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(2024)21

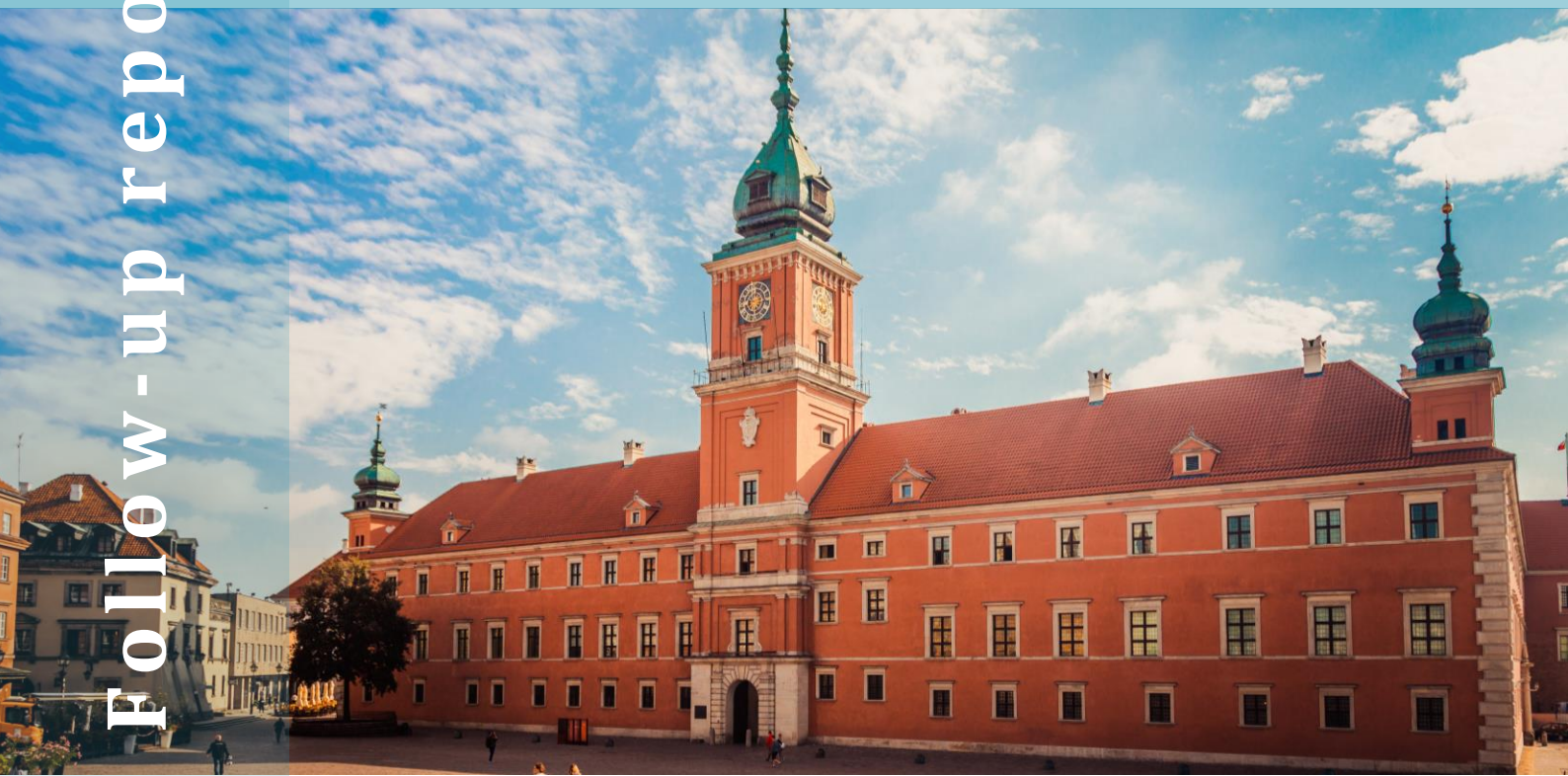
Anti-money laundering and counter-terrorist financing measures

Poland

2nd Enhanced Follow-up Report & Technical Compliance Re-Rating

October 2024

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 2nd Enhanced Follow-up Report and Technical Compliance Re-Rating on Poland was adopted by the MONEYVAL Committee through written procedure 28 October 2024.

Poland: 2nd Enhanced Follow-up Report

I. INTRODUCTION

1. The mutual evaluation report (MER)[1] of Poland was adopted in December 2021. Given the results of the MER, Poland was placed in enhanced follow-up.[2] Its 1st Enhanced Follow-up Report (FUR) was adopted in December 2023.[3] The report analyses the progress of Poland in addressing the technical compliance (TC) deficiencies identified in its MER or subsequent FURs. 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 the request of Poland for four technical compliance re-ratings and the preparation of this report were undertaken by the following Rapporteur teams (together with the MONEYVAL Secretariat):

- Isle of Man
- Israel

3. Section II of this report summarises Poland's progress made in improving technical compliance. Section III sets out the conclusion and 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.1, R.15, R.26, R.33).

5. For the rest of the recommendations rated as partially compliant (PC) (Recommendation (R.)5, R.7, R.8, 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.

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 FUR is due to be considered by MONEYVAL.[4]

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 R.1 R.33. The country asked for a number of re-ratings for other R.15 and R.26 which are also analysed but no re-rating has been provided.

