COUNCIL OF EUROPE'S COMMITTEE OF EXPERTS ON THE
EVALUATION OF ANTI-MONEY LAUNDERING MEASURES
AND THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2025)24

Anti-money laundering and counter-terrorist financing measures

Poland

3rd Enhanced Follow-up Report & Technical Compliance Re-Rating

November 2025

Follow-up report

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The 3rd Enhanced Follow-up Report and Technical Compliance Re-Rating on Poland was adopted by the MONEYVAL Committee through written procedure (3 November 2025).

Poland: 3rd Enhanced Follow-up Report

I. INTRODUCTION

1. The 5th round mutual evaluation report[1] (MER) of Poland was adopted in December 2021. Given the results of the MER, Poland was placed in enhanced follow-up[2] and its 1st Enhanced Follow-up Report (FUR) was adopted in December 2023 and 2nd enhanced FUR was adopted in December 2024. This report analyses the progress of Poland in addressing the technical compliance (TC) deficiencies identified in its MER and/or subsequent FUR, where requested to do so by the country. Re-ratings are given where sufficient progress has been made. Overall, the expectation is that countries will have addressed most, if not all, TC deficiencies by the end of the third year from the adoption of their MER.[3]

2. The assessment of the request of Poland for technical compliance re-ratings and the preparation of this report were undertaken by the following Rapporteur team (together with the MONEYVAL Secretariat):

- The United Kingdom

3. Section III of this report summarises the progress made by Poland in improving technical compliance. Section IV sets out the conclusion and a table showing which Recommendations have been re-rated.

4. In line with MONEYVAL's Rules of Procedure, the follow-up process is desk-based – using information provided by the authorities, including revised legislation. It does not address what progress a country has made to improve the effectiveness of changes introduced by the country.

II. BACKGROUND, RISK AND CONTEXT

5. Poland reported that it had conducted analysis of the non-profit organisation (NPO) sector as part of national risk assessment (NRA) in 2023. In accordance with the NRA, the risk of TF abuse for NPO sector is estimated as medium. In terms of the recommendations requested for a re-rating it is worthy to mention the enactment of EU Regulation 2023/1114 on Markets in Crypto-assets.

III. OVERVIEW OF PROGRESS TO IMPROVE TECHNICAL COMPLIANCE

6. This section summarises the progress made by Poland to improve its technical compliance by addressing the technical compliance deficiencies identified in the MER and applicable subsequent FUR for which the authorities have requested a re-rating (Recommendation (R.) 8 and R.15). The authorities requested a re-rating also for R.26, however this request has not been considered as the country's legal, operational and institutional framework has not changed since its last review.

7. For the rest of the Recommendations rated as partially compliant (PC) (R.5, R.7, R.13, R.17, R.18, R.19, R.20, R.22, R.28, R.32, R.35) the authorities did not request a re-rating.

8. This report takes into consideration only relevant laws, regulations or other anti-money laundering and combating financing of terrorism (AML/CFT measures) that are in force and effect at the time that Poland submitted its country reporting template – at least six months before the follow-up report is due to be considered by MONEYVAL.[4]

1. Source available at https://www.coe.int/en/web/moneyval/jurisdictions/poland.
2. Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up involves a more intensive process of follow-up.
3. Poland's submission of the country report for this FUR preceded a Plenary decision to amend the Rules of Procedure for the 5th Round of Mutual Evaluations. Therefore, the 2013 version of the Methodology applies to this technical compliance re-rating exercise.
4. This rule may be relaxed in the exceptional case where legislation is not yet in force at the six-month deadline, but the text will not change and will be in force by the time of the plenary. In other words, the legislation has been enacted, but it is

IV. PROGRESS TO ADDRESS TECHNICAL COMPLIANCE DEFICIENCIES IDENTIFIED IN THE MER AND SUBSEQUENT FURS

9. Poland has made progress to address the technical compliance deficiencies identified in the MER and applicable subsequent FURs. As a result of this progress, Poland has been re-rated on R.8. The country asked for R.15, which is also analysed but no re-rating has been provided.

10. Annex A provides a description of the country's compliance with each Recommendation that is reassessed, set out by criterion, with all criteria covered. Annex B provides the consolidated list of remaining deficiencies of the re-assessed Recommendations.

V. CONCLUSION

11. Overall, in light of the progress made by Poland since its MER or 2nd enhanced FUR was adopted, its technical compliance with the Financial Action Task Force (FATF) Recommendations has been re-rated as follows.

Table 1. Technical compliance with re-ratings, November 2025

R.1	R.2	R.3	R.4	R.5
LC (FUR2 2024) ~~PC (MER)~~	LC (MER)	LC (MER)	LC (MER)	PC (MER)
R.6	R.7	R.8	R.9	R.10
LC (MER)	PC (MER)	**LC (FUR3 2025)** ~~PC (MER)~~	C (MER)	LC (MER)
R.11	R.12	R.13	R.14	R.15
LC (MER)	LC (MER)	PC (MER)	LC (MER)	PC (FUR3 2025) ~~PC (FUR2 2024)~~ ~~PC (FUR1 2023)~~ ~~PC (MER)~~
R.16	R.17	R.18	R.19	R.20
LC (MER)	PC (MER)	PC (MER)	PC (MER)	PC (MER)
R.21	R.22	R.23	R.24	R.25
LC (MER)	PC (MER)	LC (MER)	LC (MER)	LC (MER)
R.26	R.27	R.28	R.29	R.30
PC (FUR2 2024) PC (MER)	LC (MER)	PC (MER)	C (MER)	LC (MER)
R.31	R.32	R.33	R.34	R.35
LC (MER)	PC (MER)	C (FUR2 2024) ~~PC (MER)~~	LC (FUR1 2023) ~~PC (MER)~~	PC (MER)
R.36	R.37	R.38	R.39	R.40
LC (MER)	LC (MER)	LC (MER)	LC (MER)	LC (MER)

Note: There are four possible levels of technical compliance: compliant (C), largely compliant (LC), partially compliant (PC), and non-compliant (NC).

