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(2023)24

Anti-money laundering and counter-terrorist financing measures

Poland

1st Enhanced Follow-up Report & Technical Compliance Re-Rating

December 2023

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 1st Enhanced Follow-up Report and Technical Compliance Re-Rating on Poland was adopted by the MONEYVAL Committee through written procedure (7 December 2023).

Poland: 1st Enhanced Follow-up Report

I. INTRODUCTION

1. The mutual evaluation report (MER) of Poland was adopted in December 2021. Given the results of the MER, Poland was placed in enhanced follow-up.[1] The report analyses the progress of Poland in addressing the technical compliance (TC) deficiencies identified in its MER. 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.

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

- Latvia

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

II. OVERVIEW OF PROGRESS TO IMPROVE TECHNICAL COMPLIANCE

4. This section summarises the progress made by Poland to improve its technical compliance by addressing the technical compliance deficiencies identified in the MER for which the authorities have requested a re-rating (R.15, R.34).

5. For the rest of the Recommendations rated as partially compliant (PC) (R.1, R.5, R.7, R.8, R.13, R.17, R.18, R.19, R.20, R.22, R.26, R.28, R.32, R.33, R.35) the authorities did not request a re-rating. However, Poland has reported some progress in relation to R.26, R.37, R.39 and R.40 that was considered when re-assessing the requested recommendations.

6. This report takes into consideration only relevant laws, regulations or other anti-money laundering and combating the 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 (FUR) is due to be considered by MONEYVAL.[2]

II.1 Progress to address technical compliance deficiencies identified in the MER and applicable subsequent FURs

7. 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 Recommendation 34. The country asked for a re-rating for Recommendation 15, however insufficient progress has been made to justify an upgrade of this Recommendation's rating.

8. Annex A provides the description of 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.

1. Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up involves a more intensive process of follow-up.
2. 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 that written comments are due. In other words, the legislation has been enacted, but it is 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.

III. CONCLUSION

9. Overall, in light of the progress made by Poland since its MER 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, December 2023

R.1	R.2	R.3	R.4	R.5
PC (MER)	LC (MER)	LC (MER)	LC (MER)	PC (MER)
R.6	R.7	R.8	R.9	R.10
LC (MER)	PC (MER)	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 (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 (MER)	LC (MER)	PC (MER)	C (MER)	LC (MER)
R.31	R.32	R.33	R.34	R.35
LC (MER)	PC (MER)	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).

10. Poland will remain in enhanced follow-up and will continue to report back to MONEYVAL on progress achieved in improving the implementation of AML/CFT measures in December 2024.

Annex A: Reassessed Recommendations

Recommendation 15 – New technologies

	Year	Rating and subsequent re-rating
MER	[2021]	[PC]
FUR 1	[2023]	[PC] (upgrade requested, maintained at PC)

1. In the 2013 MER, Poland was rated partially compliant with former R.8. The assessment identified technical deficiencies related to absence of a requirement to have policies and procedures in place to prevent the misuse of technological developments in money laundering/terrorist financing (ML/TF) schemes and absence of a requirement to have policies and procedures to address the specific risks associated with non-face-to-face business relationships when conducting ongoing due diligence.

2. Poland was rated PC for R.15 in its 5th round MER. Since the adoption of the MER, Poland introduced a virtual assets service provider (VASP) registry, fit and proper requirements in relation to natural persons carrying out virtual assets (VA)-related activities or being partners, members of the governing bodies or beneficial owners of a VASP and penalties for VASPs not complying with the registration requirements. Additionally, the threshold upon which VASPs are obliged to apply customer due diligence (CDD) measures in relation to occasional transactions has been lowered to EUR 1,000 or more.

3. **Criterion 15.1** – There is no specific provision in the AML/CFT Act that requires reporting entities to identify and assess the AML/TF risks that may arise specifically due to the development of new products and new business practices and the use of new or developing technologies for both new and pre-existing products. Notwithstanding this fact, Article 33(3)(4) requires obliged entities to identify and assess their ML/TF risks, taking into account several factors, including the types of products, services and means of distribution that the entity provides. Polish authorities refer to Article 43(2)(9), as amended post-MER, and 27(3) of AML/CFT Act as provisions covering the Criterion 15.1. However, these provisions do not require obligated institutions to assess the ML/TF risks of new technologies, products, services or business practices before releasing them. In addition, for pre-existing products risks specifically arising from the use of new or developing technologies are not listed as ones triggering an update of risk assessment.

