BAOB BELGIAN AUDIT OVERSIGHT BOARD

Insights

31 March 2023

Sectoral risk assessment of money laundering and terrorist financing 2022

Article 87 of the Law of 18 September 2017 on preventing money laundering and terrorist financing and restricting the use of cash (hereafter "the AML/CFT Law") requires competent authorities to carry out their supervision on the basis of a risk assessment.

In order to fulfil this obligation, the supervisory authority needs, on the one hand, to have a clear view of the ML/FT risks in Belgium, and on the other hand, to determine the frequency and intensity of supervision based on the risk profile of the obliged entities. In order to fulfil these requirements, a sectoral risk analysis is required. The last risk analysis by the BAOB dates back to 2018. The supervisory practice of the BAOB and the knowledge and application of AML law has evolved a great deal since, hence the need to update this analysis.

The sectoral risk analysis aims to provide insight into the risks present in the audit sector as at 2 January 2023. The risk analysis is designed so that it can be regularly supplemented or updated based on a changing understanding and the development of risks in the audit sector.

Table of Contents

Context of the sectoral risk analysis

1.1. Objective and methodology

Article 87 of the Law of 18 September 2017 on preventing money laundering and terrorist financing and restricting the use of cash (hereafter "the AML/CFT Law") requires competent authorities to carry out their supervision on the basis of a risk assessment.

In order to fulfil this obligation, the supervisory authority needs, on the one hand, to have a clear view of the ML/FT[1] risks in Belgium, and on the other hand, to determine the frequency and intensity of supervision based on the risk profile of the obliged entities[2]. In order to fulfil these requirements, a sectoral risk analysis is required.

This analysis seeks, therefore, to give insight into the risks present in the audit sector as at 2 January 2023. As required under the AML/CFT Law[3], the supervisory authority is to do so on the basis of the supranational risk assessment conducted by the European Commission and on the national risk assessment. This is also the methodology we have used in this risk analysis.

Those insights are further supplemented by the Belgian Audit Oversight Board's own observations and with valuable data it gathered via a questionnaire conducted during the summer of 2022, known as the "AML survey" [4].

The BAOB also conferred with the National Bank of Belgium and the FSMA regarding the approach to take for the sectoral risk analysis.

The objective of this risk analysis is therefore, first of all, to serve as a guide to the BAOB's supervisory activities with regard to ML/FT; the risk analysis must form the basis of a risk-based supervisory approach that uses the BAOB's time and resources allocated to AML/CFT as efficiently as possible.

Second, the risk analysis is also intended to be a resource for auditors when drawing up their overall risk assessments. Article 16 of the AML/CFT Law provides that obliged entities must take into account any and all relevant information they have. The sectoral risk analysis can provide useful insights here, as a supplement to the supranational risk assessment.

The sectoral analysis also contains elements from the national risk assessment that are relevant to auditors. The national risk assessment itself is a confidential document, but supervisors are required to share the relevant insights contained therein with obliged entities so that they can take them into account when drawing up their overall risk assessments. We fulfil this obligation by including the insights in question in our sectoral risk analysis.

1 "Money laundering/Terrorist financing".
2 Art. 87, §1 of the AML/CFT Law.
3 Art. 87, §1, 1° of the AML/CFT Law.
4 More information is available on the website of the BAOB.

1.2. Legal context

The sectoral risk assessment is not only a useful element but also a legal obligation pursuant to Article 87, §1 of the AML/CFT Law[5].

This Article is in turn the national transposition of the obligation laid down in Article 48(6) of Directive EU 2015/849 of May 2015[6]:

The FATF's Recommendation 28 on the regulation and supervision of DNFBPs[7] also requires competent authorities to conduct their supervision using a risk-based approach[8]:

1.3. The European risk assessment

The **supranational risk assessment conducted by the European Commission on 27 October 2022**[9] considers all the main ML/FT risks in all sectors at EU level. The risk assessment focuses on the vulnerabilities identified at EU level, both as regards the legal framework and in terms of its implementation, and contains recommendations on how to address these. In this sectoral analysis, we will limit ourselves to a brief discussion of the main horizontal vulnerabilities across several sectors, the most significant recommendations and the specific risk analyses relating to the audit sector and audit services.

---

5 *"The supervisory authorities shall exercise their supervision based on a risk assessment. To that end, they shall ensure that they: 1° have a clear understanding of the ML/FT risks present in Belgium, based on relevant information concerning national and international risks, including the report drawn up by the European Commission pursuant to Article 6(1) of Directive 2015/849 and on the national risk assessment referred to in Article 68".*

6 *"6. Member States shall ensure that when applying a risk-based approach to supervision, the competent authorities*
a) have a clear understanding of the risks of money laundering and terrorist financing present in their Member State;
b) have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the obliged entities; and
c) base the frequency and intensity of on-site and off-site supervision on the risk profile of obliged entities, and on the risks of money laundering and terrorist financing in that Member State.".

7 International standards on combating money laundering and the financing of terrorism & proliferation – The FATF Recommendations https://www.fatf-gafi.org/.

8 *"28. Regulation and supervision of designated non-financial businesses and professions*
Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.
(a) Casinos should be [...]
(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a 'fit and proper' test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements."

9 Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, COM(2022) 554, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:554:FIN.

1. Horizontal vulnerabilities

The 2019 European risk assessment[10] had already discussed a number of horizontal vulnerabilities identified across the various sectors. These are also mentioned in the 2022 European risk assessment.

Anonymity in financial transactions remains a major vulnerability; criminals wish to leave no traces behind. Traditional cash transactions are a known risk, as is trade in precious metals and diamonds. In addition, there are new financial products such as crowdfunding and cryptocurrencies that, based on their technology, can also offer far-reaching anonymity.

