



PRIORITIES AND TRENDS  
2024

PREVENTION OF MONEY  
LAUNDERING AND  
TERRORISM FINANCING

## CONTENTS

<i>Legal Notice (IMPRESSUM)</i> .....	3
1 Summary of material findings .....	4
2 The FMA’s role in the AML/CFT Framework .....	5
3 Topics and Focus of Activities 2024.....	8
3.1 Risk-based supervision .....	8
3.1.1 Operative supervisory activities in the area of prevention of AML/CFT.....	9
3.1.2 Observations by the supervisory authority.....	11
3.1.3 Administrative penal proceedings in the area of prevention of ML/TF.....	14
3.2 AML Colleges .....	16
3.2.1 Home Colleges .....	16
3.2.2 Host colleges .....	17
3.3 EstablishING the EU Anti Money Laundering Authority (AMLA).....	17
3.4 FMA representation in international and European committees.....	19
3.4.1 EGMLTF .....	19
3.4.2 FATF.....	19
3.4.3 AMLSC .....	19
3.5 Legal interpretation and regulatory developments.....	21
3.5.1 The FM-GwG’s “New” CASP regime.....	21
3.5.2 Legal questions about the FM-GwG.....	22
3.6 Market trends.....	23
3.6.1 Number and Breakdown of Obligated Entities .....	23
3.6.2 “top three” risk factors .....	32
3.6.3 Business relationships with correspondent banks in third countries, Russia and Belarus .....	33
3.6.4 Business relationships to Russian/Belarusian customers; beneficial owners domiciled in Russia/Belarus.....	34
3.6.5 Outsourcing: Credit Institutions sector.....	35
3.6.6 Cross-border transactions.....	36
4 Outlook.....	39

*Legal Notice (IMPRESSUM)*

*Published by: Austrian Financial Market Authority (FMA)*

*Otto-Wagner-Platz 5, A-1090 Vienna*

*Telephone: +43-1-249 59-0, Fax: +43-1-249 59-5499*

*E-Mail: [fma@fma.gv.at](mailto:fma@fma.gv.at)*

*[www.fma.gv.at](http://www.fma.gv.at)*

*Sources (unless stated otherwise): FMA:*

*Errors and omissions excepted.*

# 1 SUMMARY OF MATERIAL FINDINGS

**This report presents the material issues, developments and trends in the prevention of money laundering and terrorist financing (ML/TF) in 2024 from the FMA's perspective.** It draws in part on the findings from the FMA's activities as supervisory authority (e.g. from on-site inspections or investigative proceedings). In addition, the report contains analysis from the relevant data collected by the FMA from supervised entities at least annually. Furthermore, the report provides an insight and overview into material regulatory developments, based on the FMA's involvement at both national and international level.

**The FMA approach to supervision in relation to prevention of money laundering and terrorist financing (ML/TF) is a consistent, risk-based and integrated one.** In 2024, during its ongoing operative supervision, the FMA conducted 20 on-site inspections, 20 on-site examinations and 11 management talks. In addition, 78 investigative procedures and 12 procedures to restore legal compliance, and four virtual asset service provider registration procedures were initiated. In 11 cases, key function holders were subjected to fit and proper tests in relation to ML/TF during the reporting year. Furthermore, six home AML colleges were established, with the FMA also being invited to participate in AML colleges on 26 occasions by sister authorities. 44 (first instance) administrative penal proceedings were initiated in 2024 in the field of prevention of ML/TF, with penal orders being issued in 13 instances.

**The FMA's zero tolerance policy regarding ML/TF was demonstrated on several occasions in 2024:** severe breaches of the FM-GwG were determined in two procedures conducted regarding correspondent banking relationships. In the first case, the FMA imposed a fine of EUR 2,070,000, while a fine of EUR 791,000 was imposed in the latter case. In addition, the FMA imposed several supervisory measures upon European American Investment Bank AG for severe breaches of the FM-GwG: these measures ultimately led to the European Central Bank withdrawing the bank's licence (not legally effective).

**To ensure targeted use of resources under the risk-based approach, the FMA also conducted a comprehensive risk assessment of the obliged entities in the Austrian financial market in relation to ML/TF risks in 2024.** As a result, only a low percentage (2.5 %) of the credit institutions (CIs) sector are exposed to a high risk of being misused for the purposes of ML/TF. Most CIs fall into the "low" or "medium" risk categories. In 2024, no undertakings in the insurance sector (IUs) were categorised as "high risk" - for the first time since 2021. Just under one-third of IUs were categorised as medium risk. VASPs portray a different situation: the number of undertakings classed as "high" risk remained unchanged in absolute terms, although the number of undertakings within the sector has fallen, leading to a relative increase to 33.3% (plus 12 percentage points) being in the "high risk" category. A further third of VASPs are categorised as being at "medium risk". Payment institutions (PIs), investment firms (IFs) and investment service providers (ISPs), as well as investment fund

management companies/alternative investment management funds (MCs/AIFMs), appear to have a lower level of risk: no entity from these sectors were allocated in the “high risk” category.

**Data collected annually from obliged entities allows the FMA to derive risk trends for its risk classification.** This data shows, for example, that there has been a strong decline of correspondent banking relationships with a link to Russia and Belarus or business relationships with customers (natural/legal persons) or the beneficial owners of legal persons resident in these countries since 2019 (also prior to the enforcement of sanctions associated with Russia’s war of aggression against Ukraine). Such developments appear representative of the general trend in the banking sector towards an increasing reduction of risk. In particular, banks are increasingly retreating from markets in which they were active in countries where international embargoes are in place, or in countries on the FATF’s grey list. Stricter regulatory requirements and the associated administrative burden have led banks concentrating their business relationships on safer, more transparent markets, while also withdrawing from high-risk regions.

**Increasing numbers of insolvencies in the real estate sector in 2024, have shown that real estate transactions become an area of focus for the FMA** and have revealed significant AML risks. Opaque ownership and shareholding structures in particular make it more difficult to identify beneficial owners and trace the origin of funds. Obligated entities under the FM-GwG’s scope are therefore required to increasingly consider risk factors like complex company structures, family offices or unclear sources of financing. Detailed Know Your Customer (KYC) reviews, comprehensive documentation and plausibility assessment are essential. In addition, intensive and regular staff training are necessary to detect risk factors at an early stage and address them appropriately.

**2024 saw the finalisation of the EU’s AML Package following intensive political negotiations.** The package consists of the new Anti-Money Laundering Regulation (AMLR), the revised Anti Money Laundering Directive (AMLD) and the Regulation establishing the Anti-Money-Laundering Authority (AMLAR). AMLA’s operative activities are planned to begin in 2025, while direct supervision of 40 of the highest risk and cross-border institutions or financial groups is scheduled from 2028. The FMA is actively involved in AMLA’s establishment and is supplying expertise. Incorporating the non-financial sector into the new system of supervision as well as ensuring efficient data-driven supervision represent material challenges in establishing the new European system for AML/CFT supervision.

## 2 THE FMA’S ROLE IN THE AML/CFT FRAMEWORK

**Combating of ML/TF is a central objective for the FMA, which has adopted a consistent zero-tolerance policy for many years.** Austria’s financial market participants must first and foremost take preventative measures, such as checking customers’ identity and conducting plausibility checks regarding flows of funds to prevent the financial system from being misused for the purpose

of disguising and shifting of assets of an illegal origin as well as making assets (also legal ones) available for terrorist activities. The FMA requires all financial market participants to act in a legally compliant manner and make a sustained impact towards the required changes in conduct. The FMA uses supervisory tools and sanctioning powers at its disposal in the event of breaches of legal obligations. Breaches are punished with the due degree of severity.

Various authorities and institutions in Austria work together regarding AML/CFT.

- FMA
- The Financial Intelligence Unit (*Geldwäschemeldestelle*) of the Criminal Intelligence Service Austria (A-FIU)
- Directorate National Security and Intelligence Service (DSN)
- Federal Ministry for Justice (BMJ)
- Federal Ministry of Finance (BMF)
- Oesterreichische Nationalbank (OeNB)
- other ministries, other regional authorities, and chambers.

**AML/CFT is a complex and international issue, based on close cooperation between many national and international authorities and institutions.** At national level, the FMA cooperates closely with other supervisory or law enforcement agencies as well as academic institutions and increasingly assumes the role of an AML/CFT competence centre and information hub in addition to that of the competent authority. Its objective is to further promote networking with national and international AML/CFT players, to help in preparations to establish the future European AML supervision system headed up by AMLA – including the FMA’s role within this supervisory system.

**Pooling of data and information from different sources makes AML/CFT more effective.** The FMA therefore pursues a data-driven supervisory approach, including the pooling of ML-relevant information from various sources (from supervised entities, the A-FIU, other authorities etc.), to allow it to be used for official activities and risk analyses – and which can increasingly be prepared by automated means.

**The FMA supervises AML/CFT compliance with the obligations in the FM-GwG.** Under Article 1 para. 1 FM-GwG, the FMA is competent for the supervision of credit institutions, financial institutions and virtual asset service providers (VASPs). Obligated entities also include investment fund management company (MCs), insurance undertakings (IUs), corporate provision companies (CPCs), investment firms (IFs) and investment services providers (ISPs), payment institutions (PIs), electronic money institutions, alternative investments fund managers (AIFMs), as well as the branches and branch establishments of EEA institutions of such entities registered in Austria, in addition to classical credit institutions and financial institutions (CIs and FIs) under the Austrian Banking Act (BWG; *Bankwesengesetz*). In this context, the FMA checks that they are compliant with

AML/CFT due diligence obligations. Where such obligations are breached, the FMA takes necessary steps.

**The FMA's supervision of Austrian financial market participants regarding AML/CFT is conducted on a cross-sector basis by a single division within the "Integrated Supervision and Innovation Department"**. This division conducts on-site measures and official supervisory administrative proceedings, represents the FMA in national and international committees and also provides AML/CFT-related legal interpretation. Furthermore, since 2020, the division's scope of competence has also included the registration (market entry) of and "AML supervision" for VASPs. Where the FMA suspects during its ongoing supervisory activities that a transaction is made for ML/TF purposes, it submits a suspicious activity report to the A-FIU, which in turn analyses the report from a criminal law perspective, and where applicable also cooperates directly with the law enforcement authorities.

**The FMA pursues a risk-based approach to supervision in accordance with the EU Anti Money Laundering Directive (AMLD) and its transposition in the FM-GwG.** This approach applies across all levels from legislation through its application by obliged entities through to the planning of FMA supervisory measures (see Chapter 3.1.). The European Commission, EU Member States, competent (national) authorities and obliged entities are required to identify, evaluate and understand AML/CFT risks and to take appropriate risk mitigation measures. When drawing up their risk assessment at entity level, obliged entities are required to incorporate the National Risk Assessment (NRA), which contains the ML/TF risks that exist in Austria, also taking into account the risks contained in the European Commission's Supranational Risk Assessment (SNRA) on ML/TF risks in the Single Market.

## 3 TOPICS AND FOCUS OF ACTIVITIES 2024

The FMA's broad scope of activities including the various thematic focuses in the area during 2024 of AML/CFT is as follows:

### 3.1 RISK-BASED SUPERVISION

**The FMA monitors compliance with obligations listed in the FM-GwG in a risk-based manner in accordance with its legal mandate.** In practice, the FMA conducts a data-based risk classification of the obliged entities. In doing so, the FMA takes into account:

- the information collected annually from the obliged entities by means of questionnaires
- supervisory perceptions (e.g. from on-site inspections, investigative proceedings etc.)
- additional internal and external data (e.g. transaction data, shareholding structures)

**This data is the basis for calculating the risk classification.** A number of factors affect the calculation, for example: customer structure, transaction volumes, the proportion of transactions in cash etc. Entities classified as "high risk" include obliged entities that display a large number of factors that increase the degree of risk or where the supervisory authority has raised critical observations. Subsequently, the risk category is used to plan the FMA's on-site measures, leading to a higher frequency of inspections for "high risk" obliged entities.

**The risk classification of obliged entities is updated annually.** This allows supervision to be concentrated on those entities and areas where an elevated risk of ML/TF is identified and where more stringent requirements exist for preventive work. Ad hoc adaptations are also possible on a case-by-case basis, for instance were necessitated by current official observations or media reporting.

**In addition to objective inspection planning, the risk classification also guarantees that priorities for supervision and inspections are regularly adapted.** The "AML App" has been specially developed for the obliged entities' annual risk classification and provides the FMA with a comprehensive 360-degree view of individual obliged entities and forms the objective and risk-based basis for data-driven supervision using risk scores. Trends, risk factors and other relevant parameters may also be detected and analysed on an aggregated basis, which also facilitates the regular adjustment of priorities for supervision. The data pool and the results that emerge feed into the preparation and follow-up work for specific on- and off-site supervisory measures. The AML app is being developed further on an ongoing basis.