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. MER of Poland, available at https://rm.coe.int/moneyval-2021-25-mer-pl-en/1680a55b9a.
2. Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up involves a more intensive process of follow-up.
3. 1st Enhanced FUR, available at https://rm.coe.int/moneyval-2023-24-pl-5thround-1stenhfur/1680ae8296.
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 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 and 1st enhanced FUR were 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, October 2024

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)	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 (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).

10. Poland will remain in enhanced follow-up and will continue to report back to MONEYVAL on progress to strengthen its implementation of AML/CFT measures. Poland is expected to report back within one year's time.[5]

5. Rule 23, paragraph 1 of the Rules of Procedure for the 5th round of mutual evaluations.

Annex A: Reassessed Recommendations

Recommendation 1 – Assessing risks and applying a risk-based approach

	Year	Rating
MER	2021	PC
FUR1	2023	PC (no upgrade requested)
FUR2	2024	↑ LC (upgrade requested)

1. The requirements on assessment of risk and application of the risk-based approach were added to the FATF recommendations with the last revision and so were not assessed in the previous mutual evaluation of Poland.

2. Poland was rated PC for R.1 in its 5th round MER. Since the adoption of the MER, Poland developed and published a new national risk assessment (NRA) in 2023, enhanced the risk-based allocation of resources in relation to multiple competent authorities (such as the General Inspector of Financial Information (GIFI), Office of the Polish Financial Supervision Authority (UKNF) or the Military Police) and clarified in the AML/CFT Law the need to apply enhanced customer due diligence (CDD) in cases of higher risk of money laundering (ML) or terrorist financing (TF).

3. **Criterion 1.1** – Poland performed its first NRA in 2017-2019. The results of the NRA were published on 17 July 2019. The works were based on earlier activities undertaken already in 2012 under the project on preliminary NRA in co-operation with the International Monetary Fund. The methodology utilised in the NRA was developed by the Polish authorities.

4. The NRA provides the assessment of ML/TF "basic risks", grounded on the evaluation of threats; the assessment of "residual risk" related to the list of *modi operandi* (separately for ML and TF); and the assessment of general ML and TF risks as a result of the two assessments described above.

5. In December 2023, Poland developed and published a new NRA, which equally identifies potential ML/TF risks by looking at, inter alia, the level of estimated illicit assets, the threat of profit-generating crimes, cross-border aspects of ML and TF or other legal, environmental, operational and strategic risks and vulnerabilities, as well as sectorial risk assessment (enclosed as Annex II of the NRA) providing different levels of threat and vulnerability for each sector, separately for ML and TF, along with justification. The report was made available to competent authorities, the private sector, and the general public through the Public Information Bulletin website.

6. Apart from the NRAs, a risk assessment for entrepreneurs conducting currency exchange activity was developed by the National Bank of Poland (NBP) and contains more detailed information on the specific risks. This assessment is updated in November each year.

7. **Criterion 1.2** – The designated authority and the mechanism to co-ordinate actions to assess risk is provided by AML/CFT Act. According to Article 25(1) of the AML/CFT Act, the GIFI shall prepare the NRA in co-operation with the Financial Security Committee government, local government authorities and other state organisational units, the NBP, the UKNF, the Supreme Audit Office[6] and the obligated institutions.

8. **Criterion 1.3** – According to Article 25 (3) of the AML/CFT Act, the GIFI shall verify the validity of the national risk assessment and update it as applicable, in any case at least on a biannual basis.

9. **Criterion 1.4** – According to Article 30(1)(2) of the AML/CFT Act, after being approved by the Financial Security Committee, the NRA is submitted to the Minister of Finance for approval. After the approval, the GIFI shall publish the NRA in the Public Information Bulletin on the website of the

6. The "co-operating units".

Ministry of Finance (excluding the part containing classified information). As stated, the results of the NRAs were published in the Public Information Bulletin in July 2019 and December 2023, respectively.

10. The results of the NRAs were communicated to the public and the private sectors in a series of seminars organised by the GIFI. For example, in January 2020, the GIFI organised a conference on the NRA attended by around 100 participants from the public and private sectors. Moreover, in 2023 and 2024, the GIFI organised numerous trainings with around 11 000 participants in the AML/CFT area for obligated institutions and authorities, including ones focused on the 2023 NRA.

11. **Criterion 1.5** – According to Article 31(1) of the AML/CFT Act, based on the NRA, the GIFI shall draft the Strategy on counteracting ML and TF, including the action plan aiming to mitigate the ML/TF risk. The Strategy has been adopted by way of the resolution of the Council of Ministers on 19 April 2021 and includes measures that compound the re-allocation of resources according to the risk (e.g. measures related to the Financial Intelligence Unit's human and technical resources dedicated to operational analysis).

12. Police revised the structure of the asset recovery units within the country by replacing previously operating Asset Recovery Office in Metropolitan Police Headquarters and the Voivodeship Police Headquarters in Poznań with full-time asset recovery units in the form of sections and teams in the structures of Economic Crime Department at the level of Voivodeship Police Headquarters.

13. To implement the 2021 Strategy, the authorities and institutions responsible for preventing, detecting, and prosecuting crimes have analysed, most notably between 2022-2023, whether they have adequate financial, human, and technical resources to perform their AML/CFT tasks, which has led to several improvements in IT and human resources in the Military Police (dedicated exclusively to detection and prevention of ML and TF crimes), the UKNF or the GIFI. In the particular case of the GIFI, it has taken a risk-based approach following this analysis and a strategic plan, which has resulted in adequate resources being allocated. These resources have resulted in increases in FTEs and budget, the implementation of new IT systems, and organisational changes (new teams focusing on specific areas such as risk assessment and strategic analysis, instruction of administrative sanctioning proceedings, or co-operation with obligated institutions.