Criminals look for as many opportunities as possible to **infiltrate the regular economy**, and therefore seek ever more collaboration with obliged entities. They sometimes even become owners of an obliged entity so as to be able to carry out their money laundering under optimal conditions.

Identifying and collecting information on ultimate beneficial owners remains a delicate matter in every sector; such information is essential to prevent infiltration of the legitimate economy by organized crime. Criminals use complex legal structures to conceal their identity. Despite the implementation of national UBO registers, the system remains vulnerable because criminals can infiltrate via third countries that do not impose the same obligations, or they may focus on Member States where the management of registers is the weakest. There is also an increase in the use of **falsified documents**. The rise of the FinTech industry has increased the use of **digital identification**, which carries greater risks.

Difficulties in **collaboration** between supervisors in different member states also renders supervision more vulnerable. As regards supervision, there is the problem of a **limited exchange of information between the national financial intelligence units**[11] and obliged entities.

Lastly, a lack of resources, risk awareness and know-how as to the appropriate measures to take remains a vulnerability across all sectors.

2. COVID-19 pandemic

In the 2022 European risk assessment, particular attention is devoted to the COVID-19 crisis. The crisis, and in particular the measures taken to mitigate its effects, gave rise to certain risks of money laundering:

- misappropriation and fraudulent use of funds granted as financial support;
- taking over of businesses facing financial difficulties by ill-intentioned actors and criminal organizations;
- increased opportunities for criminals to obtain revenues from selling illicit pharmaceuticals and vaccines, including to governments;

[10] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, COM (2019) 370; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019DC0370.

[11] The Financial Intelligence Processing Unit in Belgium (CFI-CTIF, https://www.ctif-cfi.be/).

- more opportunities for cybercrime as a result of the increased volume of online purchases, including through the use of fraudulent identities;
- corruption among public servants when taking urgent measures and simplifying procurement rules, for example when ordering medical supplies.

3. The Russian invasion of Ukraine

In response to the Russian invasion of Ukraine, the EU significantly extended the sanctions that had already been adopted against Russia since 2014[12]. The EU also imposed measures on Belarus in parallel with those against Russia. The European Commission takes stock of these measures in its risk assessment, and points to their impact on ML/FT measures. The Commission emphasizes that the objective of the European AML/CFT framework to protect the integrity of the European financial system contributes to the protection of freedom, justice and security throughout Europe.

Tight enforcement of the rules governing "ultimate beneficial owners" is essential in order to be able to implement the sanctions; this requires:

- Further integration of various business registers within a member state;
- Smooth collaboration and information exchange among the different supervisory authorities and agencies involved;
- Effective detection and verification of assets hidden from the tax authorities.

4. Recommendations

The **European Commission** has made **11 recommendations** for the member states. We will review these briefly below so that the recommendations may also contribute to greater insight into the ML/FT risks in the EU. Given that the European Commission is the main regulatory authority as regards ML/FT, its recommendations are of particular value.

1. Scope of the **national risk assessments**: **cash-intensive sectors**, **the non-profit sector** and **virtual currency products** must be given due attention in the national risk assessments.

2. **Ultimate beneficial owners**: the information on UBOs must be adequate, accurate and up-to-date. Identification of the ultimate beneficial owner must always be part of customer due diligence measures.

3. Sufficient **resources** for the supervisors and financial intelligence units

4. More **on-site inspections**: supervisors must carry out on-site inspections with an intensity and frequency that is proportionate to the money-laundering and terrorist financing risks identified.

[12] The BAOB has published a communication for the sector regarding these sanctions, in order to enhance vigilance.

5. **Thematic controls**: supervisors must keep improving their understanding of the risks to which certain segments of their professional groups are exposed.

6. Ongoing reflection on **expanding of the list of obliged entities** as the ML/FT risks evolve.

7. Regular **collaboration among competent authorities and obliged entities**: in some member states, there is insufficient collaboration between the obliged entities and the supervisory authorities, although there are internal guidelines and rules in that regard. Their collaboration needs improvement in terms of: the requirements for high-quality reporting by the obliged entities, (knowledge about) ML/FT risks and the customer due diligence measures to be applied.

8. A sufficiently high level of customer due diligence as regards **occasional transactions**. A sufficiently low threshold for subjecting occasional transactions to customer due diligence.

9. A sufficient level of customer due diligence measures governing **bank safety deposit boxes** and similar services.

10. **Specialised and ongoing training** of the obliged entities: the European Commission reiterates the recommendation made in 2017 that training offered by the competent authorities must include the risk of infiltration by or ownership of the obliged entities.

11. **Annual report** by the competent authority on AML/CFT activities.

5. Risk analysis per sector and product and service

Services provided by accountants, auditors, advisors and tax advisors

The risks specific to the audit sector are discussed in the "commission staff working document" accompanying the European Commission's report[13]. The audit sector is addressed under the category "services provided by accountants, auditors, advisors and tax advisors".

The European Commission notes that auditors are active in various capacities and in **various sectors**. They are subject to the ML/FT legislation and the recommendations of the FATF.

The Audit Directive[14] and the Audit Regulation[15] introduce stricter requirements for carrying out statutory audits of public-interest entities by imposing rotation rules, encouraging professional scepticism and limiting conflicts of interest. The Regulation also sets requirements for the provision of non-audit services. In addition, it requires auditors to report to the supervisory authorities any significant infringement of the rules or significant threat to or doubts regarding the continuity of the obliged entity they audit. **The sector has a strong regulatory framework.**

13 SWD (2022) 344, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN
14 2014/56/EU
15 537/2014/EU

The European Commission describes the **main risk scenario** as follows:

Perpetrators may use or require the services of accountants, auditors or tax advisors, albeit with limited involvement of the professionals themselves, with the aim of (for example):

- misusing client accounts;
- purchasing real estate;
- creating and/or managing trusts and companies;
- undertaking litigation;
- arranging over- or under-invoicing or false declarations for import/export goods;
- providing false assurances;
- provide assistance with tax compliance.