In 2024, the FMA conducted its first separate **sectoral risk assessment** to analyse ML/TF risks in individual sectors within the Austrian financial industry in greater detail both systematically and on a sector-specific basis. Its objective was to identify new developments and specific risk factors and to adapt existing measures in a targeted manner to the respective sectoral specificities.

Austria's financial market is marked by its high level of diversity. Its diversity is accompanied by different risk profiles, and vulnerabilities of a both structural and technological nature for ML/TF form part of its diversity. Some sectors display specific vulnerabilities due to their international interconnectedness, complex financial products or digital business models, while additional challenges arise due to the interfaces between market participants. Specific risk factors have been identified in particular in areas with a high degree of digital integration, such as in payment transactions or virtual assets, which impact the transparency and traceability of financial flows. In addition, the analysis reveals that considerable progress has already been made in terms of awareness and prevention due to stricter regulatory measures and close cooperation with market participants.

The following sub-chapters form an overview about the FMA's supervisory activities regarding the prevention of ML/TF both on- and off-site, as well as the material findings that emerged in 2024:

### 3.1.1 OPERATIVE SUPERVISORY ACTIVITIES IN THE AREA OF PREVENTION OF AML/CFT

The following table contains an overview about the FMA's operative supervisory activities and official supervisory measures and procedures in 2024 regarding AML/CFT:

Operative supervisory activities	Quantity		
	2022	2023	2024
Investigative proceedings	165	39	78
On-site inspections	22	20	20
On-site examinations	19	22	20
Management talks	8	6	11
Administrative proceedings to restore legal compliance	4	10	12
Fit & Proper Tests in accordance with FM-GwG	8	11	11
Registration procedures under Article 32a FM-GwG (initial applications)	11	8	4

Table 1: Overview of operative supervisory activities

**In 2024, the FMA initiated 78 investigative proceedings in the area of AML/CFT.** A decline in numbers of investigative proceedings since 2022 can primarily be attributed to obliged entities' increased awareness about the phenomenon of "financial agents" (known as "money mules"/ or breaches of trust under the FM-GwG), their better calibrated monitoring systems and higher quality suspicious activity reports permitting the particularly efficient and bundled processing of relevant issues by the FMA. This is ultimately reflected in the number of internally initiated investigations and their more efficient handling at the FMA. In addition to official observations, further reasons for initiating investigative procedures include external information from whistle-blowers, customers or other authorities. The Austrian Financial Intelligence Unit (A-FIU) forwarded 18 analysis reports to

the FMA during the reporting year for the suspected failure to disclose a trust relationship or suspected money laundering.

**The FMA conducted 20 on-site inspections regarding compliance with the FM-GwG in 2024.**

Obligated entities were selected in a risk-based manner using data-driven planning and expert analysis. Large amounts of information were requested and analysed prior to inspections, to determine which inspection modules to focus on. On-site, the FMA checks systemic rules and how they are implemented in specific cases. 13 out of the 20 inspections were conducted at CIs, four at VASPs, two at IUs, and one at an ISP. Their primary focus on the banking sector, with a secondary focus on VASPs in reaction to their elevated risk.

**In addition, 20 on-site examinations were conducted.** These shorter or less in-depth on-site measures conducted at obliged entities' premises also checked their compliance with the provisions in the FM-GwG. Twelve were conducted at CIs, as well as one examination each respectively from the sectors IUs, PIs and electronic money institutions. Four examinations were conducted for ISPs.

**Further, the FMA held 11 management talks.** Specific or event-related current issues are discussed with the obliged entities during such management talks, either held on-site or at the FMA's premises. Here the focus was again on banks and VASPs.

**During the reporting year, 12 proceedings to restore legal compliance) were initiated.** These are official procedures with the purpose of restoring legal compliance, following a breach of FM-GwG provisions being determined to have occurred. These proceedings are only initiated in instances where FM-GwG breaches were determined of a nature and scope that require a separate official procedure to rectify the breach. While the FMA naturally determined instances with potential for improvement or breaches during the reporting year more frequently, most identified cases did not lead to the initiation of separate proceedings to restore legal compliance where legal compliance is frequently already established during, or directly after, an on-site measure or investigative procedure.

**Moreover, the FMA conducted 11 Fit & Proper tests of AML officers in 2024,** to check their personal and professional fitness and propriety regarding FM-GwG provisions. The increased use of Fit & Proper tests since 2022/2023 in the context of the registration of VASPs, or for new appointments of AML officers, also corresponds with the FM-GwG's underlying prevention principle. Relating theoretical knowledge and its practical implementation is equally relevant for being able to answer questions fully as the questions regarding knowledge about the FM-GwG and the Beneficial Owners Register Act (WiEReG; *Wirtschaftliche Eigentümer Registergesetz*).<sup>1</sup>

---

<sup>1</sup> In addition to these Fit & Proper tests, under the integrated approach to supervision, the Division for the Prevention of ML/TF also participates in F&P meetings and management talks with directors, chairpersons of supervisory boards and key function holders within the scope of prudential supervision. This happened on six occasions during the reporting year.

### 3.1.2 OBSERVATIONS BY THE SUPERVISORY AUTHORITY

**It is necessary from the outset to state that obliged entities supervised by the FMA under the FM-GwG as a rule satisfy high standards regarding the prevention of ML/TF.** Nevertheless, supervisory observations (“findings”) do arise during the FMA’s operational supervision in relation to potential for improvement or breaches in applying the provisions of the FM-GwG. Some current findings are summarised below.

**Technological developments are altering the framework of the financial market: while increased digital transformation opens new business areas and opportunities, there are also new risks.** The case of transactions concluded online, which is becoming increasingly popular, demonstrates this clearly regarding the prevention of ML/TF. For customer identification and verification purposes (for natural persons), the FM-GwG generally requires official photo identification documents pursuant to Article 6 para. 2 no. 1 FM-GwG to be presented in person but also permits the presentation of an official photo identification document to be substituted by safeguards pursuant to Article 6 para. 4 FM-GwG for business relationships or transactions without personal contact (non-face-to-face business). Online identification constitutes one of the generally permissible safeguards. The unambiguous and secure identification of customers, as part of the KYC procedure, forms a particularly key measure in the area of AML/CFT. Practical problems encountered in conjunction with online identification procedures, such as using forged identification documents are a good illustration of the potential risk from technological developments. Additionally, obliged entities are required to carefully select a trustworthy provider and to ensure that all necessary information is obtained to comply with the due diligence obligations under the FM-GwG. Under the risk-based approach, in addition to the minimum information stipulated under law (for example, the features of the identification document) it usually will be necessary to provide supplementary information, such as the address at which someone is registered. Obligated entities are required to conduct suitable internal (quality) checks to mitigate the risk of being misused for ML/TF purposes to guarantee that statutory requirements are observed.

**The inspections focus in relation to VASPs clearly demonstrates the many challenges this sector faces in 2024, since due diligence obligations for the prevention of ML/TF have only applied to them since 2020.** Room for improvement exists in this very heterogeneous group (there are significant differences in terms of the size of entities, the scope and complexity of the products offered, number of customers etc.) of obliged entities, especially regarding their understanding of risk, implementation of the risk-based approach and adequate technical and staffing resources. The FMA’s supervisory measures in this area in 2024 again addressed this, as they had done so in previous years. In addition, there was a particular focus on “shell registrations”, where service providers hold a valid registration from the FMA pursuant to Article 32a FM-GwG but have never performed any kind of operative activity. This type of registration (being operationally inactive and therefore not having any knowledge about an actual customer structure, marketed products, distribution channels, and

cooperation partners) is generally not intended, as such a registration does not permit checking of the applicability of strategies, procedures and processes in operative business, and actual ML/TF risk is unable to be conclusively assessed, thereby preventing ML/TF supervision. The FMA's consistent approach in this regard, has led to a significant decrease in the number of registrations. While 25 VASPs were registered with the FMA in December 2022, in both 2023 and 2024 the number of registrations has fallen by four service providers each year. 13 VASPs remain registered as of 30.12.2024, the date of application of the Markets in Crypto Assets Regulation (MiCAR), on which date registration under the FM-GwG also ceased. The figure below shows an initial strong increase in registered VASPs followed by a constant reduction since December 2022, due to registrations being relinquished or de-registrations. It also demonstrates the last four years' high volatility regarding registered VASPs.

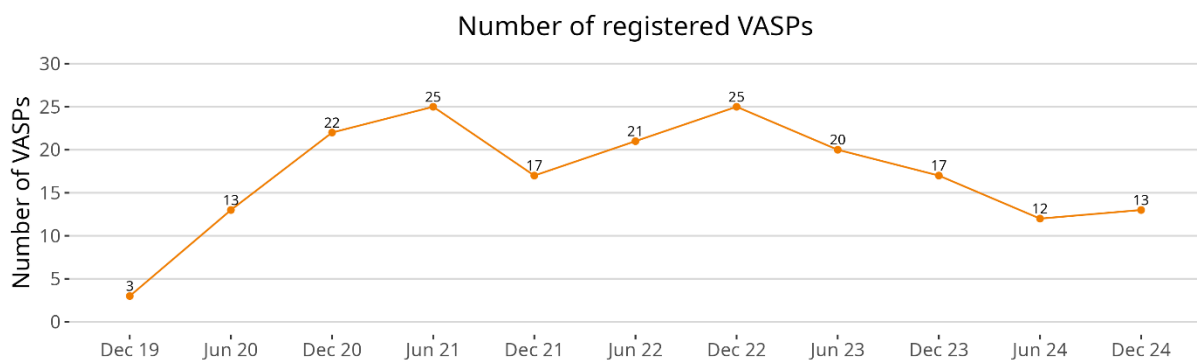


Figure 1: Number of registered VASPs

**ISPs and IFs belong to the group of obliged entities under the FM-GwG**, although, as the National Risk Assessment (NRA) results indicate, the risk of being misused for the purposes of ML/TF is lower in comparison, due to their business models tending to be less risk-prone. Significant risks nevertheless exist due to their role in the financial market and the use of external agents. To comply with the FM-GwG also requires ISPs/IFs to take comprehensive preventive measures, including a risk assessment at both enterprise and individual client level, having an appropriate AML function, and the risk-based application of due diligence obligations, above all including the checking of customers, transactions and the origin of funds. Due to their close contact to customers, ISPs/IFs pay a central role in identifying suspicious activities, which is why control and reporting systems are essential for the early detection of anomalies and for making suspicious activity reports in accordance with legal provisions. In 2024, the FMA intensified its dialogue as well as its on-site measures for checking the preventative measures taken within this sector. It focused on checking the adequacy and suitability of the systems, controls and procedures in use at ISPs/IFs for complying with the FM-GwG. A risk-based approach tailored to respective business models and client structures is essential for ISPs/IFs to meet their obligations. The financial system and its participants' ML/TF risk can only be minimised by consistent interaction between all market participants, supervisory and law enforcement authorities, thereby ensuring the financial market's integrity.

**In 2024 the FMA prioritised the prevention of terrorist financing.** Terrorist financing (TF) generally means making available or collecting legal or illegal financial means for conducting criminal offences of a terrorist nature. The FM-GwG also prescribes corresponding preventive measures and due diligence obligations for preventing TF to prevent the financial system from being misused. During on-site measures, the FMA in particular observed deficiencies in the adequate consideration of terrorist financing risk in the risk assessment at both enterprise and individual client level, inadequate internal guidelines, as well as a lack of staff training measures. To effectively prevent TF, obliged entities must analyse the risk for TF, define relevant risk factors and consider them in customers' risk classification. Implementing special strategies, controls and procedures, including appropriate monitoring for (groups of) customers with an elevated risk, as well as dedicated training measures for staff members for recognising unusual transactions are crucial for understanding the specific risks, and for identifying and preventing potential abuse at an early stage.

### 3.1.3 ADMINISTRATIVE PENAL PROCEEDINGS IN THE AREA OF PREVENTION OF ML/TF

Administrative penal proceedings/penal orders	Quantity	
	2023	2024
(First instance) administrative penal proceedings initiated	48	44
Penal orders	10	13

Table 2: Administrative penal proceedings

**The FMA stringently monitors the observance of due diligence obligations for the prevention of ML/TF. FM-GwG breaches are consistently punished.** In 2024, the FMA initiated 44 (first instance) administrative penal proceedings in the field of prevention of ML/TF. This figure also includes procedures initiated against accountable persons when pursuing the legal person. Penal orders were issued in 12 cases. Of these, nine cases related to CIs and their branches in Austria, and three cases related to VASPs. Fines totalling approx. EUR 4,331,080 were imposed. In pursuing breaches, the FMA focuses on missing or deficient strategies, checks and procedures (Article 23 FM-GwG).