14. **Criterion 1.6** – Applicable legislation does not provide for disapplication of any FATF recommendations requiring financial institutions (FIs) or designated non-financial businesses and professions to take certain actions.

15. **Criterion 1.7** – According to Article 43(1) of the AML/CFT Act, the obligated institutions shall apply enhanced CDD measures in cases when a higher risk of ML or TF is present. Specific examples of possible higher risk ML/TF scenarios are set out under Article 43(2). Nevertheless, obligated institutions are not required to take into account the higher risks identified in the NRA or to incorporate information on those risks into their risk assessments. In this regard, the provision in Article 27(2) of the AML/CFT Act establishing that the obligated institutions "can consider" the outcomes of the NRA or the EU supranational risk assessment when identifying and assessing their ML/TF risk exposure does not amount to a requirement meeting this criterion through any of the two options set out therein.

16. **Criterion 1.8** – According to Article 42(1) of the AML/CFT Act, the obligated institutions may apply simplified CDD measures in cases where the risk assessment conducted by them (referred to in Article 33(2)) has confirmed a lower risk of ML and TF. However, there is no requirement that the risk assessment conducted by the obligated institutions should be consistent with the country's assessment of its ML/TF risks. In this regard, the provision in Article 27(2) of the AML/CFT Act establishing that the obligated institutions "can consider" the outcomes of the NRA or the EU supranational risk assessment when identifying and assessing their ML/TF risk exposure, along with

the cases set out in Article 42(2) of the AML/CFT Law, does not amount to a requirement meeting this criterion.

17. Article 42(2) sets out the circumstances (as an exemplary list of criteria) that may substantiate a lower money laundering and terrorist financing risk. While Annex II of the 2023 NRA takes into account some of these circumstances (for example, publicly listed companies with appropriate beneficial ownership disclosure requirements, customers rated as low risk, or jurisdictions with AML/CFT requirements equivalent to those of the EU) for the risk estimates of different sectors, it is not clear that all of the circumstances referred to in the AML/CFT Act as possible low-risk criteria are consistent with the country's assessment of ML/TF risks.

18. **Criterion 1.9** – The AML/CFT Act requires the obligated institutions to identify and assess ML/TF risks, as described under the analysis for criteria 1.10 and 1.11. According to Article 130 of the AML/CFT Act, the GIFI shall exercise the control of the obligated institutions' compliance with the obligations in the scope of AML/CFT; the control shall also be exercised by the relevant sectoral supervisors. Nevertheless, relevant deficiencies described under R.26 and R.28 (particularly 26.5 and 28.5) impact this partial rating, while taking into account the improvements in relation to a more comprehensive risk-based approach by the UKNF and an updated risk assessment methodology for the currency exchange sector by the NBP, as acknowledged in R.26.

19. **Criterion 1.10** – According to Article 27(1) of the AML/CFT Act, the obligated institutions shall identify and assess risks associated with ML and TF referring to their activity, taking into account risk factors related to customers, states or geographical areas, products, services, transactions or their supply channels. Such measures shall be proportionate to the nature and size of the obligated institution.

(a) Document their risk assessments – The provision under Article 27(3) requires obligated institutions to prepare their ML/TF risk assessments in a hard copy or by electronic means.

(b) Consider all relevant risk factors – According to Article 27 of the AML/CFT Act, obligated institutions shall identify and assess risks associated with money laundering and financing of terrorism referring to their activity, taking into account risk factors related to customers, states or geographical areas, products, services, transactions or their supply channels.

(c) Keep assessments up to date – The provision under Article 27(3) requires the obligated institutions to update their ML/TF risk assessments as necessary, and at least on a biannual basis.

(d) Have appropriate mechanisms to provide risk assessment information to competent authorities and self-regulatory bodies. Although, according to Article 27(4) the obligated institutions may make their ML/TF risk assessments available to professional self-regulatory bodies or associations of such obligated institutions, this is a discretional rather than obligatory requirement.

20. **Criterion 1.11** –

(a) Have policies, controls and procedures – Article 50(1) of the AML/CFT Act requires the obligated institutions to introduce internal procedures on counteracting ML/TF. This internal procedure shall be approved by the senior management (Article 50(3)). The internal procedures should define activities or measures undertaken in order to mitigate the risk of ML/TF, as well as adequate management of identified risks (Article 50 (2)).

(b) Monitor implementation of controls – The internal procedures should include rules of internal control or oversight of compliance with the AML/CFT requirements (Article 50 (2)).

(c) Take enhanced measures – Pursuant to Article 43(1) of the AML/CTF Act, obligated institutions shall apply enhanced CDD in cases of higher risk of money laundering or terrorist financing, as well as in the cases referred to in Articles 44 to 46 (high-risk third countries, cross-border correspondent relationships and politically exposed persons, respectively).

21. **Criterion 1.12** – The obligated institutions may apply simplified CDD measures only in cases where the risk assessment has confirmed a lower risk of money laundering and financing of terrorism, although it is not clear that all the circumstances referred to in the AML/CFT Act as possible low risk criteria are consistent with the country's assessment of ML/TF risks (see c.1.8). The obligated institutions cannot apply simplified CDD where there is suspicion of ML/TF (Article 42 (3) and Article 35(1)(5) and (6)).