Experts in this area may become involved in **money-laundering schemes** by helping to set up opaque structures. Creating such structures, often in several legal domains, including the well-known "offshore tax havens", is complex and requires professional legal and tax advice.

The services of auditors are seen by organised crime groups as a way to compensate for their own lack of expertise. The European Commission therefore considers the threat of money laundering significant when it comes to services provided by auditors (level 3 of 4).

In general, the sector is marked by **long-term business relationships**, which enable professionals to detect unusual transactions or behaviour. However, where advice is requested specifically regarding unusual or **one-time transactions**, it can happen that the service provider carries out his or her task without having a full understanding of the client's financial situation. This has consequences for the number of **suspicious transaction reports**, which is still quite low. The sector sometimes justifies the low level of reports on grounds that the professional responsible for this area does not process or initiate any financial transactions on behalf of his or her client.

The European Commission makes the following **recommendations**:

- the competent authorities must inform auditors of the supervisory measures they have taken to ensure that the sector fulfils its AML/CFT obligations with due care. Supervisors must publish a report each year on the number of suspicious transaction reports.
- the supervisors must carry out a number of on-site inspections, in proportion to the population of professionals within the territory of the member state.
- the member states are to provide guidelines on the types of risks and risk factors arising from client transactions in which the auditors are involved.
- the supervisors may adopt measures aimed at enhancing auditors' understanding of the way in which professional secrecy is to be explained and applied.

In relation to these recommendations, we should point out that we publish information at least once a year, in our annual report, about our supervision and the result of our oversight.[16]

[16] https://www.fsma.be/sites/default/files/media/files/2022-12/en_ctr_2021.pdf (p.59, "Combating money laundering and terrorist financing")

1.4. National risk assessment

On 19 June 2019, the Ministerial Committee for the coordination of the fight against the laundering of money of illegal origin published the final version of the national risk assessment relating to money laundering. On 29 March 2018, the Terrorist Financing Platform published the final version of the national risk assessment relating to terrorist financing. The latter assessment deals with the specific risks of terrorist financing. Aspects of that assessment that are relevant to the audit sector have to do with financial fraud[17]. Given that this aspect is also covered by the national risk assessment of money laundering, we will limit ourselves here to the latter.

The national risk assessment comprises a twofold analysis, with a view to drawing conclusions regarding the risks that are present in Belgium. First, it involves a threat analysis and second, it examines the vulnerability of the various sectors. Then, looking at both factors together, it identifies a certain level of money laundering risk per professional category.

A **threat** is defined as a person, business or activity that can pose an intrinsic risk and may entail harm and damage to the company. In the context of money laundering, the term applies to the perpetrators, the laundered funds and other assets, as well as to the commission of the underlying offences. Significant indicators of a higher threat level include: the frequency of observations per profile, where international trade is involved, and in particular where these concern high-risk countries and the movement of large sums of money.

Based on these indicators, the national risk assessment has **five threat levels**: non-existent, low, medium, high and severe.

Then there is the notion of **vulnerability**. The vulnerability analysis is done on the basis of a number of criteria that we can subdivide in **6 groups**: the organization of the sector, supervision of the sector, the structure of businesses in the sector, the products or services provided, the distribution channels and the geographical spread. For each sector, the national risk assessment assigns a score per criterion: non-existent, low, medium and high.

The degree of vulnerability may have a heightening or a mitigating effect on the total money laundering risk in a given sector that is subject to a certain threat. Thus, a sector with a high threat level may be deemed to be exposed only to a medium-level money laundering risk, for instance if there is strong regulation of the services offered or if supervision is well organised.

1.5. The auditor and the national risk assessment

1. Threat level

In the threat analysis, auditors fall within the profile of "*Business advisors and investment service providers, with the exception of lawyers and credit institutions, portfolio management and investment advice companies, management companies of undertakings for collective investment, and intermediaries in banking and investment services*".

[17] Neither of the national risk assessments is available to the public but are provided only to the obliged entities where the analyses are necessary to facilitate the risk assessments carried out by those entities.

This profile has a **"serious" risk level.** If we consider the description of the activities[18] that give rise to this highest ranking, it appears that these have little to do with the core activities of an auditor, but rather with certain ancillary activities that in practice are carried on by auditors:

- offering their know-how in setting up mechanisms and structures intended to launder money;
- advising on investments as part of the laundering process;
- acting as an intermediary between financiers and other financial service providers;
- helping establish offshore companies and offshore accounts;
- assisting with repatriating funds.

This "profile" is involved mostly when dealing with money from abroad and from high-risk countries. In fact, this occurs mostly when auditors and investment service providers offer their services without authorization.

It appears that auditors were classified under this profile for practical reasons and because they cannot easily be placed under any of the other profiles. The risk assessment does not mention auditors in any description of these activities, and moreover, the activities in question are ancillary ones for auditors and not part of their core activities.

This sectoral risk analysis **focuses only** on those activities that come under the supervision of the Belgian Audit Oversight Board, and not on other activities that auditors may engage in outside their core business, and for which they may draw on their broader financial-legal-tax expertise[19].

2. Vulnerability

To determine vulnerability, auditors are assessed in the national risk assessment on the basis of several different criteria. They are discussed together with other professionals who work with quantitative data: accountants and tax advisors.

Organization

The sector is governed by a strict legal framework: access to the profession is regulated, registration in an official register is required, there is compulsory continuing professional education, there are important ethical standards and supervision specifically of compliance with the Law of 18 September 2017.

