapt quickly to digitalization. The absence of strong AML/CTF infrastructure with sound IT solutions and automated controls put insurance sector professionals at risk.
4. Insurance watchdogs worldwide continue to reinforce AML/CTF regulatory obligations and expect a risk-based approach with stricter, more frequent and efficient controls, and Luxembourg is no exception.

The Commissariat aux Assurances (CAA) requires and expects the implementation of a robust AML/CTF framework, not only through its regulation 20/03, but also through its:

Offsite inspections with qualitative and quantitative, thoroughgoing questionnaires.

The latest CAA circular letter 23/3 mandates that certain insurance intermediaries marketing certain life insurance products annually prepare quantitative data for business relationships initiated from 1 July 2023 and contracted in 2023. This is also applicable for existing contracts with a review, movement, or significant change from 1 July 2023. The

initial report must be filed on 31 January 2024 and subsequent ones on the anniversary date.

Other previous CAA circular letters (18/9, 19/8, 21/2, 21/16, 22/3, etc.) request insurers, reinsurers or intermediaries to provide data and information on their AML/CTF framework, relating to the following data and information :
- Risk-Based Approach (RBA) used,
- Customer Due Diligence measures in place, and
- Obligation of carrying out a periodic review of existing contracts:
o before 2024 for those with a higher ML/TF risk
o before 2027 for the remaining.

When the CAA conducts a review, large amounts of relevant entity data and information is obtained through CAA questionnaires. The CAA performs further risk assessment of the supervised professionals based on the responses provided or inconsistencies noted.

Tightened and in-depth onsite inspections that complement remote inspections.

As stated by CAA Director Thierry Flamand on 19 November 2021 in the newspaper *d'Lëtzebuerger Land*, professionals *"are now expected to be irreproachable, both for new businesses and for the past."*[1] According to Article 8-4 of the Luxembourg AML/CTF Law of 12 November 2004 as amended (the AML Law), the market should not be surprised to see professionals who neglect their AML/CTF obligations named in a public statement and/or summoned to pay a substantial fine.

Vigilance is expected from all professionals at all times.

Soaring compliance costs, combined with low margins and growing inflation under the current economic climate, may seem overwhelming. Navigate this matter and mitigate any related risks with the following options.

Developing a sturdy action plan should include *at minima five key components*:

1. A well-defined **Risk-Based Approach**, consisting of:

a. A comprehensive **Risk Appetite Statement** (RAS): As cited by CAA circular letter 22/3 (3 March 2022), in which the CAA questions specific professionals[2] on whether they have established a RAS. Prior to bullet (a) above, in 2021, CAA circular 21/6 indicated the requirement to define a RAS by adopting the EBA guidelines "EBA/GL/2021/02" (i.e., points 1.18, 4.7 g) and 4.64 c)). It states that *"firms should ensure that their business-wide risk assessment also reflects […] their ML/TF risk appetite."*[3]
b. The company's own **Compliance Risk Assessment** (CRA): Article 3 of the CAA regulation 20/03 requires professionals to establish a CRA. A firm should ensure that all ML/TF risk areas are catalogued, distinguishing and accurately measuring the inherent risk of each risk area, the applicable controls (by the first, second and third line of defense (LoD)), as well as corresponding residual risk. Despite being time-consuming, CRA is worth it and should include stakeholder input to provide a holistic view to the Compliance Officer and Senior Management that can easily be leveraged, updated and continuously improved when needed.
c. The **Risk Assessment** for each client and/or contract: This must be regularly reassessed during periodic review processes or on ad-hoc basis (i.e., upon occurrence of a catalyst event such change of beneficial owner or beneficiaries).

2. A sound risk-based **customer due diligence** program (CDD) that will distinguish contracts with higher ML/TF risk exposure from others and assign a corresponding due diligence level to each contract.

CDD must at least include standard due diligence (if the contract is low or medium risk) or an enhanced due diligence (if it is high risk). The AML Law offers non-mandatory simplified due diligence (SDD) measures when several low-risk conditions are met.

The SDD measures still require controls and follow-ups; even if intermediaries can be used, the responsibility of the controls remains with the insurance professional.

3. An **ongoing due diligence program** (ODD) consisting of:

a. A **name-screening** process to regularly check the names of clients, related parties and intermediaries/counterparties. However, relying only on updated sanctions and politically exposed person (PEP) lists may lead to inadequacies and inaccuracies if documentation is not current. The system might screen unrelated or incorrect counterparties, increasing a firm's risk if the "true related counterparties" happen to be criminal. This could be a detriment to a professional's 5th AML obligation (to cooperate with authorities without delay). Reliable, complete and up-to-date data is paramount.

b. A **transaction monitoring** process, whereby complex and unusual transactions should be detected and analyzed.

c. A CDD program requires **periodic review** to remain accurate and protect the insurance professionals' reputation and financial stability.

Although sufficient initial due diligence is done while opening a relationship , a periodic review of a client's information is essential to capture changes in related parties and the impact of combining client data with external data. Due to limited compliance resources, data collection, updates and analysis, plus controls designed to produce refined and relevant alerts, are recommended.

The "wait and see approach" (i.e., waiting to see the consequences that unfold when other professionals fail to comply) leads to stress for you and concerns from regulators and auditors and cascades higher compliance costs, penalties and urgent remediation measures.

Neglecting periodic customer reviews raises ML/TF risks for companies, particularly with aged or complex contracts, regardless of client type (company or individual). For example, ignoring ultimate beneficial owners in complex structures, especially when holding, structural or managerial changes occur, can increase risks. Lacking information/documentation on the source of a clients' funds or wealth amplifies risks, especially with criminal networks.

As the age-old adage advises: "Invest in your wellness instead of paying for your sickness", because the consequences can be catastrophic for both the professional, their clients and team.

Whichever option is chosen, costs are implicated. Nevertheless, a well-considered, pre-remediation plan or gap analysis is cheaper.

Before conducting a periodic review, you should categorize contracts based on their risk profile. Well-engineered technological solutions, like Deloitte's own D.KYC can also be used. These solutions should be designed around a company's size and goals and provide invaluable data analytics for leadership like a dashboard with detailed, real-time metrics ranging from contracts that pose a high ML/TF risk, to contracts that have been reviewed or are due for review, to customizable indicators.

4. Adequate governance as follows:

a. Senior Management should set the right tone and give staff the necessary support. They should prioritize AML/CTF, resilient internal processes and controls that mitigate ML/TF risks.

b. Hiring skilled AML staff and providing them with adequate training is essential. They should be equipped with suitable technological solutions to carry out their regulatory duties.

c. Internal auditors should have sound knowledge of AML/CTF requirements to fulfill their duties and assess the strength of their firm's policies and processes.

5. Cooperation with authorities: Professionals must ensure that their internal processes and controls enable immediate cooperation at all times. Immediate escalation of AML matters to the Compliance Officer should be underscored.

1) «On attend d'elles maintenant qu'elles soient irréprochables, aussi bien pour les nouvelles affaires que pour le passé.»
https://www.land.lu/page/article/680/338680/DEU/index.html
2) The scope of circular 22/3 was:
- Life insurance undertakings;
- Brokers with activity (new production or recurring premiums) relating to the life classes of Annex II of the amended Law of 7 December 2015 on the insurance sector;
- Branches of life insurance undertakings from the European Economic Area (EEA) or third countries.
3) Guidelines EBA/2021/02 were amended on 31 March 2023 by guidelines EBA/GL/2023/03. The changes relate to the risk assessment of not-for-profit organizations (NPO).