In two cases FM-GwG breach procedures were in relation to correspondent banking relationships. In the first case, the FMA imposed a fine of EUR 2,070,000 because the correspondent institution, in executing payments for two respondent institutions domiciled in a third country, failed to convince itself about the adequacy of checks undertaken by the two respondent institutions for the prevention of ML/TF. In the second case, a fine of EUR 791,000 was imposed because the correspondent institution failed to gather adequate information and proof about the origin of funds invested in the investment accounts managed by the respondent institution acting as a trustee for its customers, and because the correspondent institution had failed to subject the payment accounts held for the respondent institution to adequate risk-based ongoing monitoring.

In one instance, a credit institution received an additional fine of EUR 476,000 for failing to take appropriate measures to understand the ownership and control structure of a high-risk customer, thereby not permitting it to be certain of the identity of the high-risk customer's beneficial owner. In a further case, the FMA imposed a fine of EUR 588,000 upon a CI for its failure to classify three business relationships in an appropriate risk category.

In all four cases, non-legally effective penal orders being issued were published on the FMA website pursuant to Article 37 para. 1 FM-GwG.

In addition, the third instance, the Federal Administrative Court (BVwG; *Bundesverwaltungsgericht*) again upheld the guilty verdict returned by the FMA against a CI for deficiencies in checking the identity of beneficial owners of high-risk customers and irregular updating of documents, files and information in the case of high-risk customers with minor conditions, while also reducing the fine imposed by the FMA from EUR 2,748,000 to EUR 1,978,560.

**In addition, during the FMA's intensive supervision of the European American Investment Bank AG (Euram Bank) several measures were taken based on repeated and severe breaches of the FM-GwG.** Numerous AML/CFT deficiencies had already been determined across the board during an FMA on-site inspection in 2022 at Euram Bank. Euram Bank was therefore ordered to establish legal compliance, a governance-related measure was also enforced, and an administrative penalty and other sanctions also imposed. Despite such measures, Euram Bank failed to make adequate progress in 2023 to rectify these deficiencies. From the FMA's perspective, an acute danger existed that transactions were being conducted through Euram Bank for money laundering purposes. On 16.01.2024, Euram Bank was therefore ordered by means of an administrative decision to establish legal compliance, and a ban on new business was imposed until legal compliance was established, and transaction checking ordered for transactions that were permitted. These measures' objective was to reduce the existing risk of money laundering as much as possible during the period in which the bank was rectifying the deficiencies.

Ongoing follow-up activities in 2024 by the FMA, constantly showed, both regarding the prevention of money laundering as well as in other areas of supervision, that Euram Bank had failed to adequately rectify the deficiencies and that the checks ordered on transactions were also not being performed in an orderly manner.

Due to financial developments at Euram Bank, the FMA determined a need for early intervention under the Bank Recovery and Resolution Act (BaSAG) and appointed a temporary administrator on 16.08.2024. This was also necessary due to the bank's late submission of documentation in relation to its annual financial statement for 2023.

The FMA intensified its supervisory activity following the determination of the need for early intervention. An administrative decision ordered the bank to convene an extraordinary general meeting at which a resolution was required to be passed to either conduct a capital increase of at least EUR 25 million, or to opt for voluntary wind down. At the EGM, the bank's owners decided to liquidate the bank.

Due to Euram Bank's continuing unfavourable financial developments, on 16.10.2024, the FMA issued an administrative decision, in which it appointed a government commissioner and prohibited the bank from conducting business operations, thereby triggering a deposit guarantee pay out event. The A-FIU and the deposit guarantee scheme were both active as a result of the severe deficiencies determined by the FMA. *Deposit Protection (Einlagensicherung Austria (ESA))* was forced to suspend the repayment of covered deposits under ESAEG, to allow the A-FIU to first of all review deposits regarding the suspicion of ML/TF. During the A-FIU's analysis, relevant information emerged resulting in the A-FIU forwarding the results of its analysis to the competent public prosecutor's office.

Subsequently, Euram Bank notified the FMA about being overindebted due to an increased need for write-downs. Euram Bank failed to meet the conditions for resolution under the BaSAG regime,

especially due a lack of public interest in a resolution. On 06.12.2024, the FMA therefore lodged its application to open insolvency proceedings at the Commercial Court in Vienna (*Handelsgericht Wien*), which were opened with effect from 11.12.2024. In its capacity as competent authority for licence withdrawals, ECB withdrew Euram Bank's banking licence at the FMA's order on 13.03.2025 due to the bank's insolvency and the long-term and severe AML/CFT irregularities. This decision took effect on 14 March 2025, but (as of April 2025) is not yet legally final, since the possibility remains to appeal against the decision.

## 3.2 AML COLLEGES

**Since 2021, the FMA has established AML colleges as the lead supervisor for Austrian obliged entities active on a cross-border basis that have set up establishments in at least two other Member States (home colleges).** An AML college is a cooperation platform consisting of supervisory authorities from different member states for the purpose of joint monitoring and information exchange for combating ML/TF. EBA Guidelines on ML/TF Colleges (AML colleges) have created a framework for cooperation and exchanging information regarding the combating of ML/TF between the competent authorities by means of bilateral agreements and colleges.

**In addition to establishing and participating in AML colleges, the FMA started an initiative in 2024 to request EBA to conduct missing equivalence checks (checking of equivalence of confidentiality and professional secrecy regimes) from sister authorities in third countries.** Without such a check, a "third-country authority" cannot be invited to an AML college, with considerable redundancies not making it expedient to conduct such checks at national level. The proposed joint approach is based on a shared methodology provided by EBA and joint assessments by the national supervisory authorities in the EU.

A high-level AML college conference was **initiated by the FMA** and first held in Vienna in September 2023 and held for the second time in Budapest in October 2024. The 2024 edition, hosted by the Hungarian Central Bank, was again an opportunity for networking and exchange among sister authorities from the EU and third country authorities, particularly those in Central, Eastern and South-Eastern Europe (CESEE).

### 3.2.1 HOME COLLEGES

**In 2024, the FMA organised six AML college meetings on a risk-based basis as lead supervisor in line with the relevant EBA Guidelines.** In 2024, the A-FIU was onboarded in all the FMA's AML colleges; OeNB representatives also participated took place in the FMA's AML colleges in relation to specific supervisory cases.

In addition to the FMA as supervisory authority/lead supervisor of the area of the prevention of ML/TF, representatives from the following organisations were also represented at AML colleges

- the respective obliged entities (typically CIs or IUs);
- from AML authorities in countries where Austrian obliged entities have subsidiaries or branch establishments;
- the EBA;
- from prudential supervision (FMA/OeNB and ECB); as well as
- the A-FIU.

**During such college meetings participants from supervised entities give presentations on a range of relevant topics.** Topics include organisational precautions, “lessons learned” from on-site inspections conducted by the FMA and other authorities, actions taken, current supervisory procedures and challenges, new business models as well as monitoring systems equipped with artificial intelligence (AI). Representatives from the participating authorities then discuss about the entity’s level of risk and about observations under supervisory law.

### 3.2.2 HOST COLLEGES

**In 2024, the FMA received a total of 26 invitations to AML colleges established by other European authorities as the lead supervisor (host colleges).** The practice has emerged that the AML colleges for obliged entities with lower risk levels are conducted in writing (written exchange). The FMA participated at nine host college meetings on a risk-based basis. As standard, the FMA submits information to all host colleges about the risk of the entity and relevant observations under supervisory law, even where it does not physically participate at meetings.

## 3.3 ESTABLISHING THE EU ANTI MONEY LAUNDERING AUTHORITY (AMLA)

**Following the entry into force of the EU’s AML package in summer 2024, the legal basis has been established for the new European supervisory system for the prevention of ML/TF.** The centrepiece of this system is AMLA - the new EU AML authority. On the one hand, AMLA is required to satisfy various regulatory tasks: it will have to develop around 70 sets of Technical Standards and Guidelines in the next three years. Highlights include drawing up harmonised rules for AML reporting (e.g. their content, formats and processes) or guidelines for conducting internal risk assessments within the entity. On the other hand, AMLA also has direct and indirect supervisory competences. From 2028, it will directly supervise up to 40 of the highest risk obliged entities from the EU financial sector. In addition, it will be conferred a range of powers for performing its direct supervisory functions. Furthermore, AMLA has a predominantly supporting role as an oversight function over supervisory authorities in coordinating and supporting the non-financial sector as well as the financial intelligence units (FIUs) in EU member states.

**The implementation of the EU AML Package and operational preparations for AMLA started in 2024.** In 2025, the authority is successively commencing its activities. AMLA’s headquarters are in

Frankfurt; it moved into its offices in February 2025. A preparatory meeting of the General Board in its supervisory composition was held virtually on 19 November 2024. AMLA is expected to approach national supervisory authorities (NCAs) to request wide-scale information about their supervisory activities and obliged entities, their risk assessment and their data.

In addition, in a “Call for Advice”, the European Commission has requested EBA and the NCAs to conduct preparatory work in relation to selected Level 2/3 mandates from the AML package that are required as a matter of priority for the future supervisory system. The FMA is using its years of experience and expertise to contribute constructively to these areas and is taking a proactive stance for establishing the foundations of the new supervisory system. As the SSM’s establishment demonstrated, it is essential to contribute as intensively as possible from the outset to a new supervisory mechanism. Since AMLA and the SSM fundamentally differ in composition, a great deal will have to be defined from scratch. Incorporating the non-financial sector into AMLA’s supervisory competence represents an extra level of complexity to be overcome at both national and European level.

The FMA is actively pursuing early and targeted secondments to AMLA to be actively involved in AMLA’s establishment on-site in Frankfurt. The staffing strategy in this area stipulates that interested staff members should be provided with the best possible assistance and mobility promoted. One objective in this regard is the visible positioning of FMA staff members as EU AML experts. Significant milestones have been reached in this regard: there has been FMA representation in AMLA’s staff in Frankfurt since February 2025, forming a significant contribution in designing the new European supervisory mechanism. Further hiring procedures are ongoing.<sup>2</sup> By the end of 2025, the authority should have around 80 staff members.

A mapping exercise will be needed to identify and close potential gaps at an early stage, as well as to assess the changes needed regarding data and reporting. The general expectation, especially regarding the harmonised risk assessment, is that AMLA will request large amounts of data from supervisory authorities, and that data and information will be required to be supplied within short deadlines. To achieve this will require high quality data as well as easy access to the required data. In addition, it will be necessary to develop existing IT systems further and to adapt them to AMLA’s harmonised risk assessment. The FMA is involved in drawing up the new risk assessment methodology and in this context is clearly expressing its interest in data-driven supervision that is both practice-based and user-friendly, to ensure that financial market participants are not unduly burdened with requirements; from the FMA’s perspective, data requests should only be made if they add value for supervision.

Other specific preparatory work is under way regarding representation on AMLA’s General Board in its supervisory composition, together with the BMF, BMAW, BMJ and other non-financial sector

---

<sup>2</sup> If you are interested, see: [https://www.amla.europa.eu/careers/vacancies\\_en](https://www.amla.europa.eu/careers/vacancies_en)

supervisory authorities. The aforementioned authorities have decided that the FMA should be the permanent representative to the General Board in its supervisory composition.

### **3.4 FMA REPRESENTATION IN INTERNATIONAL AND EUROPEAN COMMITTEES**

**The FMA is actively represented in a host of international and European committees.** This part contains a brief overview of the committees, and their respective substantive focuses of work in 2024.

#### **3.4.1 EGMLTF**

In 2024, the European Commission's Expert Group on AML/CFT (EGMLTF) focussed on the results of the negotiations on the EU AML Package followed by the level 2 and level 3 legal acts arising from the package. Furthermore, Frankfurt was selected at EU level for AMLA's head office. Further focuses were the Supra-national Risk Assessment (SNRA 2025) as well as the risk assessment at European Union level, which will take place based on the new EU AML Package.

#### **3.4.2 FATF**

**The Financial Action Task Force (FATF) focussed on concluding the 4th round and preparing for the 5th round (from 2024) of country assessments.** As a result, Austria is one of the first member countries to be assessed by the IMF from the end of 2024. The 5th round of assessments is intended to focus more intensively on country-specific risks, especially a more in-depth review of the non-financial sector.

**The country assessment for Austria started in November 2024** with the submission of information about the implementation of FATF Recommendations in the national legal system (technical compliance assessment). Subsequently, Austria is ordered to prove the effectiveness of its national AML/CFT system and the actions of the involved authorities, competent bodies and the private sector (effectiveness assessment). The different areas of the legal system and the national AML/CFT system will be graded using a four-tier grading scale for this purpose. The IMF inspection team's on-site visit is scheduled for June/July 2025. Austria's country assessment is planned to be concluded with the discussion and adoption of the country's mutual evaluation report at the FATF plenary meeting in February 2026 (Austria's most recent previous assessment by the FATF was in 2015/2016).