The large number of players in the sector affects the supervisory capacity.

The sector has relatively low exposure to the risk of service providers carrying out illegal or unregistered transactions.

---

18 P. 61 NRA

19 Potential involvement by an auditor in such activities comes under the ML/FT supervision of the BAOB when it comes to activities for which the auditor must invoke his or her professional title: either company audits or other specific activities that he or she may carry out under Article 5 of the Law of 17 March 2019 on the professions of accountant and tax advisor. These activities include: accounting, accounting services and advice on accounting organization.

The national risk assessment thus ranks the **sector's organization** as **strong**.

Oversight

Oversight of the sector is ranked as **medium**. The fact that other professions that work with quantitative data are overseen by self-regulating institutes pulls the assessment down.

We can therefore qualify the assessment and say that the audit sector is ranked **strong**.

Structure

The structure of the players in the sector likewise contributes to a lower vulnerability: they are long-lasting, with activities focused chiefly on the long term and senior managers who remain in post for a long period. Thanks to thorough regulation, the use of fronts is nearly impossible. The legal structures are transparent and predictable.

The national risk assessment thus speaks of a **strong structure** among members of the sector.

Products/Services

The "products" offered by those holding the title of auditor consist entirely of regulated services. The value of those services is transparent and cash payment is rare. Client anonymity is not permitted. The products/services are thus **highly regulated and very transparent**.

Clientele

In general, professionals who work with quantitative data rarely carry out activities abroad and have few foreign clients or regular contact with high-risk countries.

3. Money-laundering risk

Taking into account both vulnerability and threat, the sector of business services ranks last in the national risk assessment and is hence the **least risky of all the sectors examined**. The analysis offers the following explanation:

"*The business services sector ranks 10th, because there have been very few cases of abuse found by the Belgian Financial Intelligence Processing Unit or among police fines in the sectors that make up this category, even though domiciliary companies are often found to be used for money laundering schemes. The business services sector's level of vulnerability is also affected by the presence of two well regulated sectors within it:* ***professionals who work with quantitative data****, and notaries. Domiciliary companies, by contrast, are not at all regulated."*

Risk analysis of auditors

In what follows, we discuss the risk level in the audit sector. From discussion of the supranational and national risk assessments above, it appears that of all the sectors subject to the AML/CFT legislation, auditors are generally ranked in a **low to very low risk category**. It is only for certain ancillary activities, and chiefly advisory services, that auditors may pose a higher threat of money laundering. An overall assessment in the form of a score or classification has limited added value in itself.

In this risk analysis, we describe the various aspects that are specific to the services and the organization of auditors and that impact the sector's money laundering risk. For each risk factor discussed, we indicate how the auditor and/or supervisor can mitigate it. The sectoral risk analysis is thus a useful instrument that can enable both the supervisor and the obliged entity to gain greater insight into the risks and the appropriate measures that can be taken.

2.1. A threefold risk

Auditors are faced with **three types of risk**. The nature of the risk is closely linked to the service provided. As regards auditing tasks, in which the auditor is responsible for assessing the accuracy and veracity of annual financial statements and other financial documents, there are two types of risk:

- **Indirect contribution to an ML/FT operation**: by providing certain, in some cases false, certifications, the auditor may indirectly, whether knowingly or not, contribute to a company's money laundering practices;
- **Failure to notice a ML/FT operation**: when carrying out an audit mission or statutory task, there is always a risk that the auditor may not notice a money laundering or terrorist financing operation. We should note in this regard that the auditor must always adopt a critical professional attitude, taking into account the possibility of a material misstatement that is the result of fraud. Thus, if the auditor notices (unnecessarily) complex operations or structures that may conceal a form of fraud, he or she must exercise particular vigilance;

Although this may not be the auditor's core activity, nevertheless he or she may carry out tasks other than audits, such as providing advisory services. In that case, a third risk may arise, that of **active participation in fraud**. The auditor's expertise lies at the interface of the legal and financial/economic playing field. This means the auditor is not only an expert in his or her regular activities, but also an ideal advisor to organizations with malicious intent.

2.2. Transversal risk factors

By transversal risk factors we mean risk factors that affect the entire sector, regardless of the activity performed or the client. These may be external risk factors as well as vulnerabilities or strengths that are specific to the sector. Below, we discuss the most important factors as they appear from the national and supranational risk assessments and the BAOB's experience.

1. Infiltration by criminal organizations

Auditors always run the risk that they may become involved (unwittingly) in tax fraud. As we can see from the (supra)national risk assessment as well as from the observations made by the Belgian Financial Intelligence Processing Unit in its 2021 annual report, money laundering is carried out increasingly by specialized organizations. The latter use the latest legal technology to infiltrate the regular economy. They conceal their identity as far as possible by setting up multi-layered, complex legal structures.

This risk is closely related to swindles by the client. Fraud is more difficult to identify than material errors. After all, fraud is designed to remain hidden. By working for a client with malicious intent, the auditor is also at greater risk of certifying documents that do not correspond to reality.

Mitigating ML/FT risk thus begins, for the auditor, with **a thorough knowledge of the client**. The auditor must pay particular attention to the identification of the client and the latter's representative, as well as to the identification of the UBOs.

If the auditor finds that it is difficult to determine the identity of the client and/or the UBO, or that the latter does not match the UBO listed in the national UBO register, this should give rise to an **increased risk level** for that client. In addition, the auditor must inform the General Administration of the Treasury and, where appropriate, the Belgian Financial Intelligence Processing Unit[20].