Weighting and Conclusion

22. The majority of the criteria are met, with shortcomings remaining only in the following criteria: obligated institutions are not required to take into account the higher risks identified in the NRA or to incorporate information on those risks into their risk assessments (although authorities do require FIs and designated non-financial businesses and professions to implement EDD when higher risks are identified) (c.1.7); there is no requirement that the risk assessment conducted by the obligated institutions should be in line with the country's assessment of its ML/TF risks (c.1.8), it is unclear that all the possible low risk examples of Article 42(2) of the AML/CFT Act are consistent with the country's assessment of ML/TF risks (c.1.8, c.1.12); some relevant deficiencies under c.26.5 and c.28.5 have an impact (c.1.9) and the requirement for the obligated institutions to make their ML/TF risk assessments available to professional self-regulatory bodies or associations of such obligated institutions is a discretional rather than obligatory (c.1.10). **R.1 is re-rated LC.**

Recommendation 15 – New technologies

	Year	Rating
MER	2021	PC
FUR1	2023	PC (upgrade requested)
FUR 2	2024	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 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 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 CDD measures in relation to occasional transactions has been lowered to 1 000 euros (EUR) 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 ML/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 27(1) requires obligated institutions 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. In practice, both the UKNF and the GIFI encourage obligated institutions to include emerging risk factors in their risk assessments, including those arising from new technologies, through their supervisory and outreach (guidance, periodic reporting, trainings, newsletters, and communications) actions.

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

   (a) requiring obligated institutions to undertake a risk assessment prior to the launch or use of new products, practices and technologies (notwithstanding the efforts done in practice by the supervisory authorities, as referred in c.15.1); and

   (b) to take the appropriate measures to manage and mitigate the risks.

5. **Criterion 15.3** –

   (a) 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/virtual assets (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 OCGs) 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.

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[7] conducting such activities on the territory of Poland. 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 VA are not covered. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets("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. 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 ("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.

(b) 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.

7. **Criterion 15.5** – 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

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.

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)), however this provision does not cover the overarching requirements for the level and frequency of supervision as a whole 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. This notwithstanding, the GIFI does not yet have a written policy or procedure in relation to the frequency of review of an obliged institution's risk rating.

(b) 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.

9. **Criterion 15.7** – 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 upcoming application of MiCA and the "travel rule" and some relevant VA typologies and risk indicators.

10. 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.

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 R.10 to R.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 CDD measures when carrying out an occasional transaction using virtual currency with an equivalent of EUR1 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 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 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 R.37 to R.40, judicial authorities are able to provide mutual legal assistance (MLA), 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 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 (MoJ) signals the urgence and prioritises the received MLA requests.

17. However, relevant minor shortcomings under R. 37 to R.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 yet 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 PC.**

Recommendation 26 – Regulation and supervision of financial institutions

	Year	Rating
MER	2021	PC
FUR1	2023	PC (no upgrade requested)
FUR 2	2024	PC (upgrade requested, maintained at PC)

1. In the 4th round MER of 2013, Poland was rated LC for R.23 and R.29. The technical deficiency identified was that there was no registration or licensing system for co-operative savings and credit unions.

2. Poland was rated PC for R.26 in its 5th round MER. Since the adoption of the MER, Poland introduced new registration requirements for non-bank lenders, ad-hoc ex-post suitability assessments for members of the management and supervisory board of banks and enhanced the risk scoring methodologies of the UKNF and the NBP.

3. **Criterion 26.1** – Under Article 130(1) of the AML/CFT Act, the GIFI exercises control over all obligated institutions for the purposes of compliance with AML/CFT obligations. In addition, under Article 130(2), control may also be exercised by the President of the NBP over currency exchange office operators; by the UKNF over entities supervised by it for prudential purposes (including banks, payment institutions, investment firms, brokerage, collective investment funds, insurers, and insurance intermediaries); by the National Association of Cooperative Savings and Credit Unions (NACSCU) and the UKNF over credit unions and by the National Revenue Authority in relation to obligated institutions controlled by these bodies. Value transfer providers are not covered by the framework as stand-alone obliged institutions, however the UKNF advised that there are no entities providing such services that are not already subject to other market regulations (foreign exchange law, payment services regulations, banking law, law on trading in financial instruments, law on stock exchange, trading including commodity exchanges, postal law, AML/CFT Act, etc.) and that it undertakes checks to detect the provision of value transfer services (see R.14). The discharge of these overlapping supervisory responsibilities is co-ordinated by the GIFI under Article 132 of the AML/CFT Act.

4. **Criterion 26.2** – All institutions carrying out financial services in Poland have to be licensed by the UKNF with the exception of currency exchange offices which are registered by the NBP, and credit unions which are licensed by the UKNF. This is required under the Act of 29 August 1997 on Banking, the Act of 27 July 2002 on Foreign Exchange Law, the Act of 5 November 2009 on Cooperative Savings and Credit Unions, the Act of 29 July 2005 on Trading in Financial Instruments, the Act of 19 August 2011 on Payment Service Providers, and the Act of 11 September 2015 on Insurance and Reinsurance Activities. The provisions of the Banking Act prevent shell banks from being established.