#### **3.4.3 AMLSC**

**EBA's AML Standing Committee (AMLSC) has focussed on the establishment of the new EU AML Authority (AMLA) in Frankfurt.**

**In addition, EBA’s Guidelines on Risk Factors for money laundering and terrorist financing were amended, and EBA Guidelines issued on information requirements in relation to transfers of funds and certain crypto-assets transfers.** Both sets of Guidelines apply from 30 December 2024. The Guidelines on Risk Factors for money laundering and terrorist financing set out in detail the systems and procedures that payment service providers and crypto-asset service providers are required to implement to detect records where information about the payer and payee of transfers is missing or incomplete. Sector-specific guidelines for crypto-assets service providers were added to because of the new Transfer of Funds Regulation (Regulation (EU) 2023/1113). The Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 (‘Travel Rule Guidelines’) describe the procedures for detecting and managing transfers of funds and crypto-assets lacking the required information, and how the risk of ML/TF is to be mitigated. Furthermore, they also specify information in relation to direct debits. Additionally, conditions are determined regarding transfers of crypto-assets that are transferred to or from a self-hosted address. The Guidelines’ addressees are payment service providers (PSPs), intermediary payment service providers (IPSPs), crypto-asset service providers (CASPs) and intermediary crypto-asset service providers (ICASPs), as well as the supervisory authorities.

**The FMA, together with the OeNB, contributed to the Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures as well as the Implementing Technical Standards (ITS) on the level of charges for credit transfers, instant credit transfers and payment accounts, and the share of rejected transactions.** Regulation (EU) No. 260/2012 (the SEPA Regulation) and Regulation (EU) 2023/1113 (Transfer of Funds Regulation) are the basis for the ITS. Both also address the FMA’s future scope of activities regarding targeted financial restrictive measures. The final versions are expected to be published in 2025.

**In December 2024, the AMLSC approved the EBA report “Report on NCAs approaches to the supervision of banks with respect to AML/CFT (round 4 – 2023/24)”.** This report summarises the findings from the fourth round of ongoing reviews of national competent authorities’ approaches to AML/CFT supervision of banks in the EU/ EEA Member States (“MS”) - (EBA peer reviews). During 2023-2024, the EBA’s review team assessed 14 national competent authorities from nine Member States and issued recommended actions tailored to each national competent authority to support its AML/CFT work. They also assessed how supervisory authorities in these Member States tackled ML/TF risk in line with their supervisory remit and scope. With the conclusion of this round, EBA has assessed all forty NCAs, who are competent for AML/CFT supervision in thirty EU/EEA Member States.

The FMA received the results of the EBA peer review in October 2023 and has defined the following measures for improving systems and for remedying specific deficiencies.

- a training programme was created for new staff members;

- the sectoral risk assessment (SRA) was developed;
- a concept for horizontal off-site analysis was drawn up and applied for the first time in 2025;
- supervisory processes were enumerated inter alia in relation to granting of licences/Fit & Proper procedures;
- The training course “Joint analysis - case studies and lessons learned” was developed, and is part of the FMA’s training offering since Spring 2024

## 3.5 LEGAL INTERPRETATION AND REGULATORY DEVELOPMENTS

### 3.5.1 THE FM-GWG’S “NEW” CASP REGIME

**MiCAR entered into force on 30.12.2024 - a comprehensive harmonised regulatory and legal framework that is no longer restricted to the prevention of ML/TF.**

Austria made use of this national discretion in Article 23 of the MiCA Regulation Enforcement Act (MiCA-VVG; *MiCA-Verordnung-Vollzugsgesetz*). Under that provision, crypto-asset service providers that provided their services in accordance with the applicable law as registered virtual asset service providers pursuant to Article 2 no. 22 FM-GwG prior to 30 December 2024 are allowed to continue to do so until 31 December 2025 or until the time at which they are granted or refused an authorisation in accordance with Article 63 of Regulation (EU) 2023/1114, depending upon which occurs first.

As of 30.12.2024, a total of 13 VASPs held an FMA registration in accordance with the FM-GwG. The FMA shall ensure that the VASPs that were already registered that submit an application for a CASP authorisation pursuant to MiCAR until the end of the transition period (until 31.12.2025), are seamlessly transferred in a legally clear manner into the new MiCAR regime, and endeavours to guarantee legal and planning clarity in the changeover to or with regard to the MiCAR regime (note: as of April 2025 only one undertaking had been issued a CASP authorisation in Austria to date).

**The Transfer of Funds Regulation (TFR) was passed at the same time as MiCAR**, and which has also been directly applicable with effect from 30.12.2024 that now also applies to transfers of crypto-assets in addition to transfer of funds. This ensures the harmonised application throughout the EU of the revised FATF Recommendations from 2019, especially Recommendation 15 on New Technologies and Recommendation 16 on Wire Transfers (electronic payment transactions).

In the first half of 2024, the FMA surveyed Austrian registered VASPs to obtain an impression about current challenges and expectations as well as to ensure that obliged entities were prepared for the impending requirements placed on them by the TFR. This initial survey contained a detailed catalogue of questions on the current state of implementation of the TFR by the VASPs including planned measures, to permit the FMA to obtain an initial impression regarding implementation, and to identify future issues. Three of the surveyed VASPs responded that the TFR is not applicable to their business model. Most of those surveyed plan to use external service providers for

implementing the TFR. The new requirements are by and large to be implemented by purchasing a product to do so. Various providers were mentioned.

### **3.5.2 LEGAL QUESTIONS ABOUT THE FM-GWG**

**As the competent primary authority, the FMA's activities include the legal interpretation and practical clarification of (abstract) legal provisions in the FM-GwG.** This includes questions occurring during on-site measures, official procedures, and to a particular extent during the process of answering relevant legal enquiries. The FMA receives a constant flow of interesting legal inquiries about the practical interpretation of individual provisions in the FM-GwG, which, for example, addressed the following topics in 2024:

#### **3.5.2.1 The vulnerability of immovable property for being exploited for money laundering purposes**

Reports in Austrian media covered various insolvencies in the real estate sector in 2024, resulting in this area entering the FMA's supervisory focus. From the findings obtained from its supervisory activities it is possible to conclude that obliged entities under the FM-GwG increasingly need to pay attention to potential risk factors in real estate transactions, especially those that arise from complex shareholding structures, unclear sources of funds, or the involvement of family offices. To ensure that due diligence obligations are observed, it is essential for staff members to attend training in this area, especially to allow them to identify the risk factors that exist from customer documentation they have access to.

Not only do opaque ownership and shareholder structures make it more difficult to clearly allocate an immovable property to its owners, but they also prevent end-to-end tracing of the origin of funds for purchasing the property or for granting a loan to finance the purchase. During the mandatory KYC checks, the aforementioned risk factors are required to be clarified in detail with the customer, and the obliged entity is required to obtain a holistic and conclusive picture (precise business activity, origin of funds, financing of repayments etc.) about the customer. To do so requires documents to be gathered and checked about the customer and the property, including documentation about the real estate project and valuations etc. They focus on the plausibility and traceability of customer information for the specific business venture.

If (implausible) grounds emerge during the course of establishing the business relationship or during the ongoing business relationship with a customer (e.g. in the chain of ownership) of the existence of a family office activity or the involvement of family office service providers (especially when providing multi-family office services), potentially existing trustee relationships or constructions need to be actively examined and documented by the obliged entities in a way that is logical for third parties.

When obtaining an “extended” excerpt pursuant to Article 9 para. 5 WiEReG, it should be noted that such an excerpt is only considered complete if it does not contain a valid remark, where the notified information matches the information that is compiled by automated means, and the completeness analysis shows that all data for the compilation of the beneficial owners are available. For example, foundations, foreign legal entities, trusts or arrangements of a similar nature to a trust, partnerships appearing at a relevant point in the participation structure, all prevent a complete extended excerpt.

If an extended excerpt is incomplete, it may still be used to verify the beneficial owner if obliged entities take additional risk-based measures. Such measures may include, for example, obtaining additional extracts for superordinate entities from the Register of Beneficial Owners or from public registers or obtaining corresponding supporting documents from the legal entity itself. The obliged entity must be convinced, when considering all the documents and extracts obtained (also regarding the organisation charts of the group of companies), that it knows who the beneficial owner is and fully understands the client’s ownership and control structure.

Finally, the supervisory authority may emphasise the importance of the intensive and regular training of staff members, especially for staff members who are active in the sales field, to ensure that staff members have the necessary awareness to detect complex customer circumstances and risk factors from the supporting documentation received from the customer, and subsequently to involve the Anti-Money-Laundering Officer at an early stage.

### **3.6 MARKET TRENDS**

The following chapter presents selected data from the internal AML App about different groups of obliged entities in the Austrian market, their respective ML/TF risk, and developments regarding their customer base and business areas in particular for CIs. In addition, there are also information about the CI’s foreign payments (this data is provided by the OeNB).

#### **3.6.1 NUMBER AND BREAKDOWN OF OBLIGED ENTITIES**

Table 3 shows the number of entities that fill out and submit the risk questionnaire for the FMA’s internal risk classification (AML App). Increases in the number of obliged entities captured by the AML app have been observed since 2019. However, a slight decreasing trend has been observed in the last three years, which points to the changing composition of obliged entities.

In 2024, the number of obliged entities captured stood at 682. The decline in the number of CIs is particularly apparent, as this group continues to make up the largest proportion of obliged entities. Their number has fallen by over 25% since 2020. This decrease is primarily attributable to mergers in the financial sector. At the same time, the risk classification process has also been developed further: Additional categories of obliged entities have been included since 2022, with ISPs/IFs and MCs/AIFMs being included in the classification using adapted risk questionnaires. This has led to the

number of supervised CIs making up a larger relative share of obliged entities, while other categories have been successively added in recent years.

Groups of Obligated Entities	Quantity		
	2022	2023	2024
E-money institutions	3	3	3
MCs / AIFMs	67	70	61
Credit institutions	492	467	444
Money remitters	4	5	4
VASPs	20	19	12
Insurance companies	27	26	24
Investment service providers/investment firms	134	133	123
Payment institutions	10	11	11
<b>Total</b>	<b>757</b>	<b>734</b>	<b>682</b>

Table 3: Groups of Obligated Entities in the AML App

The following section shows how risk is distributed overall within the individual categories of obliged entities, in the case of CIs, IUs, VASPs, PIs, ISPs/IFs, MCs/AIFMs<sup>3</sup>. The evaluations are based on specific business activities or compared to other institutions within the same category of obliged entities.

**3.6.1.1 Credit institutions (CIs)**

Figure 2 and Figure 3 illustrate the global distribution of natural and legal persons in the CI sector.

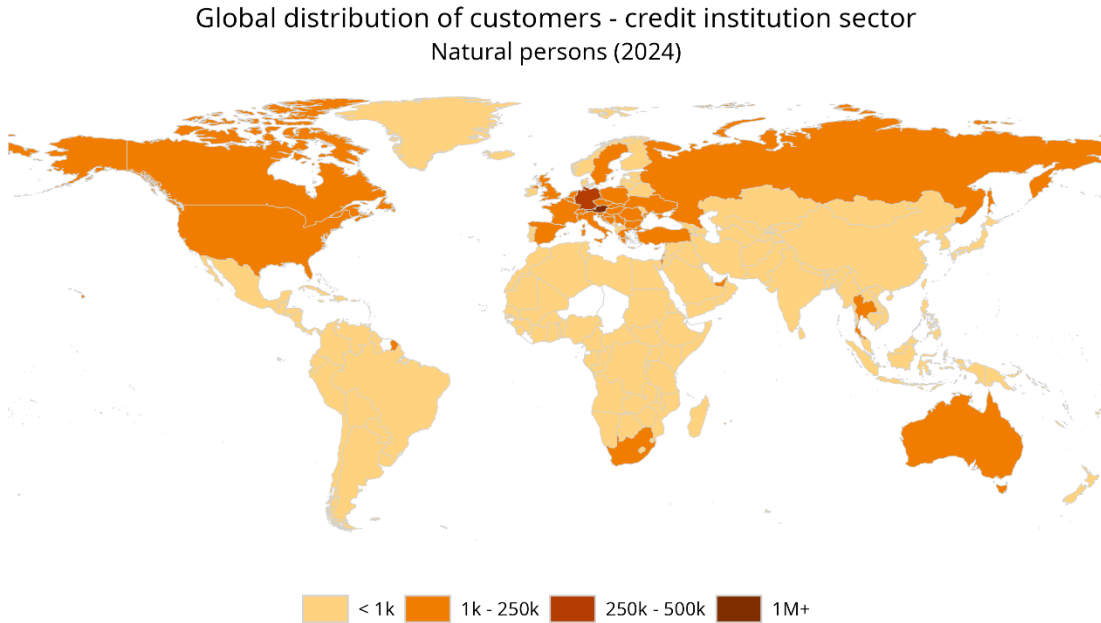


Figure 2: World map of customers in 2024, CI sector, natural persons

<sup>3</sup> There is no graphical representation of the classifications for the group e-money institutions and money remitters due to their small quantity, to prevent conclusions from being drawn about respective institutions' classifications.

