Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA Guidance 04/2026

Supplement to Guidance 05/2023 concerning the money laundering risk analysis pursuant to Article 25 para. 2 AMLO-FINMA

4 June 2026

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

Contents

Introduction **3**

1 Money laundering risk tolerance **4**

2 Money laundering risk analysis **7**

2.1 Money laundering risks to be considered 7

2.2 Implementation of the requirements according to Article 13 para. 2bis AMLO-FINMA 9

2.3 Monitoring compliance with the business strategy and risk policy 10

2.4 Other elements to consider 11

3 Relationship to margin no. 78 of FINMA Circular 2017/1 "Corporate governance – banks" **12**

4 Global monitoring of money laundering risks **12**

5 FinIA institutions **13**

Introduction

With regard to combating money laundering, the money laundering risk analysis (hereinafter “risk analysis”) is the key management tool that forms the basis of risk management. The risk analysis determines the risk tolerance and sets out the binding guidelines for the structure, organisation and day-to-day management of the anti-money laundering framework. In this way, it ensures that resources, processes and controls are designed in a risk-based and appropriate manner, thereby meeting legal and regulatory requirements. In essence, the risk analysis serves to systematically identify and assess the inherent money laundering risks associated with the business model. It first determines which risks are deemed unacceptable and are therefore excluded from the business model (money laundering risk tolerance). For risks tolerated in line with the business strategy, it sets out their scope, structure and nature in a transparent manner and defines appropriate mitigation and management measures. Very high risks must either be eliminated or effectively mitigated through adequate risk-mitigating measures and the allocation of appropriate resources. On this basis, the risk criteria relevant to the institution are defined, particularly for business relationships with increased risks.

In Guidance 05/2023 “Money laundering risk analysis pursuant to Article 25 para. 2 AMLO-FINMA” (hereinafter “Guidance 05/2023”), FINMA for the first time provided transparency regarding the observations and experiences gained in its supervisory practice with regard to risk analysis. Since then, FINMA has re-examined some of the risk analyses of over 30 banks inspected in spring 2023 and analysed those of numerous other banks and FinIA institutions[1] (hereinafter collectively referred to as “institutions”). FINMA concludes that the banks have made progress in defining their risk tolerance and in structuring their risk analysis. Some FinIA institutions are also already applying aspects of Guidance 05/2023 by analogy. Nevertheless, FINMA has identified further room for improvement at both banks and FinIA institutions, so that risk analysis can serve as an even more effective central control and management tool for combating money laundering.

This Guidance supplements previous observations and experiences and clarifies Guidance 05/2023 with regard to banks and FinIA institutions. The observations and experiences gained can be applied by analogy to the latter.

[1] Securities firms (Art. 41 FinIA), fund management companies (Art. 32 FinIA), managers of collective assets (Art. 24 FinIA), portfolio managers and trustees (Art. 17 FinIA)

1 Money laundering risk tolerance

The legal basis for banks' money laundering risk tolerance is set out in Guidance 05/2023.

The following legal principles are relevant to FinIA institutions in relation to the determination of risk tolerance: Article 9 para. 2 of the Financial Institutions Act of 15 June 2018 (FinIA; SR *954.1*), Article 12 para. 4, Article 26 para. 1, Article 41 para. 2, Article 57 para. 2 and Article 68 para. 2 of the Financial Institutions Ordinance of 6 November 2019 (FinIO; SR *954.11*) and Article 8 of the Anti-Money Laundering Act of 10 October 1997 (AMLA; SR *955.0*) require FinIA institutions to identify, control and monitor their money laundering risks (including combating terrorist financing) and to organise effective internal controls.

This chapter and the following chapters present the findings obtained since then, based on the observations set out in Guidance 05/2023.

Definition of risk tolerance

Observation pursuant to Guidance 05/2023:
a) Typically, the deliberate exclusion of certain countries, client segments, services and/or products (e.g. politically exposed persons from certain countries) is a necessary part of an adequately defined risk tolerance. However, such exclusions are often missing from the examined risk tolerances.

i. It was often observed that, rather than making deliberate exclusions, only risk-mitigating measures were described. *Example: "Foreign PEPs will only be accepted if they have an adequate KYC profile and the executive board has approved them."*

ii. Merely excluding inherent risks that must be omitted in any case is insufficient for an adequate definition of risk tolerance. *Example: One institution excludes North Korea, Iran and a small group of clients (drugs and human trafficking, proliferation).*

iii. Examples of deliberate exclusions in accordance with the relevant business model might include:

- No foreign PEPs
- No complex structures
- Certain countries that the institution does not wish to serve
- No clients from certain industries
- No crypto services
- No trade finance

iv. Institutions often fail to carry out a sufficiently documented assessment (low/medium/high) of their risk tolerance.