12. The following "big six" Recommendations[5] remain PC: R.5 and R.20. Accordingly, in line with Rule 23 of the Rules of Procedure for the 5th Round of Mutual Evaluations, Poland will be placed into compliance enhancing procedures and expected to report at the next plenary on progress in addressing remaining shortcomings under both Recommendations. The Plenary is asked to confirm that step 1 should apply.

awaiting the expiry of an implementation or transitional period before it is enforceable. In all other cases the procedural deadlines should be strictly followed to ensure that experts have sufficient time to do their analysis.

5. The "big six" Recommendations are: R.3, R.5, R.6, R.10, R.11 and R.20.

13. Poland will remain in enhanced follow-up. It is recommended that: (i) Poland should continue to report back to MONEYVAL on progress to strengthen its implementation of AML/CFT measures; and (ii) in line with Rule 23 of the Rules of Procedures for the 5th Round of Mutual Evaluations, Poland reports back in one year's time.

Annex A: Reassessed Recommendations

Recommendation 8 – Non-profit organisations

	Year	Rating and subsequent re-rating
MER	2021	PC
FUR1	2023	PC (no upgrade requested)
FUR 2	2024	PC (no upgrade requested)
FUR 3	2025	↑ LC (upgrade requested)

1. In the 5th round MER of 2021, Poland was rated PC with R. 8. The main deficiencies were in relation to: the assessment of features and types of NPOs which, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse, with a negative impact on the risk-based supervision; no review of the adequacy of measures, related to the subset of the NPO sector that may be abused for terrorism financing; limited involvement of the NPO sector in any activity to develop and refine best practices to address FT risks; no specific and complex mechanisms of cooperation between the competent authorities.

2. **Criterion 8.1** –

(a) The 2023 NRA and Annex 2 The Analysis of Money Laundering and Terrorist financing risks by sectors conducts a risk assessment of their NPO sector which consists of foundations and associations. It outlines that foundations and associations operating internationally and engaged in religious activities (posing high risk) and those carrying out activities related to social and humanitarian aid (increased risk) were the subset of organisations which fall within the FATF definition. According to the NRA which in 2020 there were 138 000 associations and foundations out of which roughly 50% were operational. The subset of associations and foundations posing high and increased risk accounted for 3,4 and 7,9% respectively. Polish authorities maintain statistics on different characteristics of the NPO sector. E.g. in 2022 the number of active associations and foundations amounted to 73 500 and out of this number 3,7 and 17,2% were ranked as high and increased risk respectively. Thus, through a sectoral risk assessment Poland have identified the characteristics of the subset of NPO that falls within the FATF definition and establishes a framework within which they could identify the subset of higher risk NPOs.

(b) Poland has identified amongst the *"most common methods used to finance terrorism"* the charitable organisations, as they benefit from public trust, have access to significant and diverse sources of funding, and their financial activities are often characterised by high cash flow. Further on, risk scenarios on the usage of charity organisations for financing of terrorism are listed and concluded that in Poland, the use of charitable organisations constitutes a medium threat of financing terrorism. In addition, risk areas at the EU level related to the use of non-profit organisations to support terrorist activities are indicated in Supra-national risk assessment (SNRA).

(c) In line with the AML/CFT strategy adopted in 2021 Poland adopted a unified reporting form for foundations on 20.12.2022. No other actions have been reported as implemented. In addition, financial institutions are issued guidelines (adopted by the European Banking Authority in March 2023), which provide for generic customer due diligence (CDD) to all foundations and associations. New actions are foreseen for implementation in 2025 AML/CFT Strategy aimed at the preparations for risk assessment of NPOs and improving the efficiency of supervision over NPOs. However, the implementation of specific actions is still work in progress.

(d) The reassessment of the sector's potential vulnerabilities to terrorist activities is to be conducted at least on a biannual basis or whenever necessary in the context of the NRA. At EU level, the regular review of new information and assessment of the sector is executed through the SNRA, which, based on Article 6(1) of the Directive 2015/849, shall be updated every two years, or more frequently if appropriate. So far, information on threats and vulnerabilities related to the non-profit sector has been included both in the 2017 and 2019 assessments. The 2023 NRA (covering the period of 2020-2022) presents a comprehensive assessment of the sector. Authorities informed that a new risk assessment was being prepared in line with the frequency requirement of risk assessment.