5. Non-bank lenders have been required to register with the UKNF since 2017. While the process was originally automatic, since January 2024, non-bank lending institutions must meet the requirements of Article 59a of the Consumer Credit Act (including capital requirements and having a supervisory board) in order to be registered, and the UKNF will refuse registration or immediately delete from the registry and the register of entrepreneurs of the National Court Register (NCR) if requirements are not met or cease to be met.

6. Other types of FIs (such as factoring businesses) are still required to register with the NCR only (which has no AML/CFT regulatory function) and only when undertaking business in a corporate form (which includes the types of partnership which can be incorporated in Poland). Value service provision is not covered by the framework as a standalone activity, as explained in c.26.1 and R.14.

7. **Criterion 26.3** – Under Article 22aa of the Banking Law, a bank's management board and supervisory board is subject to a reputation, honesty and integrity test. This test would cover association with criminals at least to some extent. Under Article 22b, the appointment of the president and members of a bank's management board requires the consent of the UKNF. Applications for consent must be accompanied by background information about the person in question, including criminal record information. The appointment only takes effect when consent has been granted.

8. The UKNF can refuse to give consent under Article 22b.3, where the criteria are not met. Under Articles 22.3 and 22a.2, other members of the management board and members of the supervisory board, together with the results of a fit and proper assessment by the bank, must be notified to the UKNF without delay after appointment. They can be removed by the UKNF. Additionally, banks' management board and supervisory board (on an ad-hoc basis, so far only covering significant banks) members are subject to ex-post secondary suitability assessment by the UKNF after their appointment, which includes background information collection from other UKNF departments and law enforcement agencies (criminal record information) and open-source intelligence analysis. The suitability assessment is supported by the 2023 "Methodology of fit and proper assessment of board members of supervised entities".

9. With regard to other members of senior management, according to Article 22aa(10) of the Banking Act, the bank is required to identify key function holders and ensure they meet the reputation, honesty and integrity test. The UKNF's consent is not required for appointment to these key function holder positions, and there are no specific provisions in relation to other members of senior management.

10. Under Article 25, changes to shareholders and beneficial owners must be notified to the UKNF before they take up their rights; they are subject to a legal suitability test. Changes of shareholder and beneficial owner can only take effect if the UKNF gives consent, and Article 25 provides the UKNF with power to require shareholders and beneficial owners to transfer their rights.

11. There are similar provisions in the Act on Payment Services, the Act on Trading in Financial Instruments, the Act on Investment Funds and Management of Alternative Investment Funds s, and the Act on Insurance, albeit containing some stronger provisions in relation to key functionaries. Overall, though, the provisions do not comprehensively cover the entirety of senior management in the way envisaged by the criterion. See c.26.2 for other types of FIs (such as factoring businesses and non-bank lenders).

12. Under Articles 12 and 13 of the Act of 27 July 2002, Foreign Exchange Law, currency exchange may only be performed by individuals with a clean criminal record certificate in respect of fiscal offences or offences committed to obtain a financial or personal benefit. In addition, shareholders (and equivalent persons) must also hold such a certificate. While there are no legal provisions specifying that the NBP's consent is required in relation to roles and appointments covered by Articles 12 and 13. Pursuant to Article 17ca to the Act Foreign Exchange Law, the President of the NBP has authority over and may prohibit exchange bureau activity by an entrepreneur, when such entrepreneur has made a false statement with regards to having a clean criminal record. As of 31 October 2021, requirements of having clean criminal record, apply to beneficial owners. There is, however, no legal requirement where a person is an associate of a criminal. Articles 17ca and 17cb to the Act Foreign Exchange Law provide that failure to fulfil the obligations in Articles 12 and 13 shall be subject to the issue a decision by the President of NBP on prohibiting the person in question from conducting bureau de change activity for three years.

13. Articles 7 and 18 of the Act on Cooperative Savings and Credit Unions provide that a credit union cannot be established unless members of the management board and supervisory board have not been

sentenced to an intentional offence against property or documents or a fiscal offence. These provisions are complemented by Article 21, which specifies that the president of the management board can only be appointed upon receipt of supervisory authorisation, which will be refused where the individual was validly sentenced for an intentional or fiscal offence (which was not privately prosecuted) or where Article 18 has not been met by the president. According to Article 71(7), a member of the management board, including its president, shall be removed from office by the UKNF in the event of a final conviction for an intentional crime or a fiscal crime, as well as in the event of failure to report charges against him or her. Regarding members of the supervisory board, these can only be persons not having been validly convicted of an intentional crime against property, documents, or a fiscal crime, or not having been prohibited from conducting business, according to Article 18(1). However, there is no legal power for the UKNF to dismiss members of the supervisory board. There are no requirements in relation to beneficial owners, legal owners or management below the level of the management board or in relation to associates of criminals.

14. There is also a power under Article 129(2) of the AML/CFT Act for supervisors to require individuals to provide a certificate that they have not been convicted for an intentional crime or an international fiscal offence.