### Global distribution of customers - credit institution sector Legal persons (2024)

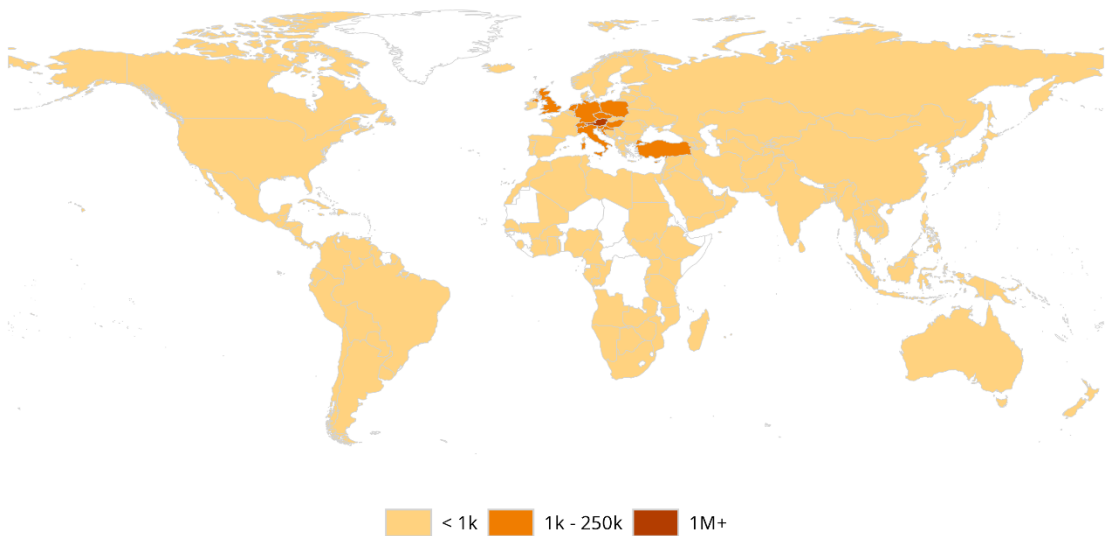


Figure 3: World map of customers in 2024, CI sector, legal persons

Figure 4 shows the distribution of overall risk of CIs. The main observation is that only a small proportion of the sector was in the highest risk category in 2024. A mere 7% of institutions were exposed to a high or elevated risk in 2024. The proportion of institutions with a medium risk level stood at 45%, a similar level to previous years. Noticeably, the proportion of institutions classified as low risk fell by three percentage points in 2024 to 48% compared against 2023. Developments in recent years point to some movement between the risk categories, with an increased concentration in medium and elevated risk identified compared with the previous year.

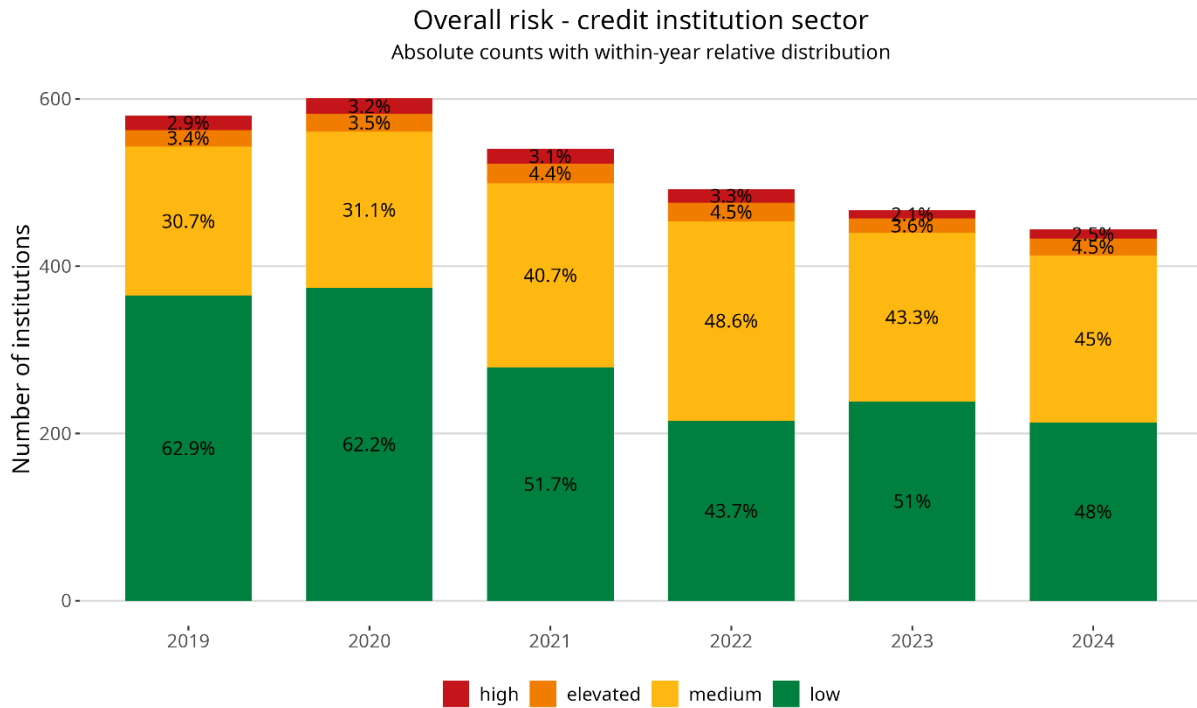


Figure 4: Distribution of the CI sector's overall risk

The left-hand graphic in Figure 5 presents the aggregated total assets by risk class for CIs: substantially the highest values are observed in the risk classes “medium” and “high”. This is particularly interesting given that the “high” risk class comprises only 11 CIs (cf. Figure 4). This is an important reason why the risk of being misused for ML/TF purposes is being taken into account with greater intensity within the scope of prudential supervision.<sup>4</sup>

In contrast, the graphic on the right-hand side of Figure 5 illustrates the respective number of business relationships CIs have in risk classes from ‘low’ to ‘high’. In contrast to the presentation of risk/total assets, these figures show that Austrian CIs in the high-risk category do not conduct the majority of business relationships in the Austrian financial market. CIs allocated to the medium or low risk categories conduct the majority of business relationships. This fact is acknowledged by the FMA by also carrying out on-site and off-site measures at appropriate intervals to review the suitability and appropriateness of preventive measures for medium and low-risk CIs as well as on- and off-site measures conducted on an ad hoc basis.

<sup>4</sup> For further information about the interplay between prudential supervision and the prevention of ML/TF, see e.g.  
 - <https://www.bankingsupervision.europa.eu/banking/tasks/anti-moneylaundering/html/index.en.html> as well as the  
 - EBA Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU (EBA/GL/2021/15, 16.12.2021).

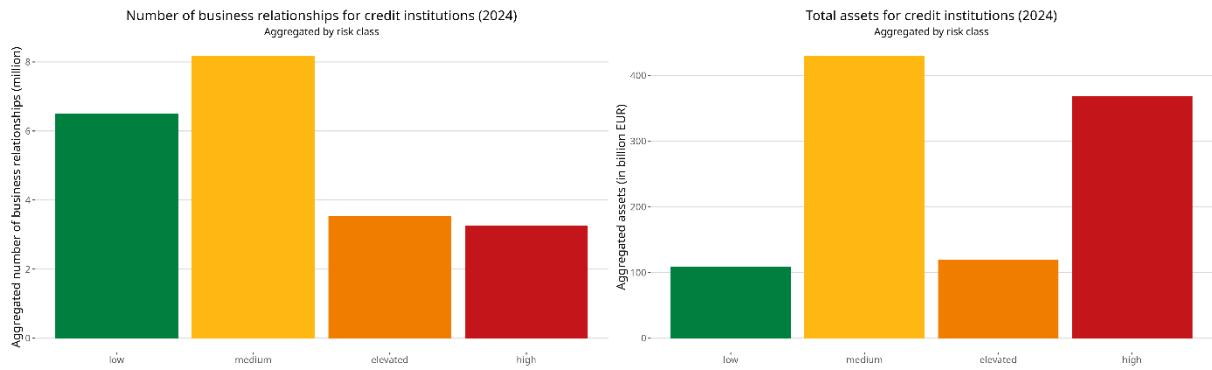


Figure 5: Number of business relationships & total assets aggregated by risk class for credit institutions

### 3.6.1.2 Insurance undertakings (IUs)<sup>5</sup>

Figure 6 and Figure 7 illustrate the global distribution of customers in the IU sector .

Global distribution of customers - insurance undertaking sector  
Natural persons (2024)

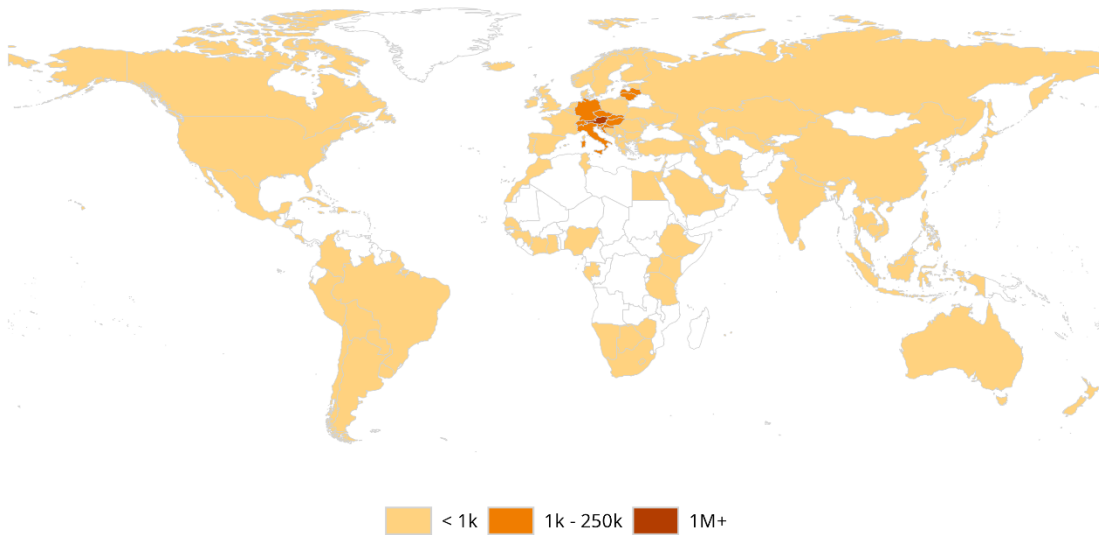


Figure 6: World map of customers in 2024, IU sector, natural persons

<sup>5</sup> The scope of application of the FM-GwG only extends to insurance undertakings pursuant to Article 1 para. 1 no. 1 VAG 2016 and small insurance undertakings pursuant to Article 1 para. 1 no. 2 VAG 2016 respectively **within the scope of their life insurance operations** (classes 19 to 22 pursuant to Annex A of VAG 2016), cf. Article 1 para. 1 in conjunction with Article 2 no. 2 lit. b FM-GwG.

### Global distribution of customers - insurance undertaking sector Legal persons (2024)

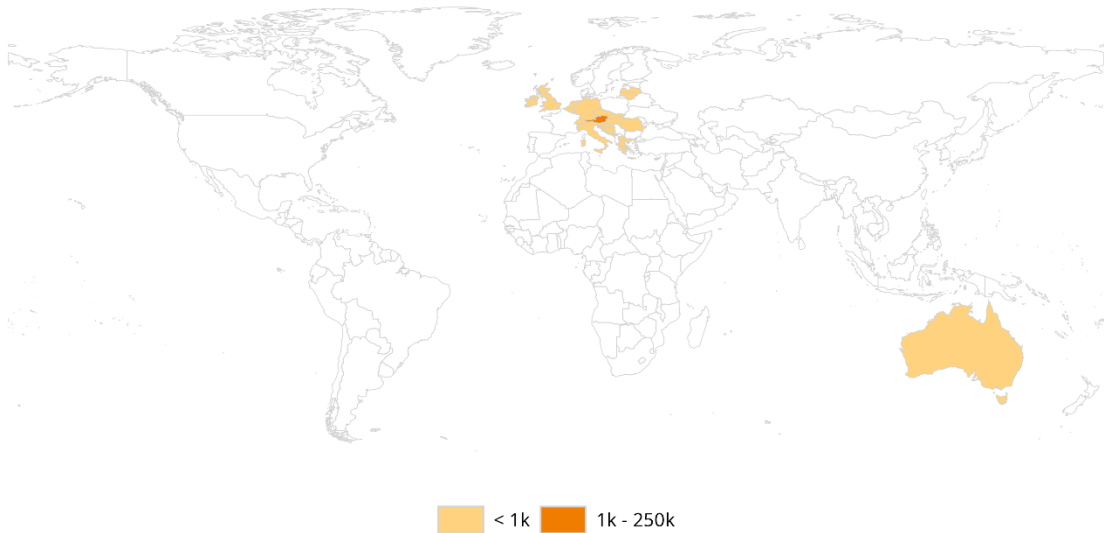


Figure 7: World map of customers in 2024, IU sector, legal persons

Figure 8 shows the distribution of overall risk of IUs. In 2024, the absence of any undertaking from this sector in the risk classification being categorised as high risk is noticeable. In 2024, only five institutions were exposed to a medium or elevated risk of being misused for the purposes of ML/TF. It is striking that the proportion of IUs with a medium risk has fallen considerably year-on-year: from 30.8% in 2023 to 16% in 2024. At the same time, the number of undertakings classified as low risk has increased to 80% of all obliged entities. This is the highest value in recent years and indicates that minimising of risk is continuing within the industry.