3. **Criterion 8.2** –

(a) There are some provisions to promote accountability, integrity and public confidence contained in the legal acts governing the NPOs.[6] Article 10(5) of the Law on Associations provides that the "authorities" of the association, the procedure for their election, the method of electing supplementary authority members and their "competences" should be written in the association statute. Associations must have a management board and an internal control authority. Nevertheless, there is no referral to any integrity requirements applicable to the administration and management of the associations. Turning to foundations, the "sponsor" shall determine its statute, its name, address, assets, purposes, principles, forms and scope of activity, composition and organisational structure of governing board, and the procedure for appointing members of that body, as well as the responsibilities and powers of that body and its members. As in the case of associations, no integrity requirements are applicable to the administration and management. There are no policies to promote accountability, integrity, and public confidence in the administration and management of NPOs. The establishment of bodies such as the National Institute of Freedom, the Public Benefit Committee, Council of Public Benefit Work might be considered as steps to promote accountability, integrity and public trust in the NPO sector, as they have prerogatives indirectly related to accountability, integrity and public confidence such as *"creating mechanisms for the provision of information on standards of public benefit organisations and on identified cases of breaches of these standards"*. Nevertheless, the mere establishment of such advisory and coordination bodies cannot be considered as fully meeting the requirements of 8.2.

(b) The NPOs are obliged entities under the AML/CFT Act; therefore, the legal requirement for the employees to participate in AML/CFT training programs is stated therein. Guidelines and articles regarding AML/CFT obligations of NPOs were published by General Inspector of Financial Information (GIFI) on the most popular website for non-profit organisations (NGO.pl) in 2020, providing information sources that NPOs can consult and measures to take to protect themselves against abuse for TF. Indications on the application of targeted financial sanctions (TFS) are included therein. The GIFI regularly offers updated editions of a free e-learning course on AML/CFT to all obligated entities. Nevertheless, educational programmes to raise and deepen awareness among the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks are absent.

(c) GIFI regularly organises workshops dedicated to NPOs in the context of AML/CFT which outlines the risk rating for NPO and outlines the potential vulnerabilities of NPO to terrorist financing. However, authorities have shown limited evidence on initiatives involve the NPO sector into developing and refining best practices.

(d) The introduction of associations and foundations performing cash payments equal to or exceeding the equivalent of 10 000 euros (EUR) (regardless of whether the payment is

6. Act of 7 April 1989 - Associations Law, the Act of 6 April 1984 on Foundations and the AML/CFT Act.

performed as a single operation or as several operations which seem linked to each other) to the catalogue of obliged entities gives an impulse to conduct non-cash transactions through financial institutions. Several activities promoting cashless transactions in Poland have been carried out by public administration and private entities, participants of the market of payment services, commercial banks and cooperative banks. The projects concerned the NPO sector, among others.

4. **Criterion 8.3** – The existing legal framework, in particular the AML/CFT Act, provides a mechanism for risk-based supervision and monitoring of the NPO sector, including from the perspective of potential TF abuse.

5. According to Article 131 of the AML/CFT Act, the control (by GIFI, heads of customs and tax control offices, governors of provinces or district governors and competent ministers of governors of the district) shall be performed based on annual control plans, which contains the list of entities subject to control, the scope of the control and its' justification. When developing the control plans, the ML/TF risks are taken into account, as defined in the NRA and SNRA.

6. According to Articles 27 and 28 of the AML/CFT Act, when identifying and assessing risks associated with money laundering and financing of terrorism referring in their area of work, the obligated institutions shall consider the NRA and SNRA. At GIFI's request, they shall provide their risk assessments and other information potentially affecting the national risk assessment.

7. The GIFI exercises control over the foundations and associations (which are obligated institutions) and the compliance with their duties in the AML/CFT area. The established supervision aims to evaluate the compliance of the organisation's operations with the provisions of law and the statutes and with the purpose for which it was established and includes financial accountability.

8. **Criterion 8.4** –

(a) Supervision of NPOs with the legal requirements is based on the general provisions stated in Article 131 of the AML/CFT Act, whereby supervisors must discharge their responsibilities on the basis of annual plans containing, in particular, the list of entities subject to control, the scope of control and the justification for the plan. The plans must take into account money laundering and terrorist financing risks, in particular as defined in the NRA and in Article 6 of EU Directive 2015/849. In addition, under Article 132, in the course of its coordinating role, the GIFI must make information available to other supervisors annually on areas and sectors particularly exposed to the risk of money laundering or terrorist financing. (see also 26.5).

The AML/CFT control over the activity of associations and foundations is exercised by the GIFI, with the involvement of other competent authorities if need be. The control shall be performed based on annual control plans of GIFI, UCS, Ministries, voivodes and governors of districts.

(b) Supervisory and control authorities have the right to impose effective, proportionate and dissuasive sanctions for violations committed by NPOs. Violations are subject to administrative penalties, such as: the order to cease undertaking specific activities; revocation of a license or a permit or deleting from the register of regulated activity; prohibition from holding a managerial position by a person responsible over a period of maximum one year and financial penalties.

9. **Criterion 8.5** –

(a) General provisions regarding information sharing are specified in the Regulation of the Chairman of the Public Benefit Committee on the exchange of information concerning public benefit organisations of 25 October 2018. This mainly concerns the Minister of Justice, the Director of Supreme Audit Office, the minister competent for public finance in relation to public

benefit organisations. More specific and complex mechanisms of co-operation between the competent authorities seem to be lacking.

(b) The main authorities responsible for examining those NPOs suspected of either being exploited by or actively supporting terrorist activity or terrorist organisations are the GIFI and the ISA. When carrying out its duties, the Internal Security Agency (ISA) monitors circles that are prone to the risk of involvement in activities of terrorist nature or activities that could pose a threat to the economic stability of the state. Within the mentioned activities, ISA analyses, among others, activity of the NPOs from the perspective of potential risk.