Exception to policy (hereinafter "ETP") process

Observation pursuant to Guidance 05/2023:
b) In most cases, there is also no suitable process to allow exceptions to the defined risk tolerance in individual cases (exception to policy process). Such exceptions are to be granted by the executive board after appropriate risk-mitigating measures have been defined. They are to be monitored by the board of directors.

i. On occasion, FINMA has come across institutions that have systematically exceeded the specified risk tolerance because their ETP process was not restrictive enough. This was evident, for example, in the very high number of ETPs approved. As a result, the defined appropriate risk tolerance was effectively ignored. The ETP process simply governs how, on a case-by-case basis, exemptions are granted for business relationships that fall outside the defined money laundering risk tolerance. In this context, there should be no provision for a defined risk limit to be exceeded generally or on a permanent basis. If a higher level of risk is to be deliberately accepted, this should be reflected in a corresponding adjustment to the risk tolerance by the board of directors.

ii. Some institutions have not documented their ETP cases centrally and do not monitor them adequately with regard to quantity (particularly with regard to number, volume and trends) and quality (particularly with regard to reasons, risk profiles, and the appropriateness and effectiveness of mitigating measures). Furthermore, there are isolated instances where ETP cases are not reported to the board of directors on a regular basis.

iii. By contrast, a few institutions stood out positively, as they do not allow any exceptions (ETPs) and strictly adhere to their clearly defined risk tolerance.

Key risk indicators

Observation pursuant to Guidance 05/2023:
c) Another finding was that no key risk indicators were defined that could be used to monitor compliance with the risk tolerance and enable the executive board and the board of directors to supervise it on a regular basis. The definition of the key risk indicators can be based on the risk limits defined in the risk analysis.

i. In a few cases, institutions equated the key risk indicators with the risk limits defined in the risk analysis (see no. 2.3 b). Key risk indicators are used to regularly monitor compliance with the risk tolerance. Accordingly, the focus should be on key figures that provide meaningful insights into the key risks. Not every existing risk limit should automatically be regarded as a key risk indicator. Rather, the institution should define its key risk indicators in a way that appropriately reflects the relevant risks.

ii. The following definitions of key risk indicators are not appropriate:

- Relative indicator values that are based on changes in risk compared with the previous year, as these effectively result in a gradual increase in risk tolerance without formal approval from the executive board.
- Indicators that relate to risks of varying criticality (low, medium and high), as this leads to a distortion of the findings and does not allow for a clear assignment to a defined criticality level, e.g. one indicator combines clients from countries with low, medium and high risk levels in an overall ratio without stating which clients come from countries with the low, medium or high level of risk.

iii. In some cases, institutions have defined key risk indicators solely for assessing the control risk and have not defined any key risk indicators for inherent risks. Examples of the latter might include:

- The number and assets under management (AuM) of business relationships with increased risks and politically exposed persons (PEPs), as well as persons closely associated with PEPs;
- Number of approved ETPs;
- Exposure in countries with increased risks outside the institution's target markets.

iv. To provide an accurate picture of a key risk indicator, several key figures should be used (typically: the number of business relationships and the amount of AuM) in order to provide a comprehensive view of the portfolio.

v. The levels of the defined limits for the indicators should be critically reviewed on a regular basis considering the defined risk tolerance and business strategy and adjusted where necessary. *Example: An institution that does not focus its business on PEPs and has a stated risk tolerance of "medium" sets a risk limit of up to 15% for PEPs.*

2 Money laundering risk analysis

The legal basis for banks' money laundering risk analysis is set out in Guidance 05/2023.

The following legal provisions are relevant to FinIA institutions: FinIA institutions are required to implement the organisational measures in accordance with Article 8 of the Anti-Money Laundering Act. These are set out in detail in Article 23 ff. of the FINMA Anti-Money Laundering Ordinance of 3 June 2015 (AMLO-FINMA; SR *955.033.0*) and include, in particular, the preparation and regular updating of an institution-specific risk analysis. The only exception to the requirement to create a money laundering risk analysis is where Article 75 para. 1 AMLO-FINMA[2] applies, provided that Article 75 para. 2 AMLO-FINMA[3] does not apply.

2.1 Money laundering risks to be considered

Comprehensiveness of the criteria to be considered and transparency of the assessment of individual risks

Observation pursuant to Guidance 05/2023:
a) It was frequently observed that the assessments regarding the inherent risk and the control risk, as well as the resulting net risk (residual risk), were not presented individually and comprehensibly for each identified money laundering risk of each money laundering risk category. In particular, it was observed that not all money laundering risks relevant to the institution were always covered.