4. **Criterion 15.2** – Similar to c.15.1, there is no provision:

   (a) requiring obligated institutions to undertake a risk assessment prior to the launch or use of new products, practices and technologies, and
   (b) to take the appropriate measures to manage and mitigate the risks. Polish authorities refer to the mention of new products, services, distribution channels or technological solutions of Article 43 (2)(9), however, this article concerns increased ML/TF risk factors for the application of enhanced due diligence and not to undertake a risk assessment or to take appropriate measures to manage and mitigate the risks.

5. **Criterion 15.3** –

   (a) Poland has considered virtual currencies in the annexes of the 2019 national risk assessment (NRA), where several money laundering and terrorist financing risks scenarios are analysed. The main conclusions are that decentralised cryptocurrencies/virtual assets 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 General Inspector of Financial Information (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. A fully revised draft NRA is under internal review, pending for its adoption and publication.

(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). However, 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 virtual asset are not covered. EU Regulation 2023/1114 ("MiCA"), in force since June 2023, contains a broader definition of "crypto-asset service providers", although it will not be directly applicable to EU Member States until 30 December 2024. Similarly, EU Regulation 2023/1113, on information accompanying transfers of funds and certain crypto-assets, amends Directive (EU) 2015/849 ("4th AMLD") and incorporates the same definition, however, given the 30 December 2024 deadline, no actions have been undertaken to align the Polish national AML/CFT Act provisions with the EU or FATF definition in the interim period. Notwithstanding the above, the 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. As such, deficiencies under c.1.10(d) and c.1.11(c) also apply.

6. **Criterion 15.4** –

(a) 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[3] conducting such activities on the territory of Poland. Deficiencies under c.15.3(b) regarding incomplete scope still apply.

(b) Article 129n of the AML/CFT Act establishes a requirement of no criminal record[4] 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.

7. **Criterion 15.5** – Article 153b of the AML/CFT Act provides an administrative sanction in a form of a fine up to PLN 100,000 (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

3. 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.

4. 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.

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.

8. **Criterion 15.6** –

(a) 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)). In relation to 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.

(b) As stated above, VASPs are registered obligated institutions and 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, but not on the grounds of non-compliance with any of the other obligations of the AML/CFT Act.

9. **Criterion 15.7** – Although 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, no specific feedback or guideline has been provided, in terms of AML/CFT, aimed specifically to the VASPs sector and the particular risks they may face, although some measures to raise awareness in relation to the risks associated with VA and VASPs have been taken, such as providing a summary in Polish of the FATF "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing" report.

10. Notwithstanding the above, a meeting to explain the new AML/CFT requirements introduced by the current version of the AML/CFT Act was held with VASPs, among the rest of obligated institutions, and VASPs participated in the national risk assessment of their sector.

11. **Criterion 15.8** –

(a) 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 also applicable.

(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 also applicable.

12. **Criterion 15.9** – Relevant deficiencies under Recommendations 10 to 21 are also applicable. 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 customer due diligence measures when carrying out an occasional transaction using virtual currency with an equivalent of €1,000 or more.
(b) EU Regulation 2023/1113, in force since June 2023, introduces obligations regarding information that should accompany transfers of "certain crypto-assets", but will not be directly applicable in EU Member States until 30 December 2024. No national level action has been taken to ensure compliance with R.16 in interim either. Therefore, this part of the criterion is not met.

13. **Criterion 15.10** – VASPs, as 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. However, the concerns related to the timeliness in the implementation of the United Nations Security Council Resolutions (UNSCRs) by obligated institutions and other relevant deficiencies expressed in R.7 are also applicable to VASPs.

14. **Criterion 15.11** – According to Article 12(1) of the AML/CFT Act, the GIFI, as both Financial Intelligence Unit and supervisor of VASPs in terms of AML/CFT, must exchange information with other Financial Intelligence Units and with any other foreign competent authority that deals with combating ML/TF.

15. Articles 110-116 regulate the exchange of information between the GIFI and its foreign counterparts/other competent authorities. These articles state that the scope of information that can be exchanged with the aforementioned foreign authorities includes all kinds of information and documents in the GIFI possession, thus including VASP-related information, as obligated institutions under the GIFI's control.

16. As stated in the analysis of Recommendations 37 to 40, judicial authorities are able to provide mutual legal assistance, thus including cases in which VASPs could be involved. Regarding the presence of a sound case management system, authorities advised that: (i) at the beginning of 2022, all units of the Prosecutor's Office were connected to a single IT system PROK-SYS, which contains a case management system and analytical applet accessible to all prosecutors dealing with mutual legal assistances (MLAs); (ii) the timely prioritisation and execution of requests has been encouraged by issuance of the Guidelines of the First Deputy Prosecutor General on 26 April 2023 on conducting investigations in ML cases; and (iii) the registration system employed by the Ministry of Justice signals the urgence and prioritises the received MLA requests.