(c) Associations and foundations are obliged to register in the National Court Register. The information contained in the National Court Register (including information on the administration and management of associations with legal personality and foundations) is publicly available. Turning to financial and programmatic information, these can be obtained on the basis of Law Enforcement Agency's prerogative depending on the stage of the investigation.

(d) The general rules of reporting of obligated institutions to the GIFI would apply in the case of NPOs. In case of TF indications, the GIFI will disseminate the case to the Prosecutor's Office. The general powers of investigative bodies provide for the relevant procedures to ensure that –under situations described in the criterion – relevant information is shared with competent authorities in order to take preventive or investigative actions. The Head of the ISA is charged with the coordination of analytical and informative activities performed by other authorities. In the frame of this coordination, the ISA collects, processes and analyses different types of information which are i.a. linked to the NPOs activities.

10. **Criterion 8.6** – International co-operation and information exchange with foreign counterparts is regulated by the general provisions of the legal framework, regardless of the connection with TF. According to the AML/CFT Act, the duties of the GIFI comprise undertaking actions with the aim of counteracting money laundering and financing of terrorism, in particular: exchange of information with cooperating units and competent authorities of other countries, as well as foreign institutions and international organisations dealing with combating money laundering or financing of terrorism. The ISA also has competence in this matter, currently being able to cooperate with over 100 partners from different countries, as well as with specialised organisations in security issues (among others Counter Terrorist Group, Club of Berne, Europol, Interpol, etc.).

Weighting and Conclusion

11. Minor shortcomings remain in respect of: (i) limited actions reported as part of the review of the adequacy of measures relating to the subset of NPOs that may be abused for TF purposes (c.8.1(c)); (ii) lack of comprehensive policies to promote accountability, integrity, and public confidence in the administration and management of NPOs (c.8.2(a)); (iii) lack of educational programmes for donor community about the potential vulnerabilities of NPOs to TF abuse and TF risks (c.8.2(b)); (iv) limited involvement of the NPO sector in any activity to develop and refine best practices to address FT risks (c.8.2(c)); and (v) lack of specific and complex mechanisms of co-operation between the competent authorities (c.8.5(a)). **R.8 is re-rated LC.**

Recommendation 15 – New technologies

	Year	Rating
MER	2021	PC
FUR1	2023	PC (upgrade requested, maintained at PC)
FUR 2	2024	PC (upgrade requested, maintained at PC)
FUR 3	2025	PC (upgrade requested, maintained at PC)

1. Poland was rated PC for R.15 in its 5th round MER. Poland did not have in place specific requirements, so that obligated institutions had to assess the ML/TF risks of new technologies, products, services or business practices before releasing them. Regarding the legal framework for virtual asset service providers (VASPs), although they had been included as obligated institutions and their risks had been considered within the NRA, there was no obligation for them to officially register, the requirements of wire transfers of R.16 were not applicable to them, and the scope of the definition of virtual asset-related activities contained in the AML/CFT Act was not fully in line with that of the FATF.

2. The AML/CFT Act, Regulation (EU) 2022/2554, or Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA) do not refer specifically to obligated institutions identifying and assessing the money laundering and terrorist financing risks present due to the development of new products, new business practices, use of new or developing technologies - for both pre-existing and / or new products. Information provided by GIFI, including annexes: FAQ quarterly reporting, GIFI communications 62-97 and typological newsletter GIFI (2-2024), demonstrates outreach to obliged institutions about money laundering and terrorist financing risks, they do not, however, provide guidance specifically about development of new products, new business practices, use of new or developing technologies.

3. **Criterion 15.2** – Requirements of c.15.2 (a) and (b) are not regulated in domestic legislation. Notwithstanding that, Regulation (EU) 2023/1114 Article 6(1)(i) does require obligated institutions- in any crypto-asset white paper relating to markets- to contain information on the risks and this must be published before offering (Article 9(1)). Information on the risks required to be determined is further clarified in Annex I of the Regulations, these do not, however, specifically fulfil the requirements of 15.2 (a) and (b).

4. The GIFI's communication No 73 (annex GIFI communications (62-97)) does reference obligated institutions requirements to apply measures and manage the risks of money laundering and terrorist financing risks generally, nevertheless, it does not specifically require the necessary particulars of 15.2 (a) and (b).

5. The Typological Newsletter issued by the GIFI (2-2024) relating to the risk of crowdfunding, does refer to technological advances and new emerging challenges that may arise as the result of the use of new technologies. It advises obligated institutions to remain vigilant about adapting their AML measures to effectively combat emerging threats, however, it does not specifically fulfil the requirements of 15.2 (a) and (b).

6. **Criterion 15.3** –

(a) At EU level, the European Commission conducts and publishes an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities in line with the requirements of the EU Directive 2015/849 as amended by EU Directive 2018/843 (Article 6) that also identifies and assesses the risks emerging from virtual assets (VAs) and the activities and operations from VASPs. The EU level risk assessment

shall be updated by a report at least every two years.