The proportion of insurance undertakings classified as having an elevated risk remains stable at 4%, a similar level to previous years. Developments in recent years have shown that there is still a low overall risk of insurance undertakings being misused for ML/TF. Reasons for the fall in numbers of those at medium risk might include stricter regulatory measures and institutions' improved internal risk controlling.

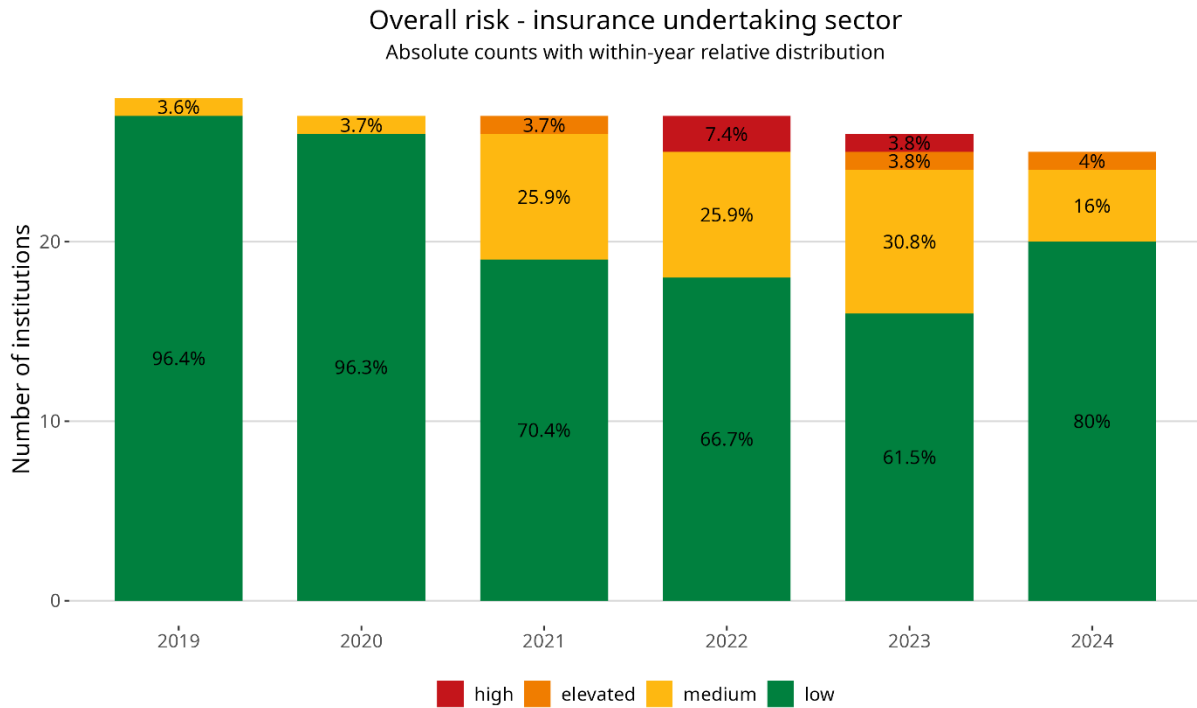


Figure 8: Distribution of the IU sector's overall risk

### 3.6.1.3 Virtual asset service providers (VASPs)<sup>6</sup>

Figure 9 and Figure 10 illustrate the global distribution of customers in the VASP sector.

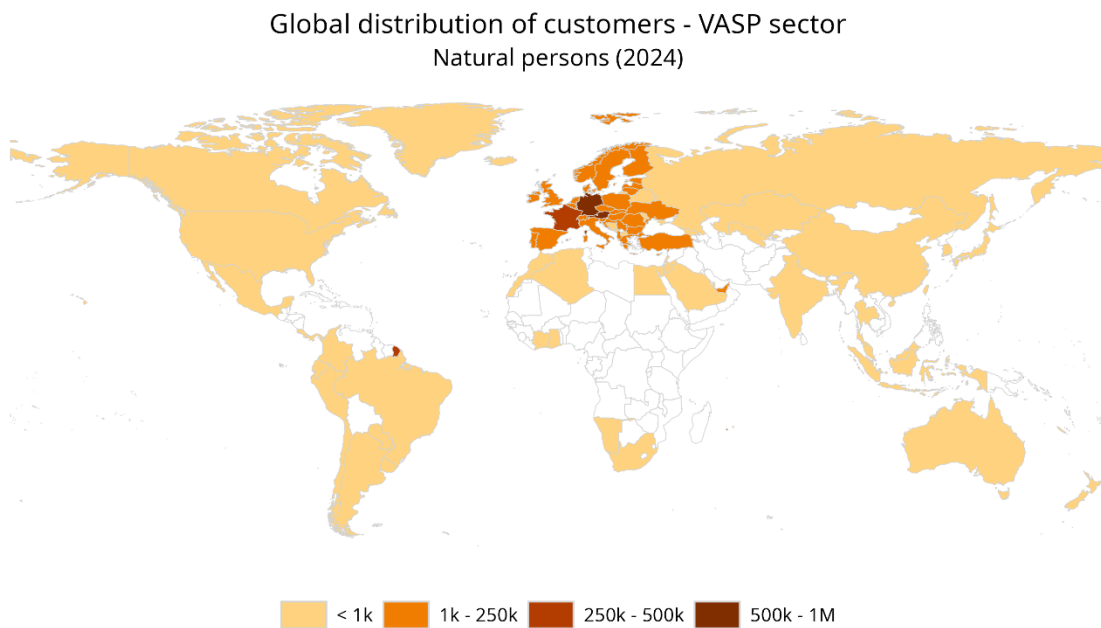


Figure 9: World map of customers in 2023, VASP sector, natural persons

<sup>6</sup> VASPs are currently exclusively subject to supervision in relation to the prevention of ML/TF, i.e. the scope of application of the FM-GwG. With MiCAR, a comprehensive regulatory and supervisory regime not restricted to the prevention of ML/TF enters into force cf. Point 3.5.1.

### Global distribution of customers - VASP sector Legal persons (2024)

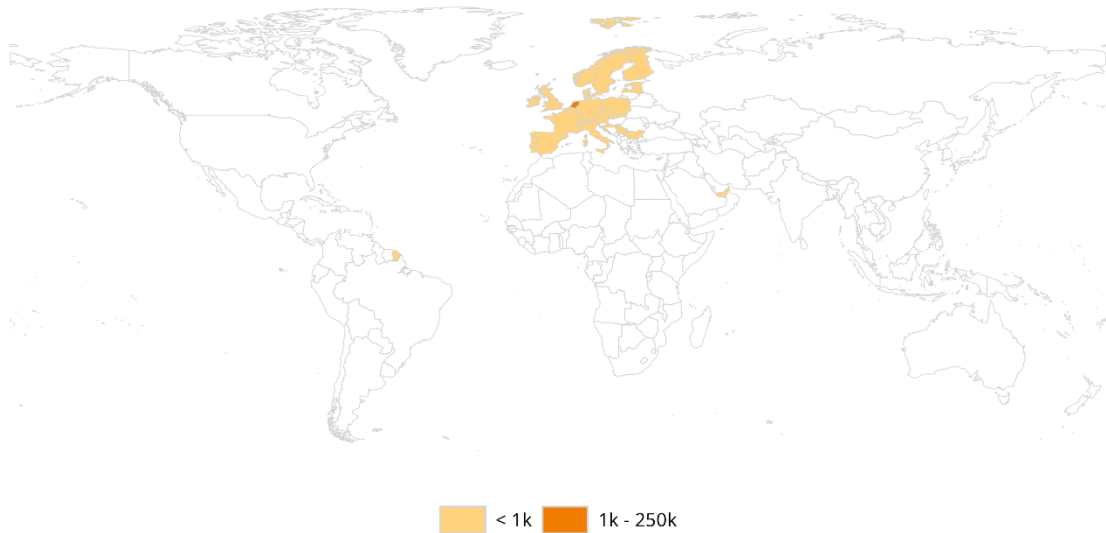


Figure 10: World map of customers in 2023, VASP sector, legal persons

Figure 11 shows VASPs' overall risk distribution. One-third of obliged entities are exposed to a high risk of being misused for the purposes of ML/TF. Nevertheless, the absolute number remained constant in comparison with the two preceding years. At the time of being surveyed, seven out of twelve VASPs are classed as low to medium risk. Classification as medium and high risk may be traced back among other things to the high risk of crypto-currencies, of being misused for purposes of ML/TF, and the design and functioning of - often complex - products and services offered. Classification in the low or medium risk categories in many case is the result of a small number of customers or transactions during the reference period compared against other institutions within the same category. The strong decline in the number of obliged entities, returning to the level observed in 2020, can be explained by new obliged entities having voluntarily surrendered their registration, often as a result of meetings with the FMA, having not conducted any business activities.