2. No transactions by the auditor

An important distinction between auditors and other sectors that are subject to the AML/CFT Law is that auditors, unlike financial institutions, do not themselves carry out any transactions. Where the AML/CFT Law speaks of "transactions", this is intended first of all as a transactions by a certain obliged entity (e.g. a money transfer by a bank's client).

Of course, as the AML/CFT Law stands, the auditor must be vigilant not only when it comes to transactions which the client carries out with the auditor in question (e.g. paying for a certain service), but also for other transactions that the auditor comes across when conducting his or her activities.

The fact that auditors do not carry out any transactions for their clients has a significant **mitigating effect on the sector's ML/FT risk**.

The fact that the auditor must look out for a great many transactions creates **a more limited, yet frequent risk of exposure to ML/FT risks**.

3. Relationship of trust with the client

The audit sector is characterized by long-standing relationships with the client. In terms of ML/FT risk, this is a double-edged sword. A long-term business relationship leads to **a thorough knowledge of the client** and its characteristics. This facilitates a risk-based approach, since the auditor knows the vulnerabilities of the obliged entity and can more readily identify abnormal transactions.

[20] Article 74/1 and 47, §1 of the AML/CFT Law.

On the other hand, a business relationship can lead to **an unwarranted trust in the client**. One thinks one knows the client and therefore may be less thorough in carrying out the activities. Or one may think one is still working for the same client, although there have been fundamental changes to the underlying structures, such as in terms of the UBOs.

This risk is less common among audit missions with PIEs, given that the law limits the term to 9 years for an audit firm and 6 years for a natural person who performs the audit. In other types of clients, a mandate that is longer than 9 years leads to a heightened risk.

4. Reports to the Belgian Financial Intelligence Processing Unit (CFI-CTIF)

The number of suspicious transaction reports made by auditors to the CFI-CTIF is low. The following table shows the numbers for the last three years. In 2021, they accounted for 0.19% of all reports received by the CFI-CTIF.

	2021	2020	2019
Number of reports received	86	38	73
Number of reports forwarded to the Prosecutor's Office	6	4	6
Percentage of reports forwarded	7%	11%	8%

The relatively low number of reports is due, first of all, to the fact that auditors do not themselves carry out any transactions for their clients. In the event of a shorter business relationship, the auditor has no insight into most transactions by the client, and therefore will not be able to report them. In the event of a long-term relationship, there is a risk of excessive trust.

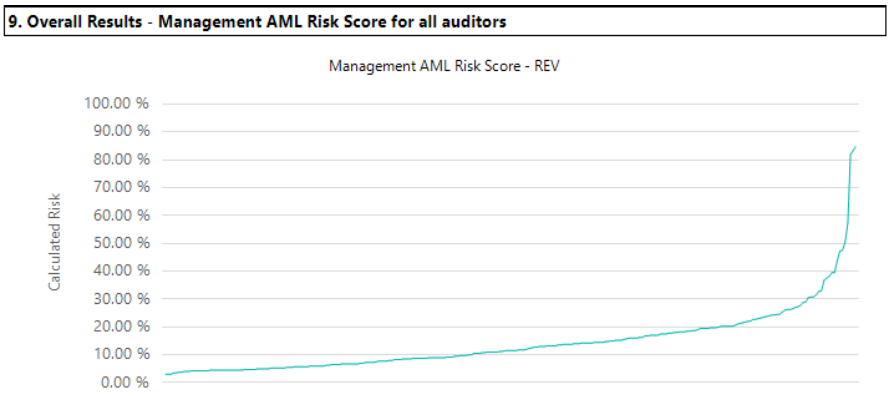
The results of the AML survey conducted in 2022 show that across the entire sector, 129 suspicious transaction reports were made to the AMLCO. 86 of those led to a report being sent to the CFI-CTIF. This seems to indicate that **the threshold for filing a report was (too) high**, given that such a report has to be filed for every atypical transaction identified, in other words every transaction that does not fit the client's profile. Only if the AMLCO also considers the transaction to be suspicious does the auditor have to report it to the CFI-CTIF.

In any case, one has to be careful about drawing too many conclusions from such a low number of reports. It is worth noting, however, that the 86 reports **are concentrated among 27 auditors/audit firms.** 51 of the reports were made by three relatively small firms. These figures indicate that vigilance for suspicious transactions may need improvement in the sector, and that the sector and its supervisor need to remain attentive in this regard.

5. Formal office organization

In the summer of 2022, the BAOB conducted a survey into the ML/FT risks to which auditors and audit firms are exposed. The questionnaire looked on the one hand at office procedures and organization, and on the other hand, at the inherent risk factors such as the clientele and the services offered. The questionnaire's results suggested, based on the sector's self-reporting, that the **organizational risk is**

very low and that it had fallen considerably since the same survey conducted in 2018, that is, within a year of the entry into force of the AML/CFT Law[21].



Overview of ML/FT organizational risk among auditors 2018

Overview of ML/FT organizational risk among auditors 2022

There are **two reasons** for this evolution. First, the AML/CFT Law was relatively new in 2018, whereas by 2022 there was better knowledge and awareness in the sector of the legal obligations. Second, the ICCI[22] published a guide in 2020 on "internal procedures for combating money laundering", and an updated version came out in September 2021. The guide contains all the requisite procedures and can

[21] The BAOB was established in December 2016 and began operations in 2017. The first ML/FT survey took place in October 2018.

[22] The Belgian Auditors Information Centre (https://www.icci.be)

be used in and of itself as an office handbook, with a few adjustments to the particularities of the individual firm. The handbook is very widely used in the sector and ensures that, at least in formal terms, almost all auditors and audit firms have the necessary procedures. Moreover, the BAOB made available a practical guide to help auditors draw up an overall risk assessment[23].