Poland has considered virtual currencies in the annexes of the 2019 NRA, where several money laundering and terrorist financing risks scenarios are analysed. The main conclusions are that decentralised cryptocurrencies/VAs constitute a high threat of money laundering, while centralised ones create a medium-level threat of money laundering, and the main vulnerabilities identified are the limited information available to the GIFI in this regard, as well as difficulty in the usage of the products and the need of specialised knowledge. In terms of terrorist financing, it is considered that the use of virtual currencies for that purpose entails a medium-level threat. The 2023 NRA also assesses the risks of virtual currencies in its Annex II. Conclusions have remained relatively similar, with a high level of ML threat (due to potential misuse by international organised criminal groups) and vulnerability (due to ease of access to services, the possibility to hide customer identification data, or the international nature of transactions) for both decentralised and centralised cryptocurrencies and equally high threat and vulnerability levels for the same products in the case of TF (due to potential misuse of collection of investor funds for the issuance of new cryptocurrencies or misuse of donations to fund terrorist fighters).

(b) Entities pursuing economic activities involving providing services related to virtual currencies are obligated institutions of the AML/CFT Act, according to Article (2)(1)(12). VASPs that do fall within the definition of the AML/CFT Act are obligated institutions, and therefore subject to all the provisions of the Act as any other type of obligated institution would be.

(c) As reporting entities, VASPs included in the definition of Article (2)(1)(12) are equally subject to the requirements set by Article 27 of the AML/CFT Act, in which obligated institutions must identify and assess the ML/TF risks associated with their activities, taking into account the risk factors related to customers, geographical areas, products and services, transactions and delivery channels and implement internal control procedures pursuant Article 50 of the same law. The deficiency under c.1.10(d) does not apply to VASPs, in the absence of any professional self-regulatory body or association for the sector.

7. **Criterion 15.4** –

a) At EU level, a person providing crypto asset services9 is subject to prior authorisation by the authority of the member state where it has its registered office (EU Regulation 2023/1114 on markets in crypto assets, Article 59). A crypto asset service provider under EU law may be: (i) a legal person; or (ii) another undertaking - if the legal form of that undertaking ensures a level of protection for third parties' interests equivalent to that afforded by legal persons and if it is subject to equivalent prudential supervision appropriate to its legal form (EU Regulation 2023/1114 or markets in crypto assets, Article 59(3)). These requirements on the legal form of undertakings exclude natural persons from being authorised as crypto asset service providers (so c.15.4(a)(ii) is not applicable).

The authorisation process for service providers includes a "fit and proper assessment" and authorisation can be granted only if members of management bodies and shareholders or members are of sufficiently "good repute" (EU Regulation 2023/1114 on markets in crypto assets, Article 21(2) and Article 63(10)).

Pursuant to Article 129m of the AML/CFT Act, virtual currency activities referred to in Article 2(1)(12) of the AML/CFT Act are regulated activities and a prerequisite for its performance is obtaining an entry in the register of virtual currency service providers. The obligation to obtain

an entry in the register of virtual currency service providers applies to all entrepreneurs[7] conducting such activities on the territory of Poland. The scope of VASPs covered in this article does not fully match the FATF definition, as the activities of participation in the provision of financial services related to an issuer's offer and/or sale of a VA are not covered. MiCA, directly applicable to EU member states since 30 December 2024, contains a broader definition of "crypto-asset service providers". Although Polish legislation is in contradiction with MiCA, the provisions of the later will supersede. EU Regulation 2023/1113 on information accompanying transfers of funds and certain crypto-assets, amends Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and incorporates the same definition.

b) At EU level, authorisation processes under EU Regulation 2023/1114 include assessments that members of the management body are sufficiently reputable and competent and that shareholders or members that have a qualifying holding fulfil fit and proper requirements (Articles 62, 63, 64 and 68 for crypto asset service providers). These provisions empower authorities to prevent individuals convicted of offences relating to money laundering or terrorist financing or of any other offences that affect their good repute from assuming relevant functions. Regarding shareholders and members whether direct or indirect, that have qualifying holdings, proof is required that those persons are of sufficiently good repute (Article 62 (2) (h)).

   Article 129n of the AML/CFT Act establishes a requirement of no criminal record[8] that applies to natural persons carrying out activities in the field of virtual currencies, as well as to natural persons who are partners or members of the governing bodies of legal persons or organisational units without legal personality and the beneficial owners of entities carrying out such activities. However, there is no requirement covering criminals' associates. Though MiCA is directly applicable to EU member states since 30 December 2024 and supersedes the national legislation, Poland has not yet adopted legislation assigning tasks and powers under MiCA to competent authorities.

8. **Criterion 15.5** – Regulation at EU level prohibits the provision of services without authorisation (Article 59 (1) EU Regulation 2023/1114). EU Directive 2015/849 and EU Regulation 2023/1114 task competent authorities in member states to ensure action is taken to identify persons that carry out VASP activities without licensing or registration and to ensure compliance with authorisation requirements by taking supervisory measures and applying sanctions. EU Regulation 2023/1114, Article 94 (1) (h) stipulates that competent authorities, in accordance with national law, shall have the power to order the immediate cessation of the activity where there is a reason to assume that a person is providing crypto-asset services without authorisation. The prerequisite of "reason to assume" the provision of service leaves sufficient room to take targeted action at service providers that address the market.

9. At EU level, the European Securities and Markets Authority assist efforts to ensure compliance by keeping a register of operators found to have provided services in breach of the authorization requirement (Article 110 EU Regulation 2023/1114).