[2] The conditions set out in Article 75 para. 1 AMLO-FINMA are that: a. the financial intermediary is a company which has five or fewer full-time employees or annual gross income of less than CHF 2 million; and b. it adheres to a non-high-risk business model.

[3] Where necessary to monitor compliance with the duties to combat money laundering and terrorist financing, FINMA may, on the basis of Article 75 para. 2 AMLO-FINMA, also require a financial intermediary that fulfils the requirements according to Article 75 para. 1 AMLO-FINMA to ensure that the competence centre for combating money laundering also fulfils the tasks specified in Article 25 AMLO-FINMA.

i. Institutions have not always considered in their risk analysis all the categories of money laundering risk (client segments, registered office/place of residence, products and services) specifically listed in Article 25 para. 2 of the AMLO-FINMA and which must be covered.

ii. Criteria with a medium or low inherent risk were often not considered in the risk analysis. Consequently, these institutions lacked the necessary overview of the risk exposure of their overall portfolio.

iii. In some cases, institutions grouped different levels of criticality for a single risk criterion together. However, such a grouping is unsuitable, as it does not allow for a clear assessment of the actual inherent risk associated with each individual criterion.
Examples: Despite differing inherent risks, retail, affluent and high-net-worth clients were grouped together under the heading "Level of assets". Similarly, countries with low, medium and high inherent risk were grouped together under the heading "Country risk (client's registered office/place of residence)", rather than being reported individually according to their criticality.

iv. Some wealth management banks with a high or very high risk tolerance use risk criteria that are not granular enough. In particular, country risks relating to the registered office or place of residence of clients are not reported at the level of individual countries, but are aggregated. Depending on the business model, categorising countries by criticality may be sufficient where risk tolerance is lower.

v. Retail banks are increasingly offering bespoke services to high-net-worth private clients. This higher inherent risk was often not taken into account in the risk analysis with a correspondingly higher level of detail.

vi. In some cases, institutions did not adequately assess the inherent risk associated with individual money laundering risk criteria in terms of their criticality:
- Complex structures with an inherent risk rating of "medium" rather than "high";
- PEPs with an inherent risk rating of "medium" rather than "high";
- Crypto services with an inherent risk rating of "medium" rather than "high".

vii. Common reasons for an inadequate assessment of the inherent risks include:
- Risk-mitigating measures are considered in relation to inherent risks, even though they fall under control risk;

- Risk tolerance is already considered in relation to inherent risks, although it must be managed through risk limits and by ensuring that net risk is in line with the tolerance (see no. 2.3 b).

viii. In some cases, net risks are not determined correctly. Regarding the correct determination of the amount of net risk, please refer to Annex 3 of the FINMA Regulatory Auditing Ordinance of 31 October 2024 (SR *956.161.1*). *Example: A net risk was incorrectly reported as "low" rather than "medium" for a money laundering risk criterion with an inherent risk of "high" and a control risk of "low".*

ix. In some cases, institutions are unaware that, in accordance with Annex 3 of the FINMA Regulatory Auditing Ordinance, very high inherent risks cannot be reduced to a level lower than "high" even through the implementation of effective risk-mitigating measures.

Description of risk-mitigating measures (control risk)

Observation pursuant to Guidance 05/2023:
b) In order to understand how risk-mitigating measures (control risk) affect inherent risks, they must be described in sufficient detail. To demonstrate their effectiveness, key figures, findings regarding the effectiveness of the controls carried out (controls of controls), etc. should be used for this purpose.

i. In some cases, the risk-mitigating measures were described only by means of a general reference to internal directives and processes. This does not allow for a sufficient understanding of the specific measures envisaged. Risk-mitigating measures should either be described in detail or accompanied by a reference to specific controls in the institution's control inventory.

ii. In several instances, only confirmation that controls had been carried out was documented, and no key figures on the effectiveness of the controls were used. An example of a key figure for the effectiveness of the controls carried out might be: *"Deficiencies in documentation were found in 5% of the monthly spot checks carried out by the Compliance department as part of transaction reviews, but in none of these cases was there any evidence of a breach of reporting requirements."*

2.2 Implementation of the requirements according to Article 13 para. 2bis AMLO-FINMA

FINMA's findings and experience were consistent with those already set out in Guidance 05/2023.

