

# Poland

## Fifth Round Mutual Evaluation Report

### Executive Summary

1. This report summarises the AML/CFT measures in place in Poland as at the date of the onsite visit, from 10 to 21 May 2021. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Poland's AML/CFT system and provides recommendations on how the system could be strengthened.

#### Key Findings

- a) The authorities have a limited understanding of the ML threats emanating from certain types of predicate offences; it lacks a comprehensive view of the factual/detected and potential/undetected amount of the proceeds of crime. There is a lack of uniform and comprehensive understanding of ML/TF vulnerabilities. Significant further efforts are needed towards appropriate identification and reliable assessment of TF risks. The National AML/CFT Strategy was adopted shortly before the onsite; there is no systemic approach and consistent action in Poland for the alignment of objectives and activities of competent authorities with national ML/TF policies. The FSC, as the national platform for co-operation and coordination at the policy-making level, is well positioned to define high-level goals and objectives, but an operative coordination platform or similar arrangements are missing. Efforts have been made to ensure that financial institutions and DNFBPs are aware of the results of the NRA, mainly through its publication on the website of the Ministry of Finance and through a series of conferences and workshops organised by GIFI.
- b) The GIFI is a key source of financial intelligence and other relevant information in Poland, with full access to a wide variety of information from the private and public sectors. Other competent authorities, including LEAs, extensively and routinely access information both from the GIFI and from other available sources. SAR reporting is not consistent with the risk profile of certain sectors and individual players. The outcomes of the GIFI preliminary and advanced analyses and the disseminations to the competent LEAs have proper structure, involve reasonable analysis and convey substantiated conclusions. Nevertheless, transformation ratios of the GIFI notifications and other disseminations to the PPO and the LEAs into investigations and indictments are low; LEAs mainly use the communication from the GIFI for their own statutory activities with little or no focus on tracing proceeds of crime.

- c) Poland has a broad range of LEAs, but none of them are designated with specific responsibility to investigate ML, which impacts their appetite to venture into an ML investigation. Overall, the ML cases are not fully prioritised, and the number of ML investigations remains behind the number of convictions for proceeds generating offences. ML investigations and prosecutions reflect, to some extent, the risk profile that the country faces, at least for the top three threats. Poland has demonstrated effective results in prosecuting and securing ML convictions, mostly in relation to self-laundering and third-party ML cases. As to stand-alone and foreign predicate offences connected ML cases, a positive trend is noticed. The authorities face a number of obstacles in investigating, prosecuting and adjudicating ML cases, including in relation to the high evidentiary standard applied in connection to the underlying predicate offence, the uncertainty as to the evidentiary requirements in proving stand-alone ML, the general lack of specialised experts in conducting parallel financial investigations (all authorities) and the limited expertise in conducting criminal investigations, impacting the quality of the presented evidence before the court (KAS). The penalties imposed in ML gradually increased, and whereas proportionate, they are not fully effective and dissuasive.
- d) Although LEAs have achieved some results, especially in cases of ML, the confiscation of proceeds and instrumentalities is not pursued as a policy objective. This is confirmed by the lack of relevant statistics on confiscations applied in relation to predicate offences, which negatively impacts authorities' ability to assess the effectiveness of the system and to take targeted policy measures to address the weaknesses. In cases of detected false or non-declaration, the restrained assets concern only the equivalent value of the fine for a fiscal crime and the remaining assets are returned, even in cases of suspicions of ML. The confiscations are not consistent with the ML/TF risks and national AML/CFT policies and priorities.
- e) Poland has taken some steps in a positive direction in the field of TF investigations - the legal framework has been expanded, and practical experience has been gained. The ISA is the main LEA responsible for identifying and investigating TF cases, which in practice are conducted primarily in connection with a terrorist offence. In the last seven years, ISA handled several TF cases, out of which three ended with charges. Further on, two TF convictions of four individuals were achieved, which is a positive outcome. The profile of the TF convictions is partially in line with the country risk profile. The prosecution and other LEA have not adopted methodological guidelines or instructions for TF investigations. It cannot be concluded that FT investigations have been integrated and used to support national counter-terrorism strategies. The sanctions applied in relation to the two sentences reached are minimal, hence not dissuasive or proportionate.
- f) Poland implements UNSCRs 1267 and 1373 and its successor resolutions without delay based on EU and internal legislation. No requests were received by the authorities, nor proposals or designations were made pursuant to UNSCRs 1267 and 1373. Poland did not apply freezing measures and did not restrain TF funds, partly corresponding to the overall TF country risk profile. Most material sectors of obligated institutions demonstrated comprehensive knowledge on the TF TFS related issues and their freezing and reporting obligations. Poland still needs to make efforts to perform a specific risk assessment on the NPO sector's exposure to TF risks. There

was guidance published on the GIFI website, however, the level of understanding by the NPO sector of their risk of FT exposure is not fully satisfactory.