7. Pursuant to Article 4(1) of the Act of 6 March 2018 - Entrepreneurs' Law, an entrepreneur is a natural person, a legal person or an organisational unit that is not a legal person, to which a separate act grants legal capacity, performing business activity.
8. Finally convicted of an intentional crime against the operation of state institutions and local government, against the justice system, against the credibility of documents, against property, against economic turnover and property interests in civil law transactions, against money and security trading, for the crime referred to in Article 165a of the Act of 6 June 1997 – Penal Code, a crime committed for the purpose of material or personal gain or an intentional fiscal offense.

10. Article 153b of the AML/CFT Act provides an administrative sanction in a form of a fine up to 100 000 Polish zlotys (EUR 23 600 approximately) for performance of virtual currency activities by an entity that has not obtained an entry in the register of virtual currency service providers. The authority competent to impose the fine is the minister responsible for public finance (Article 129q (2)(4) of the AML/CFT Act), as the competent authority for the register of virtual currencies service providers (Article 129p). Additionally, as any other business operating in Poland, obtaining an entry in the business register of companies or trusts is mandatory and non-compliance is criminally punishable under Article 60(1) of the Code of Offences.

11. **Criterion 15.6** –

(a) At EU level, when assessed for market entry, crypto asset service providers are required to have mechanisms and controls in place that ensure compliance with AML/CFT requirements (EU Regulation 2023/1114, Articles 63 (2) to (10)).

VASPs included under Article (2)(1)(12) of the AML/CFT Act as reporting entities are subject to compliance controls of the GIFI. In terms of risk-based approach, the control capabilities of the GIFI take into account the risk of ML/TF of the institutions that will be subject to those control measures (Article 131(2)), however this provision does not cover the overarching requirements for the intensity and frequency of supervision as a whole (onsite and offsite) to be risk-based. In relation to other applicable deficiencies under c.26.5, the GIFI has adopted, between 2022 and 2023, several measures to further converge their supervisory frameworks with a risk-based approach. These measures would include the adoption of a new "control procedure" for supervision and an extension of the scope of the information submitted quarterly by obligated institutions. GIFI determines the frequency through an annual supervision plan, pursuant to Article 131 of the AML/CFT Act. However, the overall frequency of supervision planning (annual) does not anticipate emerging risks which could require a shorter timescale for risk assessment and a pivot in supervision planning and effective supervisory tools. Overall, elements of c.26.5(a) and (c) are not covered. These issues have a cascading effect to c.26.6.

(b) EU Directive 2015/849 and EU Regulation 2023/1114 task competent authorities in member states to ensure compliance by crypto asset service providers with requirements to combat money laundering and terrorist financing. EU Regulation 2023/1114, Article 94, stipulates that competent authorities in accordance with national law shall have the power to inspect and to compel documents. The withdrawal of the authorisation of crypto asset service providers is regulated at EU level in Article 64 of EU Regulation 2023/1114 and, alongside other administrative penalties and administrative measures, shall also be implemented at national level (EU Regulation 2023/1114, Article 111).

As stated above, VASPs are registered obligated institutions subject to the controls implemented by the GIFI to ensure compliance with AML/CFT requirements. Chapter 12 of the AML/CFT Act defines how the "controls" (referring to onsite inspections) must be conducted and their scope. Similarly, as obligated institutions, VASPs are subject to the penalties for non-compliance set in Articles 153 and 154 of the AML/CFT law, applicable when any of the infringements established in Articles 147-149 are performed. Article 129w of the AML/CFT Act provides for the possibility to delete from the register of virtual currency service providers those providers who fail to meet the registration requirements or that have provided false information upon registration, and upon an application of the GIFI following the imposition of an administrative penalty referred to in Article 150(1)(2) (order to cease undertaking certain activities), which can be imposed for any of the infringements of the AML/CFT Act of Articles 147-149.

12. **Criterion 15.7** – After amendment by EU Regulation 2023/1113 EU Directive 2015/849 (Article 18) mandates the European Banking Authority to issue guidelines on risk variables and risk factors to be taken into account by crypto-asset service providers when entering into business relationships or carrying out transactions in crypto-assets. (Guidelines published on 16 January 2024 and to be applied from issued from 30 December 2024).

13. The AML/CFT Act establishes a provision for which the GIFI must make knowledge and inform about ML/TF-related issues in a public information bulletin on the website of the Ministry of Finance. Specific guidance has been provided, in terms of AML/CFT, aimed specifically to the VASPs sector and the particular risks they may face, as well to other obligated institutions concerning VA risks. In particular, the GIFI published on its website a number of communications addressed to obligated institutions (including some dedicated to VASPs), regarding conducting business in the field of virtual currencies, e.g. GIFI communications No. 67, 71, 77, 79, as well as the typological newsletter No. 1 of 2024, which covers activities in the field of VAs, the application of MiCA and the "travel rule" and some relevant VA typologies and risk indicators.

14. Other outreach and awareness actions included meetings to explain the AML/CFT requirements to VASPs, as well as the rest of obligated institutions, or the participation of VASPs in the national risk assessments of their sector.

15. **Criterion 15.8** –

(a) EU Directive 2015/849 and EU Regulation 2023/1114 require member states to provide competent authorities, in accordance with national law, with the power to apply appropriate administrative penalties and other administrative measures. Article 111 of EU Regulation 2023/1114 stipulates sanctions for a number of infringements including minimum fines.