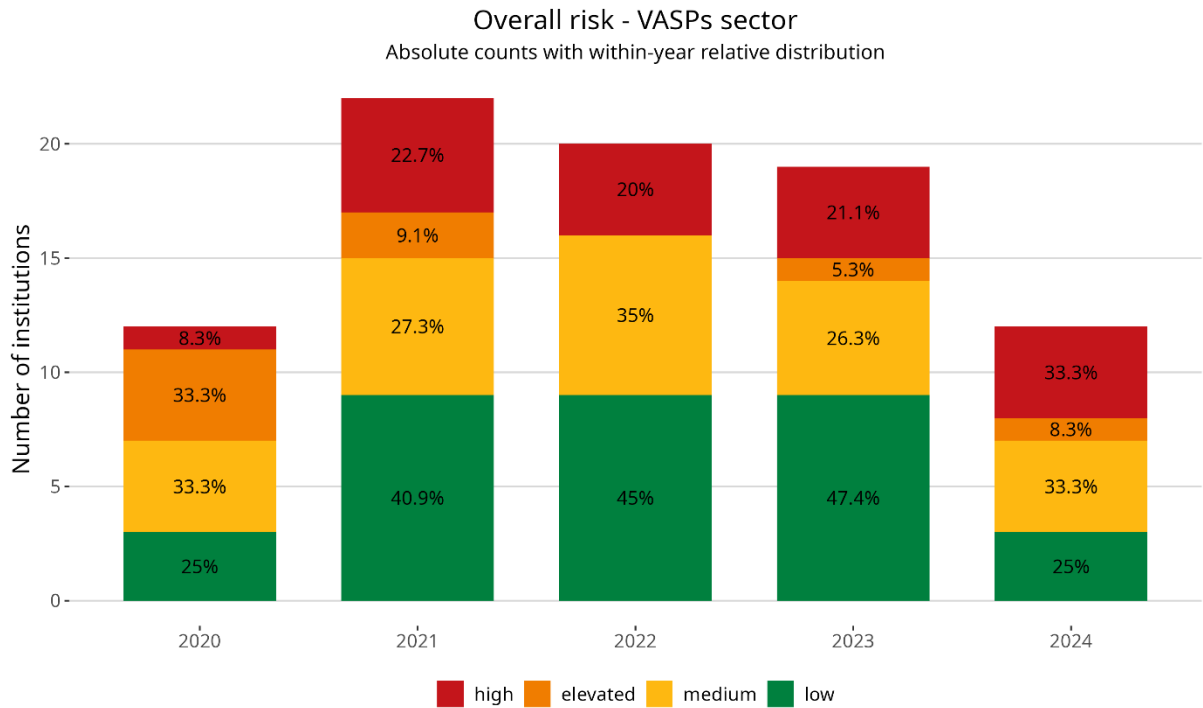


Figure 11: Distribution of the VASP sector’s overall risk

### 3.6.1.4 Other sectors

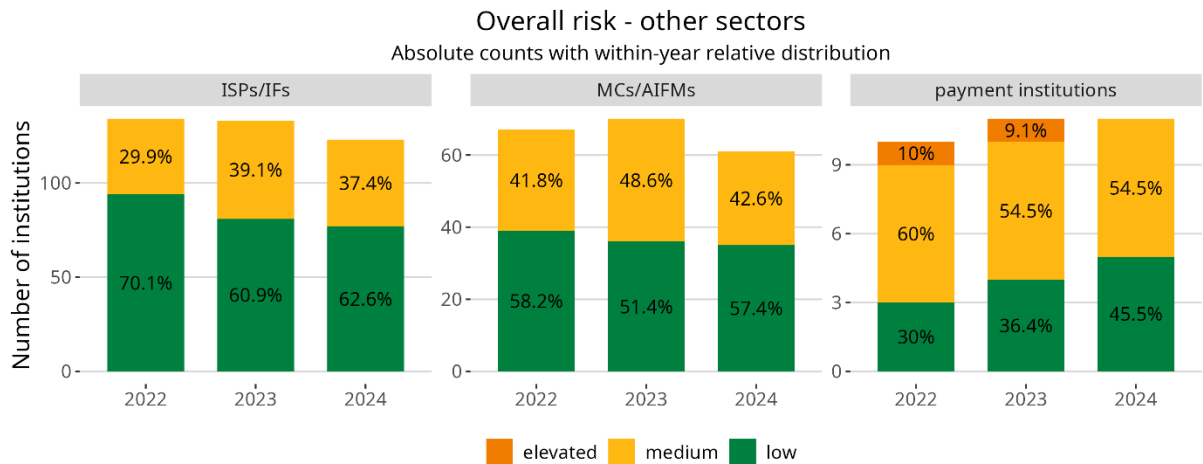


Figure 12: Distribution of other sector’s overall risk

Figure 12 illustrates other sectors’ risk classifications. A significant milestone in 2024 was no obliged entity from the PI, ISP/IF or MC/AIFM sectors being exposed to an elevated or high risk.

### 3.6.2 “TOP THREE” RISK FACTORS

Figure 13 shows the development of the three sub-risks with the strongest (albeit moderate) increases in the Credit Institutions sector from 2016 to 2024.

The significant increase of the “Number of HNWI (High Net Worth Individuals) customers” sub-risk can be traced back in particular in the 140% increase in the number of HNWI’s serviced by credit

institutions since 2016. This increase correlates with increases in savings deposits of Austrian private households for a number of years. This may also be attributed to the economically uncertain times (e.g. the Russian invasion of Ukraine, inflation etc.). While HNWI's have increased, total numbers of customers of all credit institutions have fallen by 10% during the same period.

The increase in the sub-risk weighted by country groups in relation to beneficial owners primarily results from an increased number of beneficial owners notified from countries on the FATF grey list.

For the sub-risk "Number of outgoing transactions" a particularly strong increase has been observed of transactions in third countries with a high risk.

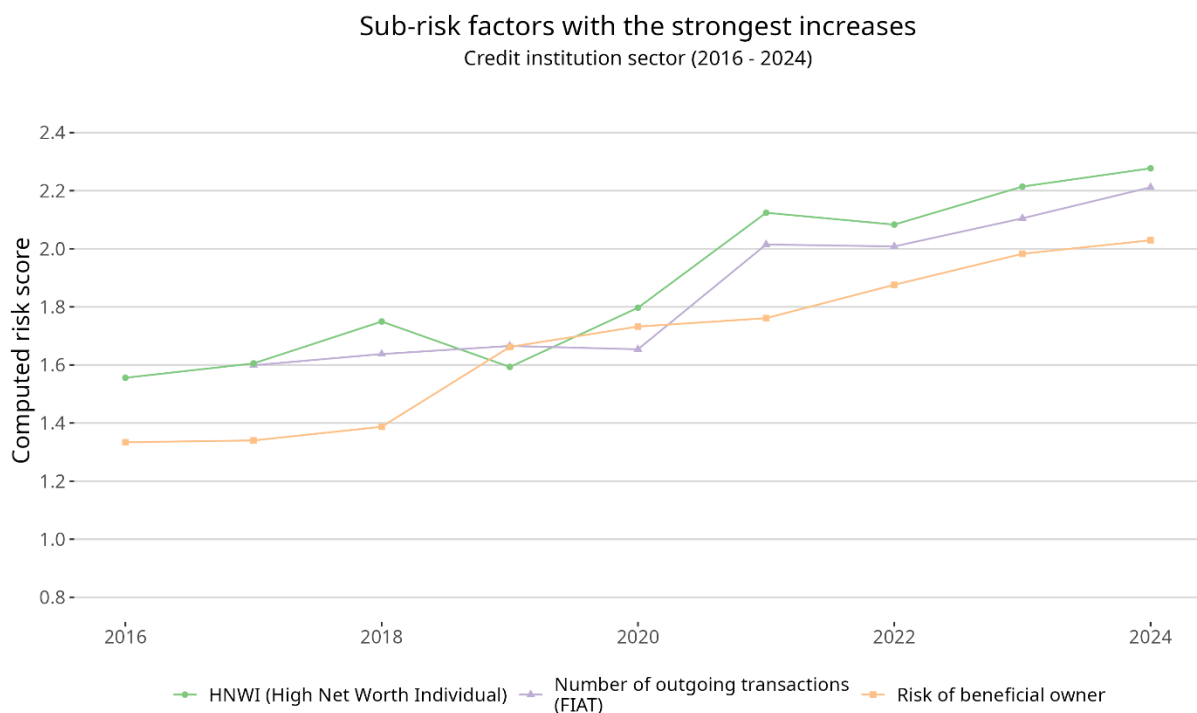


Figure 13: Top three risk factors: strongest increases

### 3.6.3 BUSINESS RELATIONSHIPS WITH CORRESPONDENT BANKS IN THIRD COUNTRIES, RUSSIA AND BELARUS

Figure 14 shows the development of the number of correspondent banking relationships between 2021 and 2024. There has been volatility in the total number of such relationships with third countries during this period. A downwards trend is still observable for Russia and Belarus. In 2024, there were 281 correspondent banking relationships in third countries, the second highest amount since 2019. In contrast the number of relationships to Russia and Belarus has fallen further. 14 correspondent banking relationships in Russia and 5 in Belarus represents the lowest level over the last six years.

Such developments in relation to Russia and Belarus are representative of the banking sector's general trend to increasingly avoid risk. Especially those banks that are active in countries that are

subject to international embargoes, or countries on the FATF's grey list, are increasingly withdrawing from high-risk regions, to prevent adverse media reporting from damaging their reputation, and to avoid the enforcement of sanctions associated with Russia's war of aggression against Ukraine. Stricter regulatory requirements and the associated administrative burden have led banks to focus their business relationships on safer, more transparent markets, and to withdraw from high-risk regions.



Figure 14: Business relationships with correspondent banks by country groups

### 3.6.4 BUSINESS RELATIONSHIPS TO RUSSIAN/BELARUSIAN CUSTOMERS; BENEFICIAL OWNERS DOMICILED IN RUSSIA/BELARUS

Figure 15 shows the development in business relationships to customers (natural/legal persons), or beneficial owners of legal persons domiciled in Russia and Belarus since 2019. The clearly observable downward trend is apparent for business relationships with customers/beneficial owners of legal persons domiciled in Russia as well as Belarus. There has been at least a 45% decline in both countries for all three customer groups over the last six years. The number of beneficial owners in Russia (-78%) and in Belarus (-75%) display the most marked decline. This trend already prevailed prior to comprehensive sanctions being imposed in relation to the war in Ukraine.

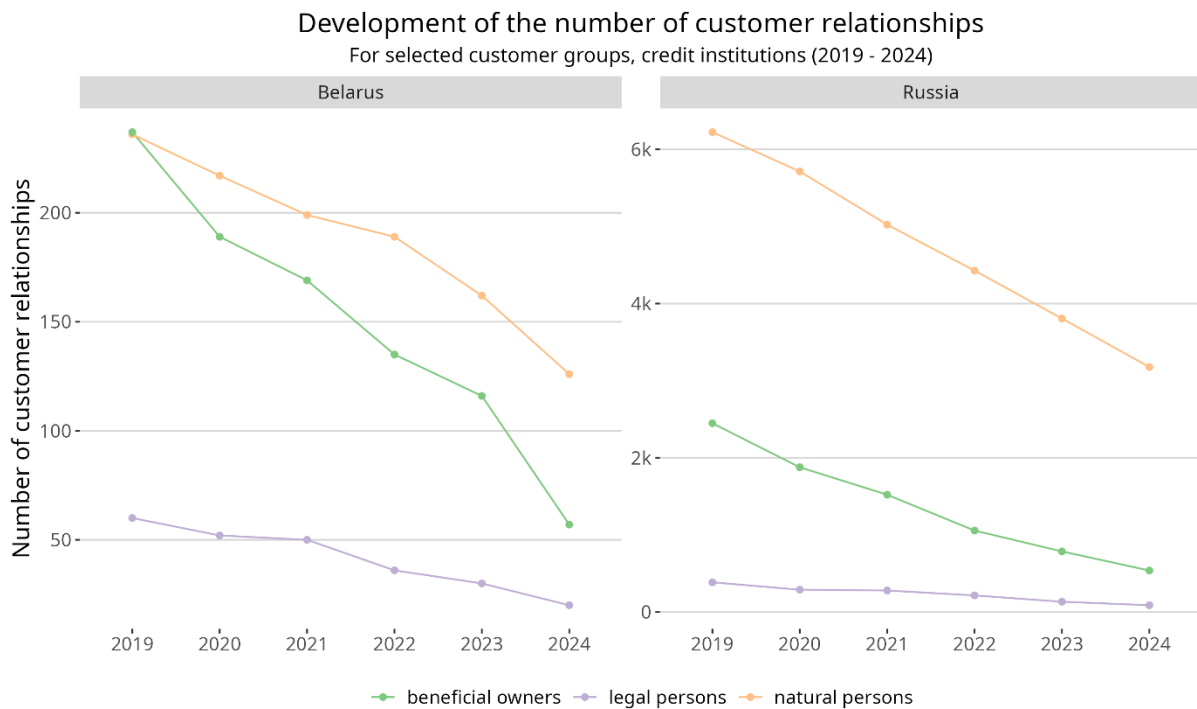


Figure 15: Development of the number of customer relationships

### 3.6.5 OUTSOURCING: CREDIT INSTITUTION SECTOR

Figure 16 illustrates the prevailing trend towards outsourcing models in the credit institutions sector. A significant proportion of institutions has at least partially outsourced activities relating to the due diligence obligations defined in the FM-GwG. In total, around 68% of credit institutions have outsourced processes accordingly, with only a small proportion of institutions (ca. 12%) remaining that still perform all relevant activities internally.

24% of credit institutions outsource the position of the AML Officer. More detailed examination shows that transaction monitoring is affected to a significant extent: while 43% of institutions only outsource the “first vote” i.e. an initial assessment of the transaction, just under half of institutions fully outsource this process.

Nevertheless, a high proportion of credit institutions that either partially or fully outsource due diligence obligations (87%) shows their structural adaptation to the Austrian financial market’s conditions. The financial market’s large number of market participants, make a risk-based and targeted allocation of the FMA’s resources particularly relevant. In this context, the FMA inspects larger “sectoral banks” that deal with many outsourcings, using targeted on-site measures.

Such an approach ensures that potential irregularities or room for improvement is not only identified at an individual obliged entity but also has a multiplier effect on affiliated institutions or the entire sector. In addition, the bundling of resources and expertise in outsourcing centres enables the more efficient identification and combating of money laundering and terrorist financing risks

(ML/TF). Processing and analysing data centrally allow risks to be identified at an early stage, and targeted countermeasures initiated more quickly.