15. **Criterion 26.4** –

(a) See c.26.1 and 26.2 for the overall authorisation framework, R.27 for powers of monitoring/supervision by FI supervisors and R.40 for the powers of supervisors to exchange information, which only have minor shortcomings. Poland was reviewed under the Financial Sector Assessment Program in 2018. The review concluded that "banking regulation and supervision" were "largely in line with Basel Core Principles", although there were needs, at the time, to enhance the approach in some areas (such as, in relation to the UKNF regulatory powers, governance and operational capacity; the licensing regime for banks; resource and staffing for onsite and offsite activities; or the enforcement regime). Authorities advised that there have not been any additional internal or external assessments under the International Association of Insurance Supervisors Peer Review Process (in particular on the implementation of Insurance Core Principle 22), nor based on the Basel Core Principles (in particular, Principle 29) or by the International Organization of Securities Commissions. This notwithstanding, the Financial Sector Assessment Program review of 2018 concluded that, in relation to insurance, regulation and supervision had been enhanced, including comprehensive group supervision, and that, in the case of capital markets, their oversight was "broadly aligned with the International Organization of Securities Commissions principles" (although, in both cases, issues relating to resources remained). Regarding group supervision, Article 145(3) of the AML/CFT Act states that supervisors are authorised to control the implementation of group-wide procedures in subsidiaries and entities being credit institutions and FIs that are part of a group for which an obligated institution is the parent undertaking. Therefore, group supervision is subject to the same considerations as described above.

(b) As explained under c.26.1 and c.26.2 and R.14, value transfer services are not explicitly covered as standalone activities, although the Polish authorities have advised that no value transfer, as a standalone business, exists in practice. The NBP has established systems for monitoring and ensuring compliance by currency exchange offices, having regard to the risks. The UKNF and GIFI have established systems for monitoring compliance by payment institutions, having regard to risks. The UKNF has a risk rating methodology and the most comprehensive approach to supervision, with payment institutions featuring as a significant part of its supervisory engagement in 2018. The onsite supervisory programme for such

institutions has been reduced since then. The UKNF's supervisory programme had, at the time of the MER, good risk-based elements; and since then, several improvements have been introduced to it to enhance the comprehensiveness of the risk-based approach (see c.26.5). GIFI bases its assessment of risks of FIs on the UKNF methodology however its approach to supervisory engagement of payment institutions is less comprehensive than that of the UKNF.

16. **Criterion 26.5** – Under Article 131 of the AML/CFT Act, 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 co-ordinating 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. These legal provisions deal with the generality of ML/TF risks and, through the reference to the NRA, can be considered to cover sub-criterion (b), but they do not cover the overarching requirements for the level and frequency of supervision as a whole (onsite and offsite) to be risk-based, and there is no explicit reference to the elements at sub-criteria (a) and (c).

17. Under Article 132, the GIFI, which has a lead role, provides guidelines to other supervisors on the approach to supervision they should adopt. In this regard, GIFI has issued annual guidance to each supervisor specifying the frequency of onsite inspections for each level of risk (e.g. high risk being inspected at least every two years). This would seem in part to meet the element of the recommendation dealing with frequency of supervision.

18. Onsite inspection plans are prepared annually by each supervisor, who decides on the frequency and intensity of supervision of controlled institutions based on varying sources of information in their possession.

19. Looking at each supervisor in turn:

- The UKNF has a risk tool (ORION), which main objective is to assess obliged institutions for their exposure to ML/TF risks. The risk matrix has been progressively enhanced (ORION 2.0) over time in order to better assess FIs' risks by taking into account an increasing number of information sources, such as the bank's supervisory review and evaluation process questionnaires and scores, quarterly FI's AML/CFT reporting, the IT system of the Clearing House, the UKNF database of negative information or the Inspection Support System (results of UKNF inspections). The risk score is used to ensure an effective allocation of resources for the UKNF supervision and to take appropriate supervisory measures to prevent the materialisation of, or to mitigate, ML/TF risks. To support and develop the ORION 2 risk matrix, the methodology for assigning risk ratings to obliged institutions that are subject to the UKNF's AML/CFT supervision was created, which takes place on a continuous basis and establishes the requirement to update the individual risk assessments of FIs on an ongoing basis should any of the individual risk factors change. This methodology is meant to support the inspection process and timeline of onsite and offsite inspections. The methodology does not detail the intensity of supervision, although, in practice, risk factors form part of the supervisory engagement.
- GIFI does not have a methodology of its own for assessing the ML/TF risk of each FI. Instead, the GIFI co-ordinates with other supervisors (most notably, the UKNF) when establishing its annual supervision plan. It takes into account, in order to select the entities for its own inspections, the other supervisors' plans, the results of their inspections, quarterly data

reported by REs, data from Clearing House Information and Communication System,[9] and other sources of data, including the results of the ML/TF risk assessment of the entities in the ORION scoring provided by the UKNF (prioritising those scoring "high"). The GIFI contributes to this risk assessment by preparing questions for the quarterly reporting. The annual planning does not detail the intensity of supervision, although, in practice, risk factors form part of the supervisory engagement.

- The NBP assesses the risk of each currency exchange office. It issued a methodology which it used to assess the risk of each office in 2018. It has subsequently updated this methodology in 2022 in order to better assess ML/TF risks separately by taking into account new risk factors. The methodology establishes that the risk assessment of individual entrepreneurs conducting currency exchange activities is reviewed on an ongoing basis (e.g., after an inspection or upon changes in the scope or location of the entrepreneur activities or other significant information) and, at least, annually in October. The risk factors are taken into account in the yearly inspection plans in order to determine the intensity of inspections. In addition, it has issued onsite methodologies and a document on criteria for planning inspections. The document indicates that control is subject to the level of risk. The methodology does not detail the intensity of supervision, although, in practice, risk factors form part of the supervisory engagement.
- The NACSCU undertakes risk assessment of each credit union, and the assessment team (AT) has been advised that the key factor is the risk of services provided and that this has an impact on onsite inspection frequency. The approach would seem to meet the aspects of the criterion not met by the AML/CFT Act to a very limited extent. The AT has not been provided with further information.
- Further information can be found in IO.3, where it is stated that there is scope for the UKNF, GIFI and NBP to develop more comprehensive approaches to risk-based supervision.