As explained in c.15.6(b), VASPs, as obligated institutions, are subject to the penalties set in Articles 153 and 154 of the AML/CFT law, applicable when any of the infringements established in Articles 147-149 are performed. Deficiencies under c.35.1 are applicable, including the lack of the authority of the supervisor to suspend the activities of a registered VASP or to direct the obliged institution to take specific actions. Financial penalties available to supervisors are not proportionate or dissuasive and this has a cascading effect to c.35.2.

(b) The sanctions mentioned in the paragraph above are equally applicable to senior management and employees holding management functions (directors) of the obligated institution, according to Article 154, which states that the penalties may also be imposed on the persons in Articles 6-8 (that include the natural persons referred), additionally to the legal person/obligated institution. Deficiencies under c.35.2 are applicable.

16. **Criterion 15.9** – Preventive measures under R.10-21 are not applicable to VASPs participating in and providing financial services related to an issuer's offer and/or sale of a virtual asset as the latters are not foreseen as OEs.

17. Other VASPs are subject to preventive measures under R.10-21, however relevant deficiencies thereunder apply, including the lack of a prohibition for keeping anonymous accounts or accounts in obviously fictitious names remains. Legal frameworks described under the analysis of R.13 and R.14 do not apply to VASPs.

(a) Pursuant to Article 35(1)(2)(c) of the AML/CFT Act, VASPs included under Article (2)(1)(12) shall apply CDD measures when carrying out an occasional transaction using virtual currency with an equivalent of EUR 1 000 or more.

(b) EU Regulation 2023/1113 repeals and replaces EU Regulation 2015/847 formerly regulating the transfer of funds and extends the scope to cover both transfer of funds and transfer of VAs.

i. Article 14 (1) of EU Regulation 2023/1113 requires the originating crypto asset service provider to obtain and hold originator information (Article 14 (1), (2) and (3)) and to submit it to the beneficiary service provider immediately (in advance or simultaneously) and securely (Article 14 (4)). Before transferring crypto-assets, the service provider shall verify the accuracy (Article 14 (6). In accordance with Article 24 of EU Regulation 2023/1113, information has to be provided to competent authorities in the Member State in which they are established. The originating crypto asset service provider submits beneficiary information to the beneficiary's service provider in line with Article 14 (2) of Regulation 2023/1113 and holds it on record according to Article 26 (1) Regulation 2023/1113.

   The distributed ledger address (DLT) information is required for both the originator and the beneficiary. If the transfer does not occur on the DLT, the Regulation requires the crypto-asset account number instead (EU Regulation 2023/1113, Article 14 (1) (b) and (2) (b)).

   EU Regulation 2023/1113 imposes additional requirements to be implemented in the case of transfers being made to self-hosted addresses (where no crypto asset service provider is involved on the originator or beneficiary side), such as individual identification of transfers and ensuring that the address is controlled by the originator/beneficiary.

   EU Regulation 2023/1113 does not make a distinction between crypto-asset transfers within and outside the EU, treating all crypto-asset transfers as cross-border.

ii. Article 16 of EU Regulation 2023/1113 requires the crypto asset service provider of the beneficiary to implement effective procedures, which may include post-event or real-time monitoring, to identify transfers that lack required originator or beneficiary information and to verify accuracy of the beneficiary information (EU Regulation 2023/1113, Article 16 (1) and (3)). Service providers are obliged to make information available to competent authorities on request according to Article 24 of EU Regulation 2023/1113.

iii. EU Regulation 2023/1113 covers the requirements of Recommendation 16 and applies them to virtual asset transfers, especially on monitoring and risk-based procedures (Article 14 (8) and Article 16 (1)) as well as freezing action and prohibiting transactions with designated persons and entities (Article 23).

iv. Financial institutions are covered by the scope of relevant provision of EU Regulation 2023/1113 through the broad definition of crypto asset service provider in Article 3 (1) 15 of that Regulation with reference to Article 3 (1) (15) EU Regulation 2023/1114, including credit institutions that provide crypto asset services in accordance with Article 59, 60 of EU Regulation 2023/1114.

18. **Criterion 15.10** – VASPs that are reporting entities under the AML/CFT Act, must implement the restrictive measures and freezing mechanisms defined in Article 119 of the Act to the entities described in Article 118(1), which include the list announced by the GIFI pursuant to the relevant United Nations Security Council Resolutions (UNSCRs). However, the concerns related to the timeliness in the implementation of the UNSCRs by obligated institutions, notwithstanding the Guidance published at an EU level through the European Commission's website. EU Regulation 2017/1509, Article 50, Council Regulation 267/2012, Article 40, requires all natural and legal persons to report any information which would facilitate compliance with TFS obligations. No explicit reference is made to reporting attempted transactions by sanctioned entities or individuals, therefore this deficiency remains and has a cascading effect on R.7.

19. **Criterion 15.11** – EU Regulation 2023/1114, Article 107, expressly provides that competent authorities should, where necessary, conclude cooperation arrangements with supervisory authorities of third countries concerning the exchange of information with those supervisory authorities of third countries and the enforcement of obligations under this Regulation in those third countries.

20. Deficiencies in some cascading areas remain for this criterion. Specifically, R.37 where Poland's legal framework does not ensure in all cases where a request does not involve coercive actions, that dual criminality will not be a condition for rendering the assistance. Article 11 section 1(e) of the Directive 2014/41/EU is provided upon in this matter and domestic law Article 589zj section 2 subsection 1 CPC is relied upon when considering rejection of a request.