- g) PF-related UNSCRs are applied in Poland through the EU mechanisms which do not suffer from technical problems in relation to the time of their transposition when it concerns Iran. Delays in the implementation of the UNSCRs of DPRK can still occur. No case of freezing assets held by persons or entities designated under PF sanctions programs has been registered in Poland. Most financial institutions understand their obligations and can take restrictive measures effectively should the situation occur. Some DNFBPs perform manual screening on the “lists” which are understood in a global manner: TF, PF TFS, together with the high-risk countries and PEPs. Others lack knowledge and understanding of their PF-related obligations. Supervisory authorities do not have responsibilities in ensuring and monitoring compliance with the PF TFS. Little specialised training on PF was provided to the private sector.
- h) All obligated institutions perform periodically updated risk assessments, and the banking sector, in particular, has demonstrated a good understanding of risks and implementation of mitigating measures, while smaller FIs and DNFBPs have a less sophisticated and sometimes more formalistic approach. The private sector is aware of the AML/CFT obligations, including adoption of CDD, EDD and TFS (with some shortcomings in the understanding of TFS by DNFBPs), and implement internal (or group-wide) controls and procedures. EDD measures mostly consist of incrementing the frequency and intensity of regular CDD measures, and, in the case of FIs, also includes ascertaining the source of funds and wealth via external support documentation, amongst other measures. DNFBPs tend to avoid high-risk business relationships and, as a result, the implementation of EDD is limited in practice. In terms of reporting suspicious activities, FIs employ comprehensive transaction monitoring systems and the reporting behaviour of REs is largely commensurate with their materiality and exposure to risks. VASPs equally implement preventive measures, but there is a lack of a harmonised approach due to the absence of a regulatory framework and guidance.
- i) The market entry licensing verifications checks carried out by the UKNF are generally robust, particularly in relation to legal and beneficial ownership. Some gaps in the controls of the senior management remain, mostly as a result of the legislation. The NBP performs fit and proper controls on currency exchange offices, but is also subject to limitations in the legislative framework it administers. Licensing and market entry checks are in place for the DNFBPs with some areas for improvement. Overall, the understanding of ML risks at individual firm and sector levels in relation to FIs by GIFI, the UKNF and the NBP is greater than that for DNFBPs and greater for ML risks compared with TF risks. The UKNF has the most comprehensive approach to supervision; its use of IT and data analytics is a key part of this. The UKNF supervisory team would benefit from a relatively small number of additional staff. There is no supervision of DNFBP sectors that are not subject to registration by the NCR. GIFI has a long history of applying sanctions and has made recommendations for prosecution. Limited sanctions have been imposed on DNFBPs in recent years, which is not consistent with the associated risks. While noting that there are areas for improvement in a range of areas relevant to this IO, the AT has attached significant weight to supervision of the banking sector.