These observations suggest that the sector is generally well aware of the importance of the AML/CFT procedures and that these procedures are widespread. This has a significant mitigating effect on the ML/FT risks in the sector.

An **ongoing point** needing the BAOB's attention is the **effective implementation** of these procedures when carrying out the audit mandates and other audit activities. It is not enough for these procedures to exist, be formalized and known; they must also be implemented.

6. Temporarily inactive auditors

Temporarily inactive auditors fall within the scope of the AML/CFT Law. The BAOB is not competent, however, to supervise compliance with the AML/CFT Law by temporarily inactive auditors[24].

An auditor who has reported being temporarily inactive as an employee of a firm most likely does not have the office organization required by the AML/CFT Law.

Yet such auditors can return to their profession at any time. During the first five years they can do so without any exam, and after that period they have to take a simplified test. In the meantime, they are not subject to any ML/FT supervision, since they are not allowed to perform any regulated activities.

Given that only a **limited number** of temporarily inactive auditors return to the profession, we describe this risk as **medium**. Nevertheless, it merits due attention by the supervisor.

As at 9 December 2022, there were 190 auditors listed as "temporarily inactive" in the public register.

7. Continuing professional education

Auditors take a legally mandated number of continuing professional education hours. The specifics are laid down by a standard adopted by the Institute of Registered Auditors (IBR-IRE). The standard was updated on 17 June 2021. It stipulates that auditors must take at least 84 hours of training over a period of 3 years, consisting of a selection of relevant training courses. Compliance with the anti-money laundering legislation is given as an example of a training that is eligible for these continuing professional education hours. It is good that this is used as an example in the standard, but of course this is no guarantee that auditors will in fact receive sufficient training in this regard.

---

[23] The BAOB has published a communication for the sector regarding these sanctions, in order to enhance vigilance.

[24] Article 5, 23° of the AML/CFT Law defines the scope. "*23° natural or legal persons operating in Belgium that are registered or recorded in the public register held by the Institut des réviseurs d'entreprises / Instituut der Bedrijfsrevisoren (Institute of Registered Auditors), in accordance with Article 10 of the Law of 7 December 2016 on the organisation of the profession and the public supervision of auditors, natural persons that are trainee external auditors as referred to in Article 11, § 3 of the aforementioned law, and audit firms and persons exercising the profession of statutory auditor*."
Article 85, §1, 6° of the same Law on the competence of the BAOB: "6° *the Belgian Audit Oversight College, with regard to the obliged entities referred to in Article 5, § 1, 23°, for their auditing tasks and the other activities they can carry out by enrolling or registering in the public register of auditors or in their capacity of trainee-auditor;*"

Good knowledge of the anti-money laundering legislation helps mitigate the ML/FT risks. It is thus worth recommending that auditors take **9 hours of training on this topic every three years**.

8. Digitalization and automation

As in every sector, auditors are subject to increasing digitalization and automation. This trend entails a twofold risk.

First, this development means less direct contact with clients, in favour of **more remote relations**. In terms of ML/FT, this involves greater risk, in particular when it comes to identifying one's client.

Second, it can lead to **disadvantages of scale** for smaller audit firms. They have to join this trend but cannot make the same investment as their larger competitors. In order to remain competitive in terms of price, they risk adopting less thorough procedures, including as regards the identification of their clients.

Digitalization cannot of course be stopped, nor would it be desirable to do so. But sufficient and sustained attention needs to be devoted to the effectiveness of the AML/CFT procedures adopted, and in particular to the reliability of the knowledge about the client. When it comes to **identifying one's client remotely**, the Belgian e-ID must be used; if not, the client risk is higher, and greater vigilance is required.

The results of the ML/FT survey conducted in 2022 show that **93 of the 221 people** questioned in the past calendar year identified their clients and/or their clients' representatives remotely.

9. Introduction of clients by third parties

The BAOB noted in the course of its supervision that auditors sometimes come into contact with their clients via the latter's external accountant and that the subsequent business relationship is conducted entirely via the accountant. In such cases, the auditor incorrectly failed to verify the mandate of the accountant, who was thus serving as the client's representative.

It is difficult to determine how often this practice occurs, but in the cases where it does, and in any case where the contact person's mandate is not verified, there is a **significantly higher ML/FT risk**.

Auditors can rule out this risk by always following the legal procedures and identifying both the client and the latter's representative, and checking not just their identity but also **verifying their mandate**.

220 of the 221 auditors reported in the 2022 survey that they had in place the proper procedures for identifying and confirming the identity of their client and the client's representative[25].

[25] Article 21 and 22 of the AML/CFT Law.

10. Professional secrecy

Auditors are subject to a legally protected obligation of **professional secrecy**. Sometimes auditors hide behind professional secrecy in order not to **report suspicious transactions** to the Belgian Financial Intelligence Processing Unit, or at the very least they have a certain hesitation. Not necessarily just because of the legally required professional secrecy, but also from the perspective of the relationship of confidence between the auditor and the client. The obligation of professional secrecy on the part of auditors does not apply, however, in such cases.

The effect of this fact on ML/FT risks in the sector is rather low.

The sector can work on this by improving familiarity with the rules governing professional secrecy. The Institute of Registered Auditors (IBR-IRE) and the ICCI offer useful training sessions each year on this topic.

11. Politically exposed persons (PEP)

The 2022 survey indicates that the number of clients who are recognized by the auditor or audit firm as politically exposed persons is relatively modest.

162 of the 221 respondents said they had no PEPs among their clients. The remaining 59 reported having a total of 1674 PEPs among their clients.

We can see that the majority of these clients are with the major firms, which is understandable given that there is a degree of concentration of public legal entities at the larger firms. However, this alone does not explain this distribution, and so it appears that some auditors may not be recognizing PEPs as such.