21. Improvements in coordination of the disposal/management of seized or confiscated property and steps taken towards establishing a single centralised authority to manage such property regarding deficiencies under R.38 are reported in this follow-up report. Draft legislation and strategic coordination initiatives are underway progressing Poland towards addressing these deficiencies.

22. Clarification is provided by Poland pursuant to R.40 regarding National Revenue Administration (KAS) or ISA having powers, or not, to refuse to provide information with regard to non-EU countries. Exchange of tax information with non-EU states the Convention on Mutual Administrative Assistance in Tax Matters, drawn up in Strasbourg on January 25, 1988, as amended by a protocol drawn up on May 27, 2010, agreements on avoidance of double taxation and agreements on exchange of information in tax matters to which Poland are parties, are the mechanisms by which refusal to non-EU countries can be enacted. Poland's clarification does not extend to alternative arrangements for international cooperation with third countries, where those third countries are not signatories to this voluntary convention.

Weighting and Conclusion

23. Poland considers risks in the VASP sector, takes steps to identify and prevent the unauthorised activities of VASPs, competent authorities provide guidance and feedback to VASPs in applying national AML/CFT measures. With the enactment of the EU Regulation 2023/1114 Poland has improved its compliance with c.15.4 and c.15.9. However, Poland does not have in place: (i) specific requirements for obligated institutions to assess and mitigate the ML/TF risks of new technologies, products, services or business practices before releasing them (c.15.1 and c.15.2); and (ii) proportionate and dissuasive sanctions for infringements by VASPs and their senior managers (c.15.8). Also, deficiencies are in place with regards to assigning tasks and powers under MiCA to competent authorities (c.15.4(b); supervision of VASPs (15.6); the applicability of preventive measures under R.10-21 to all types of VASPs and application of remaining deficiencies under R.10-21 to VASPs; the application of TFS by VASPs (15.10) and international cooperation relating to VAs (15.11). **R.15 remains PC.**

Annex B: Summary of Technical Compliance – Deficiencies underlying the ratings

Recommendations	Rating	Factor(s) underlying the rating[9]
8. Non-profit organisations	PC (MER) **LC (FUR 2025)**	• Limited actions are reported as part of reviewing the adequacy of measures in relation to the subset of NPOs that may be abused for TF purposes (c.8.1(c) – FUR3). • No comprehensive policies to promote accountability, integrity, and public confidence in the administration and management of NPOs (c.8.2(a)). • Educational programmes to raise and deepen awareness among the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks are absent (c.8.2(b)). • Limited involvement of the NPO sector in any activity to develop and refine best practices to address TF risks (c.8.2(c)). • Lack of specific and complex mechanisms of co-operation between the competent authorities (8.5(a)).
15 New technologies	PC (MER) PC (FUR 2023) **PC (FUR 2025)**	• There is no specific provision in the AML/CFT Act that requires reporting entities to identify and assess the ML/TF risks that may arise specifically due to the use of new or developing technologies for pre-existing products (c.15.1). • There is no provision requiring obligated institutions to undertake a risk assessment prior to the launch or use of new products, practices and technologies and to take appropriate measures to manage and mitigate the risks (c.15.2). • Poland has not yet adopted legislation assigning tasks and powers under MiCA to competent authorities (c.15.4(b) – FUR3). • Legislation does not cover the overarching requirements for the intensity and frequency of supervision as a whole to be risk-based (c.15.6 (a)). • The frequency of supervision planning does not anticipate emerging risks (c15.6 (a)- FUR2). • Elements c.26.5(a) and (c) are not covered (c15.6 (a) – FUR2). • Deficiencies under c.15.6(a) have cascading effect on c.26.6. • Relevant deficiencies under R.35 are applicable (c.15.8(a) – FUR2). • Preventive measures under R.10-21 are not applicable to VASPs participating in and providing financial services related to an issuer's offer and/or sale of a virtual asset (c.15.9 -FUR3). • Deficiencies under R.10-21 are also applicable (c.15.9 -FUR2).

9. Deficiencies listed are those identified in the MER unless marked as having been identified in a subsequent FUR.

		• No explicit reference is made to reporting attempted transactions by sanctioned entities or individuals (c.15.10 – FUR4). • Deficiencies under R.37- 40 also apply.

GLOSSARY OF ACRONYMS

AML/CFT	Anti-money laundering and combatting terrorism financing
CDD	Customer due diligence
EU	European Union
FATF	Financia Action Task Force
FUR	Follow-up report
GIFI	General Inspector of Financial Information
ISA	Internal Security Agency
MER	Mutual evaluation report
MICA	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets
NPO	Non-profit organisation
NRA	National risk assessment
R.	Recommendation
SNRA	Supra-national risk assessment
TC	Technical compliance
TFS	Targeted financial sanctions
VA	Virtual asset
VASP	Virtual asset service provider
UNSCRs	United Nations Security Council Resolutions

www.coe.int/MONEYVAL

November 2025

Follow-up report

Anti-money laundering and counter-terrorist financing measures -

Poland

3rd Enhanced Follow-up Report &

Technical Compliance Re-Rating

This report analyses Poland's progress in addressing the technical compliance deficiencies identified in the December 2021 assessment of their measures to combat money laundering and terrorist financing and in subsequent follow-up reports.