- j) Basic and BO information is publicly available in Poland. There are a few elements of information on the creation and operation of business entities in the 2019 NRA report, albeit these are generic and not detailed. It is clear that the most serious risk of abuse of Polish companies is uniformly regarded as VAT fraud facilitated by the use of fictitious companies and “straw men”. Turning to mitigation measures, the National Court Register undertakes wide-ranging checks prior to registration and also after, including concerning financial statements. The number of fictitious companies has reduced during the last few years as a result of the national initiative aimed at identifying and dealing with such companies. Legal persons registered at the NCR after 13 October 2019 were required to insert BO information on the CRBO within one week of registration. Other sources of BO information are the obligated institutions and the KAS. The KAS prevented a significant number of legal persons from registering on the VAT register and has struck off a significant number of companies from the register. It has also increased VAT receipts. It has tangibly addressed the issue of use by fictitious companies, and statistics indicate it is being effective.
- k) Poland has a comprehensive legal framework for international co-operation. Most of the co-operation is carried out with other EU Member States, based on a simplified mechanism, while the co-operation with non-EU jurisdictions bordering Poland appears to be less constructive. The existing case management system is fragmented, and no guidelines exist with regard to the handling and prioritisation of the MLA requests, which impact the quality and timeliness of the execution of foreign MLA requests. There is no proactive harvesting of incoming MLA requests by competent authorities to detect potential domestic ML suspicions or TF cases related to these. Although statistics on MLA, extradition, and other forms of co-operation are not collected systematically (and there are doubts as to their accuracy), several successful examples of co-operation in ML and TF cases, including by establishing JITs, have been provided. Nevertheless, the co-operation in relation to seizure, freezing, confiscation and asset sharing have been demonstrated to be of limited effectiveness. The GIFI and LEAs proactively exchange information with their foreign counterparts and provide a good quality of assistance, although it remains unclear the extent to which this co-operation is carried out for AML/CFT purposes. The requirement to cooperate only upon the prior consent of the Prime minister (for CBA and ISA) may impact the effectiveness/ constructiveness of the provided/ required international assistance, especially in relation to urgent cases. Besides the GIFI, no other supervisory authority exchanges information with its foreign counterparts for AML/CFT purposes.

## Risks and General Situation

2. According to the first National Risk Assessment (NRA), conducted in 2019, Poland is exposed to medium money laundering (ML) and terrorism financing (TF) risks, which emanate from tax offences, corruption, illicit trafficking of narcotic drugs and psychotropic substances, human trafficking and immigrant smuggling, offences against property and economic transactions, offences related to the infringement of copyright and industrial property rights, financial crime, offences related to illegal gambling and document forgery. A high risk of money laundering arises from organised criminal groups, both domestic (or with Polish membership/connections) and international.

3. The terrorist threat is considered low in Poland. Nevertheless, the authorities are aware that the geopolitical situation and involvement in military actions may result in a certain risk of terrorist attacks. The geographical location of Poland also results in a risk of the use of on routes for the transportation of people and goods from Eastern Europe and Central and South-Eastern Asia. The NRA assesses the TF vulnerability as medium. The NPO sector was not assessed from a TF perspective. The authorities advise that, as of the moment, they have not identified cases where local NPOs were used for TF purposes, but there have been investigations with the GIFI on TF involvement of foreign NPOs.

### **Overall Level of Compliance and Effectiveness**

4. Poland has taken steps in strengthening its AML/CFT framework since its last evaluation, most notably by undertaking NRA and through changes in the AML/CFT Act. In most respects, the elements of an effective AML/CFT system are in place to some extent, but the practical application of the existing framework is still to be improved to reach a substantial level of compliance. Urgent action should be taken to ensure that criminals are deprived of the proceeds and instrumentalities of their crimes. There is a need to implement a mechanism to systematically collect comparable statistics to allow the authorities to critically evaluate the effectiveness of the criminal justice system and international co-operation. The private sector is more advanced in applying AML/CFT preventive measures commensurate to their risks.

5. In terms of technical compliance, the legal framework has been enhanced in several aspects, such as the customer due diligence requirements (R.10), the FIU (R.29) and TF-related TFS (R.6). Nevertheless, several issues remain, including criminalisation of TF (R.5), new technologies (R.15).

### ***Assessment of risk, coordination, and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)***

6. The authorities have a limited understanding of the ML threats emanating from certain types of predicate offences, with VAT-related tax crimes in the first place followed by investment and other fraud, trafficking of drugs, tobacco, alcohol and other goods, cybercrimes, abuse of power and misconduct in the trade of pharmaceuticals/ medicaments, etc. Nevertheless, organised crime, cross-border movements of cash and funds, corruption, specific predicate offences with the highest potential of generating proceeds of crime in the country are among the issues that need proper analysis and reasonable conclusions regarding Poland's exposure to the risk of ML/TF.

7. The risk of terrorism financing is perceived primarily as a derivative of the risk of terrorism, which is considered moderate in Poland. The understanding of TF risk is not supplemented by good awareness among intelligence and investigative agencies about the financial activities of individuals, groups and organisations potentially interested in infiltrating the AML/CFT system, as well as by express ability to trace potentially TF-related cash movements and transfers (especially those through the Hawala networks present in the country).