17. However, relevant minor shortcomings under Recommendations 37 to 40 apply.

Weighting and conclusion

18. Poland does not have in place specific requirements for obligated institutions to assess the ML/TF risks of new technologies, products, services or business practices before releasing them. Regarding the legal framework for VASPs, although they have been included as obligated institutions, their risks have been considered within the NRA and there is an obligation for them to officially register, the requirements of wire transfers of R.16 are not applicable to them, and the scope of the definition of virtual asset-related activities contained in the AML/CFT Act is not fully in line with that of the FATF. **R.15 remains rated as partially compliant.**

Recommendation 34 – Guidance and feedback

	Year	Rating and subsequent re-rating
MER	[2021]	[PC]
FUR1	[2023]	[↑LC] (upgrade requested)

1. Based on the 2013 MER, Poland was rated LC with previous R.25. Assessors noted that: consideration could be given to some case-specific feedback, and sector-specific AML/CFT guidance issued by the financial supervisors is missing.

2. Poland was rated PC for R.34 in its 5th round MER. After the adoption the MER, the GIFI and the Office of the Polish Financial Supervision Authority (UKNF) continued to provide guidance and feedback to obligated institutions in the form of, among others, "communications", newsletters and organisation of trainings, some of them addressing suspicious activity reporting and risk indicators.

3. **Criterion 34.1** – On feedback: Art. 103 (2) AML/CFT Act imposes the obligation for the GIFI to inform the obligated institution or the co-operating unit about the notifications made to the prosecutor no later than 30 days from the time of the notification. The GIFI also provides feedback on the results of control activities. Another feedback avenue is the GIFI's annual activity and the information meetings with representatives of the private sector.

4. On guidelines: Art. 132 (3) of the AML/CFT Act states that GIFI may provide entities referred to in Article 130 (2) with the guidelines related to the control of compliance with the provisions of the Act. Nevertheless, Art. 132 makes reference to GIFI's control activities, and the entities referred to in Art. 130(2) are other supervisors, not reporting entities (REs).

5. The GIFI provides guidance in the form of publications at the GIFI's public and secure website. On its public website[5] the GIFI publishes "communications", which include short instructions pertaining to the way the REs are expected to fill out the threshold reports or information notes (i.e. on naming files containing the information on above threshold transactions; on adaptation of ITC systems of the obligated institutions in terms of reporting, launching of projects of harmonisation etc.), reactions to recurrent issues posed by the private sector, or guidance containing references to certain subjects such as customer verifications, CDD or SAR reporting. Particularly, Communication No 45, "on evaluation of information obtained on customers by obligated institutions and actions in case of inability to apply financial security measures", contains case examples about situations where CDD, including ongoing monitoring, cannot be fully implemented, the impact this has on the risk assessment of the customer and the actions to undertake, including reporting the situation to the GIFI and what the report should contain.

6. The GIFI has also published on its secure website 5 typological newsletters[6] for obligated institutions providing risk indicators in relation to trade-based ML, ML from trafficking in human beings, ML schemes using the so-called 'Laundromat', ML from corruption and a newsletter on protection of non-profit organisations from being used for TF purposes.

7. The GIFI also provides guidance in a form of individual letters to obligated institutions when irregularities have been detected that need prompt improvements in order to be compliant with internal AML/CFT procedures and the AML/CFT Law.

8. Guidance has been issued by other supervisors such as UKNF's "Position of the KNF on risk assessment of obligated institutions", the "Statement on identification and verification of the identity

5. Some of them are available in English at https://www.gov.pl/web/finance/communications.
6. The information on every new edition of the newsletter is published at the GIFI's public website and if an obligated institution does not have an access to the site it can send a request to GIFI.

of institutional clients based on the video-verification method" and "Recommendation H concerning the internal control system at banks" as well as NBP "Guidelines for assessing the risk of money laundering and terrorist financing resulting from the obligation the AML/CFT Act".

9. The GIFI prepared an online on training Anti-money laundering and countering the financing of terrorism to familiarise obligated institutions, co-operating entities and other entities with the subject of anti-money laundering and anti-terrorist financing within the scope of existing regulations. The trainings available on the GIFI website. In addition, during 2022 and 2023, the GIFI has organised trainings on AML/CFT legislation, beneficial ownership, TF risks, application of restrictive measures and other obligated institutions' obligations and suspicious activity reporting. Regarding this last topic, there were 922 participants registered for the training, which focused on the best practices in SARs reporting to the GIFI, as well as on the most common errors made by the obliged entities that happened while reporting SARs. The UKNF has organised 9 AML/CFT webinars addressed to entities under their supervision.