20. **Criterion 26.6** – The UKNF and the NBP review the assessment of the risk rating of the supervised entity (and the group) at the time of an onsite inspection. The UKNF reviews the risk scoring for each entity on an ongoing basis (as a result of trigger events, meaning every time there are any changes in any risk factor considered in the ORION risk matrix, including the FIs quarterly reporting). When planning its annual supervision, the GIFI takes into account and contributes to the FIs risk scoring of the UKNF. The NBP reviews its risk ratings on an ongoing basis and, at least, annually (every month of October). There are written policies and procedures in relation to the frequency of review assessment of a FI's risk rating for the UKNF and the NBP, as explained in c.26.5. The AT has not been provided with information about the NACSCU.

Weighting and Conclusion

21. There are a few minor gaps in the scope of coverage of FIs of the requirements in c.26.1 and c.26.2. There are some moderate gaps in relation to market entry requirements for preventing criminals and their associates from beneficially owning or otherwise controlling FIs (c.26.3). There are moderate gaps: (i) at a legislative level with regard to meeting the precise language of the FATF on the components of risk-based supervision, and (ii) the intensity of supervision itself not being detailed in the risk-assessment methodologies or annual plans of the UKNF, GIFI, and NBP (c.26.5). There is little information about the NACSCU (c.26.5 and c.26.6). **R.26 remains rated as PC.**

9. The Clearing House Information and Communication System is a tool used by the National Revenue Authority to process the data submitted by banks and other FIs in order to analyse the risk of using the financial sector for fiscal fraud.

Recommendation 33 – Statistics

	Year	Rating
MER	2021	PC
FUR1	2023	PC (no upgrade requested)
FUR 2	2024	↑ C (upgrade requested)

1. Based on the 2013 MER, Poland was rated LC with previous R.32. Assessors noted that: no statistics were kept on confiscation of proceeds of crime which are not ML or TF-related; detailed statistics kept by law enforcement agencies were absent; review of effectiveness of the AML/CFT systems on a regular basis was insufficient; detailed statistics on information exchanged between domestic law enforcement bodies and their foreign counterparts lacked.

2. Poland was rated PC for R.33 in its 5th round MER. Since the adoption of the MER, Poland has upgraded the GIFI suspicious activity report (SAR) registration system to require determining whether a SAR relates to ML or TF, has introduced a uniformed IT system for the Public Prosecutor's Office (PPO) that contains data on the seizure of property and MLAs, and has introduced new sections in the statistical reporting of the MoJ to record MLAs and extradition requests.

3. **Criterion 33.1** –

(a) Article 14 (2) of the AML/CFT Act, the GIFI shall collect statistical data on SARs received, measures taken by the GIFI pursuant to submitted information, disseminations to the prosecutor's office and other public administration bodies and units, as well as statistical data regarding the information as a result of which the prosecutor and another public administration body or unit have undertaken further activities. GIFI keeps statistics on SARs received and disseminated which are broken down by ML or FT suspicion.

(b) Department for Organised Crime and Corruption of the PPO, based on Article 20 (3-5) of the Regulation of the Minister of Justice of 7 April 2016, is responsible for collection of detailed information on investigations, prosecutions and convictions for ML/TF. The authorities keep statistics on ML/TF investigations, prosecutions and convictions: number of cases and number of legal persons and natural persons involved. The convictions are further broken down on first instance and final.

(c) As per Article 14 (2) of the AML/CFT Act, the GIFI collects information on assets in respect of which either freezing, suspension of transactions and blockage has been performed, or seizure, property securing, or forfeiture has been adjudicated. According to Article 20 (3-5) of the Regulation of the Minister of Justice of 7 April 2016, information on seizure of property and forfeiture in cases concerning ML/TF is collected by the Department for Organised Crime and Corruption of the PPO. Since 2022, all statistics are kept on a uniformed IT system known as PROK-SYS. This implements a case management system which contains data on the seizure of property and enables the data to be interrogated in a number of different ways (broken down by years and criminal offences). Data on confiscated property is collected by the respective department of the MoJ.

(d) The Bureau of International Co-operation of the PPO and the MoJ are responsible for collecting the data on MLA or other international requests for co-operation made and received in relation to non-EU countries. In the case of the MoJ, in 2024 the appellate, district and regional courts introduced new sections in their statistical reporting, to record MLAs and extradition requests sent to or received from foreign partners in relation to ML, TF, or predicate offences-related proceedings. Regarding the PPO, the statistics on the execution of out-going and in-coming requests of the MLA requests and European Investigation Orders, including pending, executed,

and refused requests (and the time for completing each request), can be obtained through PROK-SYS software and more specifically the OZ REGISTER applet. The collected data can be broken down by jurisdiction. The GIFI collects statistics on international co-operation requests made and received, inclusively requests, responses, spontaneous disseminations and cross-border reports. As part of co-operation with Europol, police information is exchanged via the secure information exchange network application channel on international organised crime in categories covered by Europol's mandate, including ML.