The ability to determine that a client is a politically prominent person is essential in order to apply the appropriate degree of due diligence as regards ML/FT. Insufficient knowledge in this regard or a lack of due diligence **increases the risk** in the sector.

2.3. Inherent risk factors

Inherent risks are those that are specific to a particular activity or client.

The ML/FT risks that are inherent in certain audit activities are in any case limited, given the strict regulation of those services.

1. Advisory function

As explained above, auditors may also take on a certain advisory role.

As indicated in the supranational risk analysis, the risk of money laundering in these services is heightened if the advice has to do with the creation, business activities or winding up of a legal person and legal or tax structures.

It should be noted, however, that these must remain an **ancillary activity**. As already mentioned above, the BAOB is not competent to oversee ancillary activities that do not involve auditing tasks, with the exception of accounting and related activities.

2. Valuation

Auditing tasks that concern transactions in which assets may be over- or undervalued are exposed to a higher ML/FT risk than other types of audit. This applies, in particular, to contributions in kind and quasi-contributions. In the past, there were a few suspicious transaction reports to the Belgian Financial Processing Unit regarding contributions in kind.

155 of the 221 respondents to the 2022 survey reported that they had carried out activities relating to contributions in kind or quasi-contributions. In all, 560 tasks were involved, representing a turnover of nearly EUR 7 million. This is thus only a fraction of the total turnover from audit activities in the sector, but it is certainly one that occurs quite frequently.

For the supervisor, it is important, despite the limited financial scale, to **include this activity in the scope of the AML inspections**, given the inherent risk.

3. Clients

The national risk assessment describes the risk factors of **10 sectors**. Given that auditors have clients from every sector, and given that their vigilance must be shown to apply to all (significant) client transactions, the client's sector has an impact on the risk to which the auditor is exposed. In what follows, we describe the main risk factors per sector. We list the sectors in the order of the identified risk level in the national risk assessment, starting with the highest risks.

The client risk level reported is **an indication that can be sued by the auditor in its individual risk assessment**. This of course applies only to the "sector in which the client is active", and must be examined in conjunction with the other characteristics of the client in order to assign an appropriate risk score.

Luxury goods sector

This covers traders in antiques, art, diamonds and precious metals as well as jewellers. The risk factors are the high volatility of the prices and the fact that the assets are subject to valuation. The sector often uses liquid funds that they can easily keep off their official books. There is increasing use of remote sales, which facilitates anonymity and thus also increases the risk of money laundering.

The client risk for this sector is **high to very high**.

34 of the auditors or audit firms indicated in the 2022 survey that they have clients in the luxury goods sector. This amounts to a total of **267** clients.

Second-hand vehicle sector

The risk of money laundering in this sector is high because there is a wide margin of appreciation on the value of the goods, up to around 50% of the market value. Trade in cars that have been written off is often conducted using cash, given that the (official) resale value is often under EUR 3000.

This sector is sensitive to parallel under-the-counter payments between companies. A large part of this trade is intended for export, often to countries with limited oversight and using various intermediaries. It is therefore difficult to determine who the actual client is and therefore also, for instance, to verify that the claims can in fact be collected.

The client risk for this sector is **high to very high**.

59 of the auditors or audit firms indicated in the 2022 survey that they have clients in the second-hand vehicle sector. This amounts to a total of **418** clients.

Hospitality sector

This sector is characterized by a high risk of intervention by criminals. The sector sees a lot of cash transactions and there is a lot of tax and social insurance fraud. Transactions by service providers are still not always recorded (although this has improved since the introduction of the 'registered tills, also known as 'white tills'). Turnover among managers is high and companies and businesses are very often bought and sold.

The client risk for this sector is **high to very high**.

61 of the auditors or audit firms indicated in the 2022 survey that they have clients in the hospitality sector. This amounts to a total of **401** clients.

Leisure sector

The leisure sector consists of football clubs, the National Lottery, casinos, video arcades, betting gambling businesses and racehorses. This sector is quite highly regulated and is subject to thorough oversight, yet it is nevertheless exposed to a number of significant ML/FT risks. Specifically in the case of racehorses, there is a valuation risk; these activities are also sensitive to sales-related risks, since they change ownership without changing locations.

Casinos, arcades and gambling businesses generate significant cash flow. 80 to 85% of bets are placed in cash. The winnings are also paid out in cash. These establishments are also vulnerable to fraud with documents, such as fake winnings statements.

The football sector is known to have many ultimate beneficial owners abroad, often in countries with an elevated risk. The source of the money is not always clear. The valuation of the players traded on the transfer market is highly variable, and takes place via intermediaries (brokers) who have a major incentive to persuade club managers to make their trades through them. Bribery is not unknown.

The client risk for this sector is **high**.

18 of the auditors or audit firms indicated in the 2022 survey that they have clients in the leisure sector. This amounts to a total of **83** clients. Football clubs are not included here.

Retail sector

This group comprises night shops, call shops, tobacconists and bonded warehouses. The sector has limited exposure to the risk that service providers may carry out illegal or unregistered transactions. They frequently use fronts, while the actual owner of the (store) chain is hidden behind complex structures. There is also considerable use of cash. Night shops are used to mix legal and illegal cash flows, as a way to launder the latter.

The client risk for this sector is **high**.

10 of the auditors or audit firms indicated in the 2022 survey that they have clients in the retail sector. This amounts to a total of **78** clients.

Real estate sector

Notaries, the construction sector and real estate agents make up the real estate sector.

Two of the subgroups in this sector face serious threats of money laundering, namely, the construction sector and real estate brokers.