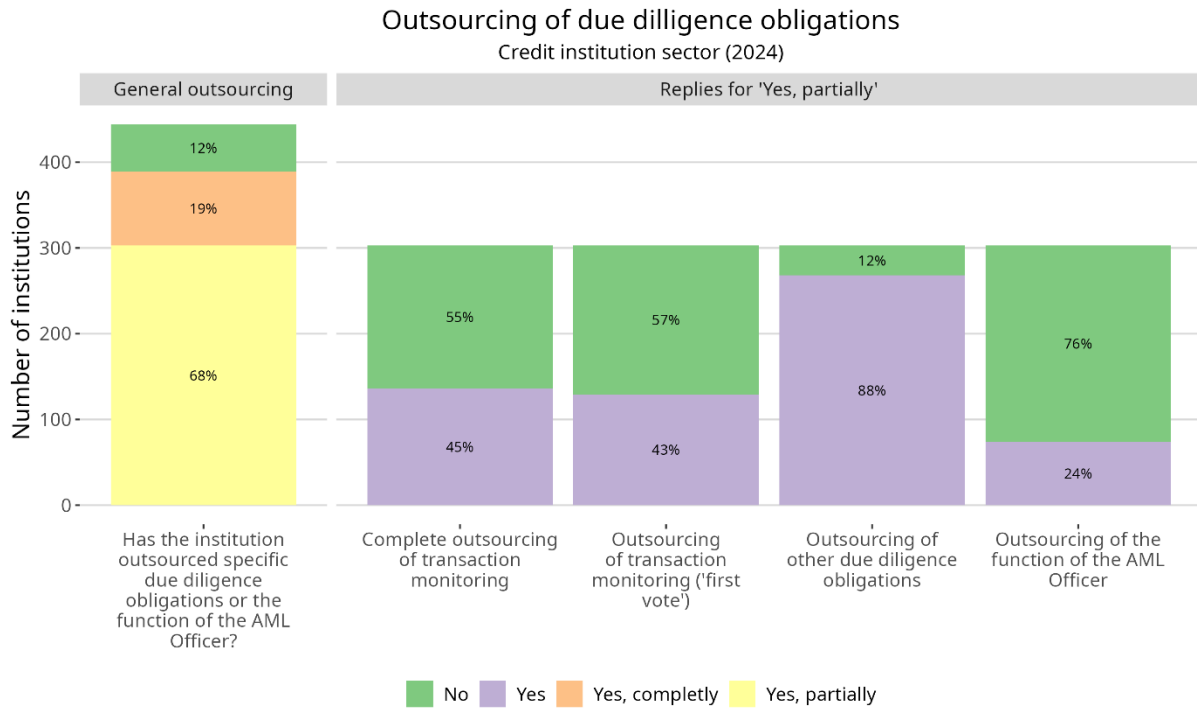


Figure 16: Outsourcing of due diligence obligations in the CI sector (2024)

### 3.6.6 CROSS-BORDER TRANSACTIONS

Cross-border payments in the Credit Institutions sector continued to be dynamic in 2024. The total volume of incoming and outgoing payments stood at EUR 880.27 billion or EUR 864.65 billion respectively, which reflects Austria and Europe’s continuing economic interconnectedness.

Figure 17 clearly shows Germany at the top, followed by France, Great Britain and the Netherlands. Smaller financial centres like Luxembourg and Switzerland also have high volumes of payments. The general balance between incoming and outgoing payments accentuates the stability of international capital flows.

The FMA continually observes developments in the payment transactions sector to identify risks quickly and to guarantee financial market stability. Digital transformation and regulatory changes remain key issues for the coming year.

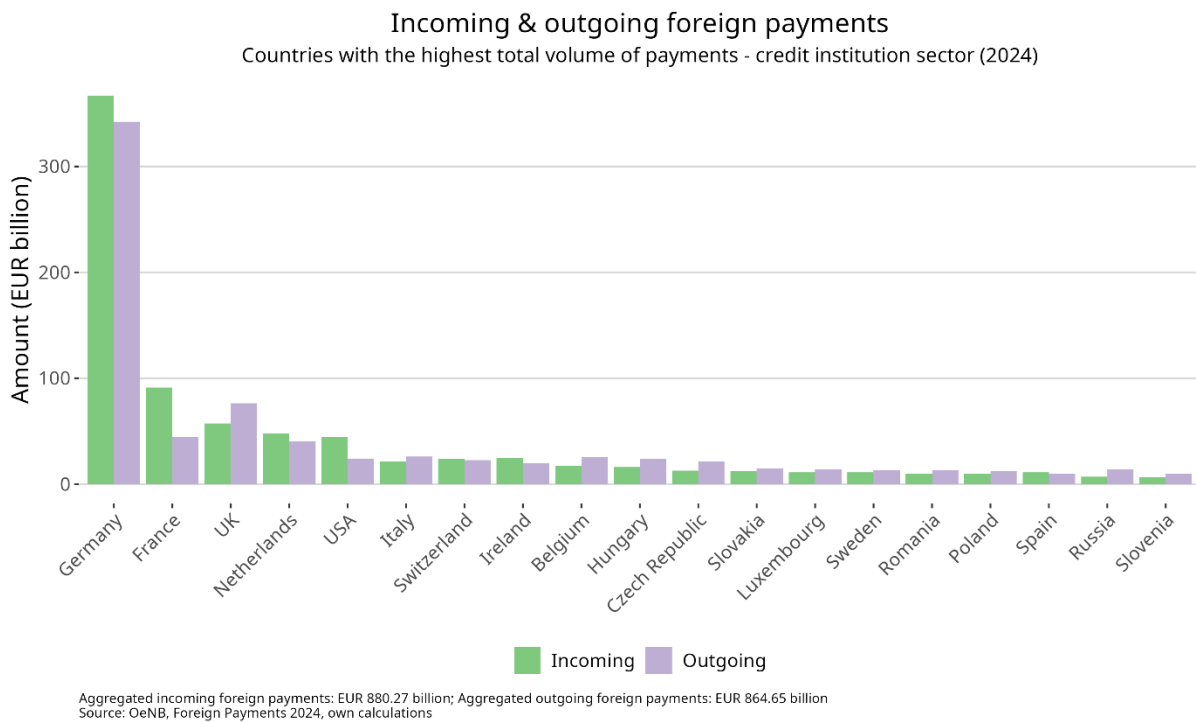


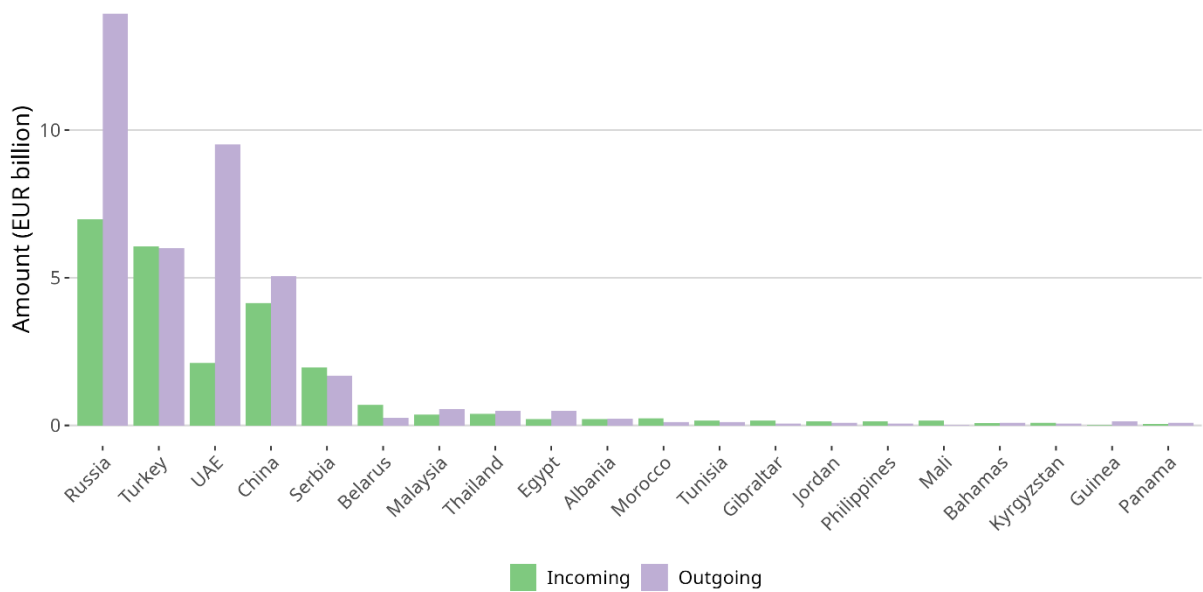
Figure 17: incoming & outgoing foreign payments for countries with the highest total volume of payments in the CI sector (2024)

In 2024, the volume of cross-border payments with high-risk countries remained high. Figure 18 highlights such payments in particular flowing to and from Russia, Turkey, the United Arab Emirates, and China. The total outgoing transaction volume was EUR 39.75 billion, while incoming payments stood at EUR 24.89 billion.

The strong imbalance between the level of outgoing and incoming payments is striking, particular for Russia, China and the United Arab Emirates. This might be attributable to capital outflows or regulatory framework conditions. Payments with other high-risk countries remained comparatively low.

The FMA monitors such developments in particular for potential money laundering and terrorist financing risks. Intensified international cooperation and targeted risk mitigation measures remain key regulatory focuses in 2025.

Incoming & outgoing foreign payments  
Selected high-risk countries - credit institution sector (2024)



Aggregated incoming foreign payments: EUR 24.89 billion; Aggregated outgoing foreign payments: EUR 39.75 billion  
Source: OeNB, Foreign Payments 2024, own calculations

Figure 18: Incoming & outgoing foreign payments for selected high-risk countries in the CI sector (2024)

## 4 OUTLOOK

**The new European AML/CFT supervisory authority, AMLA, started work in early 2025. It has already moved into its premises in Frankfurt and is continuing to make progress in terms of its organisational and staffing structure. In addition, work has begun in its first work streams.**

Bruna Szego (previously at Banca d'Italia) has been appointed as AMLA's chairperson. The five members of AMLA's Executive Board were also fixed in Q2 2025. The initial meeting of the AMLA General Board was held in March 2025. From mid-2025 onwards, AMLA will become increasingly operationally active. The FMA will continue to make use of its years of experience and expertise to contribute constructively, adopting a proactive stance for establishing the foundations of the new supervisory system.

**The Financial Markets Anti-Money Laundering Act's ("FM-GwG"; Finanzmarkt-Geldwäschegesetz) scope was extended on 15 December 2024. The new arrangements relate to the prevention of the non-implementation and evasion of targeted financial sanctions in relation to financing of proliferation**

for financial market participants. The amendment implemented recommendations issued by the FATF's international anti-money laundering experts as well as EU regulatory standards, some of which had been pending for years. Proliferation is the broader distribution of atomic, biological, or chemical weapons of mass destruction, and the accompanying delivery systems (e.g. rockets) and products used to manufacture them (e.g. certain raw materials and raw products) including the necessary related know-how (e.g. for production purposes). The material provisions relate to the organisational measures in relation to risk management requirements to be implemented. Subsequently, from 1 January 2026, the FMA will also take over the duties performed by the OeNB in the area supervision of financial sanctions. Financial market participants are also required to implement strategies, checks and procedures for minimising risk in this area. These arrangements are set out in the Sanctions Act 2024 (*Sanktionengesetz* 2024). The scope of supervised entities will be extended to cover insurance companies, investment firms and crypto-asset service providers, to guarantee comprehensive observance of financial sanctions. The reform brings supervision in this field together in a single authority, strengthens transparency, and increases its power in enforcement. The FMA will cooperate closely with the OeNB during 2025, in monitoring observance of financial sanctions at credit institutions and financial institutions as well as payment service providers, before taking over duties fully from 1 January 2026. In 2025, the FMA will already participate in the OeNB's on-site inspections in relation to financial sanctions, as well as also conducting on-site inspections in its own right, on the OeNB's behalf (support measures under the Sanctions Act 2024). The purpose of this is to ensure the best possible gradual transferring of duties. In the future, there some inspections will focus exclusively on either AML/CFT or financial sanctions, as well as combined inspections. Furthermore, the FMA will adjust its annual data query of obliged entities for risk classification purposes in line with its new supervisory competences.

**The Markets in Crypto Assets Regulation (MiCAR) and the Transfer of Funds Regulation (TFR) entering into force on 30 December 2024 created a harmonised and comprehensive regulatory framework for crypto-assets in the EU.** MiCAR replaces the previous registration procedure for VASPs and introduces an extended definition for CASPs. At the same time, the TFR introduces stricter traceability requirements for crypto-assets transfers. These new rules present major challenges especially for smaller crypto service providers, who are required to fulfil high regulatory standards, especially in the area of AML/CFT. The FMA will actively accompany the transitional period to ensure the seamless integration of previously registered VASPs into the MiCAR regime, and to monitor the consistent observance of the new requirements.

**Since Q4 2024, Austria has been being assessed for the fifth time by the FATF regarding its implementation and effective application of the 40 FATF Recommendations.** The country assessment, conducted by the International Monetary Fund, started in November 2024 and is expected to last for 15 months. The inspection team will be on-site in Vienna in June/July 2025 to conduct interviews with various stakeholders (supervisory authorities as well as industry representatives). Particular significance is placed on such meetings with ministries, supervisory authorities as well as industry representatives. The final mutual evaluation report is planned to be discussed and accepted at the FATF's Plenary Meeting in February 2026.