Weighting and Conclusion

4. **R. 33 is re-rated as C.**

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

Recommendations	Rating	Factor(s) underlying the rating[10]
1. Assessing risks and applying a risk-based approach	PC (MER 2021) **LC (FUR2 2024)**	• Obligated institutions are not required to take into account the higher risks identified in the NRA or to incorporate information on those risks into their risk assessments (c.1.7). • There is no requirement that the risk assessment conducted by the obligated institutions should be consistent with the country's assessment of its ML/TF risks (c.1.8). • It is not clear that all the circumstances referred to in Article 42(2) of the AML/CFT Act as an exemplary list of possible low risk criteria are consistent with the country's assessment of ML/TF risks (c.1.8), (c.1.12) *(as per FUR December 2024).* • Relevant deficiencies described under R.26 and R.28 (particularly 26.5 and 28.5) impact this partial rating (c.1.9) *(as per FUR December 2024).* • Although, according to Article 27(4) the obligated institutions may make their ML/TF risk assessments available to professional self-regulatory bodies or associations of such obligated institutions, this is a discretional rather than obligatory requirement (c.1.10(d)).
15. New technologies	PC (MER 2021) PC (FUR1 2023) **PC (FUR2 2024)**	• 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 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.15.4) *(as per FUR December 2023)*. • Some relevant deficiencies under R.26 are also applicable (c.15.6(a)) *(as per FUR December 2024)*. • Relevant deficiencies under R.35 are also applicable (c.15.8(a)-(b)) *(as per FUR December 2023)*. • Relevant deficiencies under R.10 to R.21 are also applicable (c.15.9) *(as per FUR December 2023)*. • Regulation (EU) 2023/1113 is not yet directly

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

Recommendations	Rating	Factor(s) underlying the rating[10]
		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 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 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 FUR December 2023)*. • Some minor deficiencies under R.37 to R.40 are also applicable (c.15.11) *(as per FUR December 2024)*.
26. Regulation and supervision of financial institutions	PC (MER 2021) **PC (FUR2 2024)**	• Value transfer providers are not explicitly covered by the framework as stand-alone obliged entities (c.26.1, c.26.2, c.26.4(b)) *(as per FUR December 2024).* • Other types of FIs (such as factoring businesses) are only required to register with the NCR when undertaking business in a corporate form (which includes the types of partnership which can be incorporated in Poland) (c.26.2, c.26.3) *(as per FUR December 2024).* • The reputation, honesty and integrity test of Article 22aa of the Banking Law would cover association with criminals only to some extent (c.26.3). • The UKNF's consent is not required for appointment to key function holder positions, and there are no specific provisions in relation to other members of senior management of banks (c.26.3). • Provisions in the Act on Payment Services, the Act on Trading in Financial Instruments, the Act on Investment Funds and Management of Alternative Investment Funds, and the Act on Insurance, do not comprehensively cover the entirety of senior management in the way envisaged by this criterion (c.26.3). • Other types of FIs are only required to register with the NCR when undertaking business in a corporate form (c.26.2, c.26.3) *(as per FUR December 2024).* • For currency exchange offices, there is no legal requirement in relation to associates of criminals (c.26.3) *(as per FUR December 2024).* • For co-operative savings and credit unions, there are no powers to dismiss a member of the supervisory board, and there are no authorisation requirements for beneficial owners, legal owners, management below the level of the management board, or in relation to associates of criminals (c.26.3) *(as per FUR December 2024).* • GIFI approach to supervisory engagement of payment institutions is less comprehensive than that of the UKNF (c.26.4(b)) *(as per FUR*

Recommendations	Rating	Factor(s) underlying the rating[10]
		December 2024). • The legal provisions (Articles 131 and 132 of the AML/CFT Act) do not cover the overarching requirements for the level and frequency of supervision as a whole (onsite and offsite) to be risk-based, and there is no explicit reference to the elements at sub-criteria (a) and (c) (c.26.5(a)-(c)). • The UKNF, GIFI and NBP methodologies do not detail the intensity of supervision, although risk factors form part of supervisory engagement in practice. According to IO.3, there is scope to develop more comprehensive approaches to risk-based supervision. The approach from the NACSCU would seem to meet the aspects of the criterion not met by the AML/CFT Act to a very limited extent (c.26.5(a)-(c)) *(as per FUR December 2024).* • For GIFI there is no written policy or procedure in relation to the frequency of review assessment of a FI's risk rating (although in practice the annual inspection planning is based in the UKNF risk scoring of FIs, among other sources of data). There is no information about the NACSCU (c.26.6) *(as per FUR December 2024).*
33. Statistics	PC (MER 2021) **C (FUR2 2024)**	• All criteria are met.

GLOSSARY OF ACRONYMS

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
AT	Assessment team
C	Compliant
CDD	Customer due diligence
EU	European Union
EUR	Euro
Europol	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
FIs	Financial institutions
FUR	Follow-up report
GIFI	General Inspector of Financial Information
IT	Information technology
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	Money laundering
MLA	Mutual legal assistance
MoJ	Ministry of Justice
NACSCU	National Association of Cooperative Savings and Credit Unions
NC	Non-compliant
NBP	National Bank of Poland (Narodowy Bank Polski)
NCR	National Court Register
NRA	National risk assessment
PC	Partially compliant
PPO	Public prosecutor's office
R.	Recommendation
SAR	Suspicious activity report
TC	Technical compliance
TF	Terrorist financing
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

October 2024

Follow-up report

Anti-money laundering and counter-terrorist financing measures -

Poland

2nd 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.