In the **construction sector**, there is a lot of social dumping. Workers are hired on secondment from third countries. The monies that flow to the other country are difficult to trace. There are often parallel payments made under the counter. Various foreign subcontractors are used. These companies often use fronts. The management keeps on changing and there are many bankruptcies. It is mainly companies that lack continuity in their organization and work via multiple and complex collaboration agreements that constitute a heightened risk for auditors.

Real estate brokers are subject to higher risk because foreign investors from high-risk areas are often involved in the purchase. The sums of money are very high and there is a risk of parallel payments under the counter. There is always a significant element of valuation of the property, which makes it a particularly **sensitive sector for auditors**. In particular, those real estate brokers that buy and sell properties themselves, rather than serving purely as intermediaries, constitute a higher risk.

The client risk is, depending on the specific sector, **medium to high**.

100 of the auditors or audit firms indicated in the 2022 survey that they have clients in the real estate sector. This amounts to a total of **2552** clients.

Cryptocurrency sector

A sector that was not included in the previous edition of the national risk assessment is that of cryptocurrencies or virtual currencies. Given the distinctive features and risks of this sector, the BAOB has added this sector here[26].
With the creation of Bitcoin in 2009, an entirely new class of assets came into existence: cryptocurrencies. These currencies are marked by the fact that they are entirely digital and are managed by a distributed computer network. The currencies are not managed by a central entity, and users can take charge on their own without needing an intermediary such as a bank.

The purchase of cryptocurrencies can be carried out in different ways, but the most popular method is to buy them via a decentralized trading platform. These platforms can be compared to the purchase of shares via a trading platform. Well known examples include Coinbase and Binance. The use of such a platform is not necessary, however. So-called **"peer-to-peer" trade** is also very important. People can create a wallet and can move money from one wallet to another without having recourse to a third party. This form of money transfer is difficult to monitor.

Although only a few smaller cryptocurrencies offer full **anonymity**, it is more difficult for supervisors or auditors to determine the identity of the parties involved in cryptocurrency transactions. Cryptocurrencies can also be sent internationally without any delay. All these aspects make cryptocurrencies interesting to criminals and money laundering.

Auditing cryptoactivities is very complex. Companies that provide trading services in cryptocurrencies offer comparable services as the traditional financial sector. The most important of these are the buying and selling of financial assets, offering savings products, lending money and providing custodial services (the latter service is mainly important to users who do not have the requisite knowledge to set up their own cryptowallet).

The **underlying processes** are very different, however, from the traditional financial sector. In the case of cryptotrading platforms, one has not only to ensure that all transactions are correctly entered in the accounts but also that the underlying custody of the currencies is handled correctly. This takes place entirely digitally and requires the right cryptographic procedures to rule out the risk of a "hack". The "stock" of cryptocurrencies must match the currencies held by users. Moreover, there is an elevated risk that the custodian itself uses the cryptocurrency to make loans or for speculation.

This complexity applies not only to companies for whom cryptocurrencies are the core activity, but any company that uses cryptocurrencies, for example, as a means of payment or that holds cryptocurrencies on its balance sheet.

There is therefore a **doubly elevated ML/FT risk**: first, the **increased risk inherent** in (trade in) cryptocurrencies, and second, the potential **lack of specific knowledge** on the part of the auditor, who therefore may not notice money laundering activity.

[26] The FSMA is the competent supervisory authority for Virtual Asset Service Providers, and it publishes on the topic of fraud related to cryptocurrencies, among other things, on https://www.fsma.be/en/virtual-asset-service-provider-vasp

The client risk for this sector is **high**. Among other companies for whom cryptocurrencies are not the core activity, auditors should always treat the presence of cryptocurrencies at the company as a higher risk factor when evaluating client risk.

Financing sector

This sector comprises consumer credit, leasing and crowdfunding.

The sector is subject to strict supervision. Each type of activity is highly regulated. Little or no cash is used, and there are also no anonymous transactions (except for crowdfunding, where this is possible to a limited extent).

The client risk for this sector is **medium**.

Financial sector

The financial sector includes banks, stockbroking firms, portfolio management and investment advice companies, the money transfer sector and electronic money.

This sector is subject to strict supervision, has a strong organization and is relatively transparent.

The client risk for this sector is **medium**.

Special attention must, however, be paid to payment institutions and electronic money institutions that engage in the transfer of money, whether in cash or in the form of anonymous electronic money. Such institutions are subject to potentially elevated risk, particularly if the institution uses a network of agents.

Currency exchange offices may constitute elevated risk since they handle relatively large sums of cash and their clients are anonymous. Because of the limited size of the average currency exchange office, however, the risk is generally fairly **limited**.

Insurance sector

The insurance sector is subject to strict supervision and regulation and is well organized. The products are transparent and there is limited international activity.

The client risk for this sector is **low**.

Business-to-business services sector

This sector, also known as the business services sector, consists of accountants, bookkeepers, tax advisors and notaries as well as auditors. These professions are strictly regulated and well organized. The products are transparent and there is limited international activity. The sector depends partly on self-regulation.

The client risk for this sector is **low.**

***

Abbreviations

- DNFPBs: Designated Non-Financial Businesses and Professions: a collective term for non-financial sectors to which the AML/CFT Law applies. These include auditors, lawyers, notaries, accountants, etc.
- EC: European Commission
- FATF: FATF Financial Action Task Force
- GAFI: Groupe d'Action Financière (French name of the ATF)
- IBR/IRE: Institute of Registered Auditors (Instituut van de Beroepsrevisoren/Institut de réviseurs d'entreprise)
- ICCI: Informatiecentrum voor het bedrijfsrevisoraat/Centre d'information du révisorat d'entreprises [Company auditor information centre]
- ML/FT: Money laundering and the financing of terrorism
- PEP: Politically Exposed Persons
- UBO: Ultimate Beneficial Owner