10. All the measures described above (GIFI's communications, newsletters and individual letters, UKNF's statements and recommendations, NBP's guidelines and the trainings from both the GIFI and UKNF) assist both financial institutions (Fis) and DNFBPs in applying the national AML/CFT measures, including the detection and reporting of suspicious transactions, even if a specific and comprehensive guidance document exclusively addressing SAR reporting is not available to all the different FIs and DNFBPs sectors.

Weighting and conclusion

11. The GIFI has a legal obligation to provide feedback to an obligated institution or the co-operating unit about the notifications made to the prosecutor. There is no legal obligation to provide guidance to obligated institutions. Overall, REs are provided with guidance and feedback, mainly from the GIFI and the UKNF. Such measures include communications, newsletters and trainings on different AML/CFT-related topics, which also encompass suspicious activity reporting, even if there is no specific and comprehensive guidance document aimed at the different sectors of FIs and DNFBPs exclusively addressing the detection and reporting of suspicious transactions. **R34 is re-rated largely compliant.**

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

Recommendations	Rating	Factor(s) underlying the rating[7]
15. New technologies	PC (MER) PC (FUR1 2023)	• 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) (as per the 1st FUR, December 2023). • 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 (a)-(b)). • The scope of VASPs covered in Article (2)(1)(12) 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 virtual asset are not covered. (c.15.3) (as per the 1st FUR, December 2023). • The deficiencies under c.1.10(d) and c.1.11(c) are also applicable (c.15.3(c)) (as per the 1st FUR, December 2023). • De-registration measures are only applicable to VASPs who fail to meet the registration requirements or who provided false information upon registration, but not for non-compliance with any of the other obligations of the AML/CFT Act. (c.15.6(b)) (as per the 1st FUR, December 2023). • Relevant deficiencies under Recommendation 26 are also applicable (c.15.6(a)-(b)) (as per the 1st FUR, December 2023). • No specific feedback or guidance has been provided, in terms of AML/CFT, aimed specifically to the VASPs sector and the particular risks they may face. (c.15.7). • Relevant deficiencies under Recommendation 35 are also applicable (c.15.8(a)-(b)) (as per the 1st FUR, December 2023). • Relevant deficiencies under Recommendations 10 to 21 are also applicable (c.15.9) (as per the 1st FUR, December 2023). • Regulation (EU) 2023/1113 is not yet

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

		directly applicable in Poland, and no national level action has been taken to ensure compliance with R.16 in interim either. (c.15.9(b)) (as per the 1st FUR, December 2023). • The concerns related to the timeliness in the implementation of the UNSCRs by obligated institutions expressed in R.7 are also applicable to VASPs. (c.15.10) (as per the 1st FUR, December 2023). • Relevant deficiencies under c.7.2(d), 7.2(e) and c.7.3 are also applicable (c.15.10) (as per the 1st FUR, December 2023). • Some minor shortcomings regarding the timely prioritisation and execution of requests impact the MLA capabilities of judicial authorities. (c.15.11) (as per the 1st FUR, December 2023). • Relevant deficiencies under Recommendations 37 to 40 are also applicable (c.15.11) (as per the 1st FUR, December 2023).
34. Guidance and feedback	PC (MER) LC (FUR1 2023)	• Lack of a specific and comprehensive guidance document exclusively addressing the detection and reporting of suspicious transactions. (c.34.1) (as per the 1st FUR, December 2023).

GLOSSARY OF ACRONYMS

4th AMLD	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
AML/CFT	Anti-money laundering and combating the financing of terrorism
AML/CFT Act	Act of 1 March 2018 on Counteracting Money Laundering and financing of Terrorism
C	Compliant
CDD	Customer due diligence
DNFBPs	Designated non-financial businesses and professions
EU	European Union
FATF	Financial Action Task Force
FIs	Financial institutions
FUR	Follow-up report
GIFI	General Inspector of Financial Information
IT	Information technology
ITC	Information technology and communication
LC	Largely compliant
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
ML/TF	Money laundering/terrorist financing
MLA	Mutual legal assistance
NC	Non-compliant
NBP	Narodowy Bank Polski (National Bank of Poland)
NRA	National risk assessment
PC	Partially compliant
PLN	Polish złoty
REs	Reporting entities
SAR	Suspicious activity report
TC	Technical compliance
UKNF	Urząd Komisji Nadzoru Finansowego (office of the Polish Financial Supervision Authority)
UNSCRs	United Nations Security Council Resolutions
VA	Virtual assets
VASPs	Virtual assets service providers

www.coe.int/MONEYVAL

December 2023

Follow-up report

Anti-money laundering and counter-terrorist financing measures - **Poland**

1st 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.

The report also looks at whether Poland has implemented new measures to meet the requirements of FATF Recommendations that changed since the 2021 assessment.