2.3 Monitoring compliance with the business strategy and risk policy

Definition of key figures

Observation pursuant to Guidance 05/2023:
a) It was regularly noted that no key figures were defined to determine how large the respective risk exposure is in the bank's client population and range of services and to what extent compliance with the business strategy and risk policy is ensured.

i. In some instances, the risk analysis used only a few key figures to illustrate the risk exposure of individual risk criteria within the overall portfolio; for example, only the ratio of AuM to the total portfolio. A combination of several key figures, on the other hand, is more meaningful. At a minimum, the AuM and the number of client relationships should be taken into account – both in absolute terms and in relation to the total portfolio.

ii. On occasion, risks of varying severity were combined into a single key figure. However, this does not allow for any conclusions to be drawn regarding the risk exposure of individual criticalities.

Defiition of risk limits

Observation pursuant to Guidance 05/2023:
b) Often there is no definition of risk limits for monitoring risk tolerance so that appropriate measures can be taken if the thresholds are not met.

i. In some cases, risks were monitored using limits based on year-on-year growth. However, such an approach does not allow for a proper assessment of risk exposure in relation to the total portfolio (see also no. 1 c.) ii).

ii. In isolated cases, an ETP authorisation was granted for instances where risk limits were exceeded, which does not appear to be appropriate from a risk management perspective. Rather, in the event of non-compliance with the thresholds, appropriate risk-mitigating measures should be planned and implemented to ensure compliance with the risk tolerance.

Aligning net risks with risk tolerance

Observation pursuant to Guidance 05/2023:
c) Net risk (residual risk) was often not compared with the risk tolerance. Such a comparison is necessary to take measures in case of non-compliance with the risk tolerance.

i. Increasingly, institutions have calculated a net risk for each money laundering risk and compared this with the risk tolerance. However, they have not aggregated these into an overall money laundering risk. Consequently, no meaningful comparison was made between the total net risk and the established money laundering risk tolerance.

ii. It was also noted that no action was taken when the risk tolerance threshold was exceeded. If the net money laundering risk associated with an individual risk criterion, or the overall net risk, exceeds the defined tolerance level, risk-mitigating measures must be taken with the aim of bringing the risks back within the tolerance range.

2.4 Other elements to consider

Changes in risks

Observation pursuant to Guidance 05/2023:
a) Often, the changes in risks (inherent risks, control risk and net risks) compared to the previous year were not apparent and comprehensible in the risk analysis, although these help to determine the measures needed to manage and monitor the risks.

In some cases, the development was not presented in a way that was clear for all risks (inherent risks, control risks and net risks).

Resource analysis

b) It was often found that the qualitative and quantitative resources required to ensure the implementation of the bank's anti-money laundering processes were not critically examined so that they could be adjusted if necessary.

The qualitative and quantitative analyses of resources should be supported by appropriate key figures that facilitate the monitoring of these developments.

3 Relationship to margin no. 78 of FINMA Circular 2017/1 "Corporate governance – banks"

The money laundering risk analysis pursuant to Article 25 para. 2 AMLO-FINMA should follow a different methodology to that used for the compliance risk analysis. The compliance risk analysis focuses on the risk of non-compliance with statutory, regulatory and internal requirements (risk of non-compliance) and the resulting supervisory, financial and reputational consequences. By contrast, the money laundering risk analysis assesses the risk that an institution might be misused for money laundering or terrorist financing because of its business activities, client relationships or transactions (risk of misuse).

These differing objectives require different approaches both to identifying the inherent risks and to assessing them. The identification and assessment of inherent risk as part of the money laundering risk analysis must, in accordance with Article 13 para. 2 AMLO-FINMA, be carried out in a consistent manner across all institutions. The assessments of relevant international specialist organisations (e.g. the Financial Action Task Force, the Wolfsberg Group) may also be used as a guide in this regard.

The calculation of net risk is based on this consistent framework for assessing inherent risk. This results from a combination of inherent risk and control risk. For the correct calculation of net risk, please refer to Annex 3 of the FINMA Regulatory Auditing Ordinance.

4 Global monitoring of money laundering risks

No further comments are made regarding the relevant points set out in Guidance 05/2023.

5 FinIA institutions

The observations and findings set out in this guidance may be applied by analogy to FinIA institutions. These must be implemented taking into account an institution's actual risk exposure. The level of detail and the structure of the risk analysis should be determined by the nature, scope, complexity and risk profile of the institution's business activities. The higher the inherent risks to which an institution is exposed, the more detailed the risk analysis must be. This should be taken into account in particular

- when determining the number and structure of the key risk indicators used (see no. 1 c) iv.) and
- when determining the granularity of the money laundering risks to be considered (see no. 2.1 a) iv.). A FinIA institution that, by virtue of its activities, is not exposed to increased money laundering risks is not required to break down country (domicile) or sector risk into individual countries or sectors. Similarly, services can be grouped into broad categories according to their criticality, without the need for a detailed breakdown (e.g. traditional asset management services: low/medium/high; other ancillary activities: low/medium/high).