8. The measures stipulated under the priorities defined by the National AML/CFT Strategy would undeniably contribute to the enhancement of the effectiveness of the national AML/CFT system. Nonetheless, it is not apparent how these priorities reflect and address – by means of focused and targeted actions – the most prevalent threats and vulnerabilities identified through the NRA<sup>1</sup> and,

---

<sup>1</sup> For example, those listed in Tables 2 and 3 of the National AML/CFT Strategy as risk scenarios with highest likelihood levels (e.g. use natural persons as money mules for cross-border transportation of cash; use of Hawala networks; purchase or top-up of SIM cards or use of online payment services to transfer funds, etc.)

more importantly, those that still need proper identification and comprehensive assessment, as described under the analysis for Core Issue 1.1 and the introductory part of this report.

9. The current legislation does not provide for exemptions from any FATF Recommendations requiring financial institutions or DNFBPs to take specific actions. Obligated institutions may apply simplified CDD measures when their risk assessments confirm a lower risk of ML and TF. However, there is no requirement that such risk assessments are consistent with the NRA.

10. There are two platforms<sup>2</sup> considering issues related to AML/CTF coordination and co-operation. The first platform is comprised of 22 member agencies and chaired by the GIFI is the Financial Security Committee (FSC), operating under the provisions of the AML/CTF Act. It is an advisory and consultative body at the GIFI with competencies of giving opinions on programming documents (*e.g.* NRA and AML/CTF strategies), on EC recommendations and application of specific restrictive measures in the field of AML/CTF. The second platform comprised of 22 member agencies and chaired by the Minister of the Interior and Administration is the Inter-Ministerial Team for Terrorist Threats. Its tasks include monitoring terrorist threats, presenting opinions and conclusions to the Council of Ministers, and developing draft standards and procedures. SRBs with functions relevant for AML/CTF are not represented at any of these platforms. Moreover, none of these platforms is tasked with coordination and co-operation of issues related to CPF.

***Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; 10.6, 7, 8; R.1, 3, 4, 29–32)***

11. Accessing information held by obligated institutions is part of the GIFI's routine activities with appropriate legal empowerment and practical implementation. The GIFI is also authorised to request cooperating units, including LEAs, to provide or make available any information or documents, including the findings of analyses/ audits and the data in ongoing investigations, indicating timelines and forms for the communication of information. The authorities confirmed that such requests are part of daily operations of the GIFI and the cooperating units, for which separate statistics are not kept, but no impediments have ever been identified/reported.

12. On average, 91% of all SARs come under the regime stipulated by Article 74 of the AML/CFT Law, i.e. are associated with lower level suspicions whereby obligated institutions articulate circumstances potentially indicating the possibility of – but not features substantiating – ML/TF suspicions. The SARs filed under Article 86 over the considered period show a slowly increasing dynamic, which is indicative of the need for further guidance and training for obligated institutions to improve their skills and ability to file better justified SARs.

13. The GIFI advises that the significant majority of SARs filed by obligated institutions contain complete, accurate and adequate information that enables evaluating the case and, in combination with additional data available to it, making the decision whether the case should be disseminated to the PPO as a notification on suspicion of ML or TF, or other competent authorities as a notification on suspicion of other crimes.

14. The outcomes of the GIFI preliminary and advanced analyses, as well as of the disseminations to the competent LEAs, have proper structure, involve reasonable analysis, and convey substantiated

<sup>2</sup> The authorities also reported on another platform for co-operation and coordination, i.e. the Inter-Ministerial Team for coordinating activities under the 2015-2020 Program for the Preventing and Combating Economic Crime, comprised of 16 member agencies and chaired by the Minister of the Interior and Administration, with some tasks relevant for AML/CTF (*e.g.* establishing a register to enhance security and accessibility of financial data, preparing draft new regulation in accordance with EU requirements, etc.). However, this team ceased to exist in 2020.

conclusions. Nevertheless, transformation ratios of the GIFI notifications and other disseminations to the PPO and the LEAs into investigations and indictments are low; LEAs mainly use the communication from the GIFI for their statutory activities with little or no focus on tracing proceeds of crime.

15. Poland has demonstrated effective results in prosecuting and securing ML convictions, mainly in relation to self-laundering and, to some extent, in third-party ML cases. The absence of designated LEAs with specific responsibilities to investigate ML negatively impacts the appetite to initiate ML investigations. The focus primarily remains on the predicate offences with no due attention to the identification of proceeds and associated ML activities. This is confirmed by the general mindset that ML has little added value in criminal proceedings. Half of the ML prosecutions are initiated based on the FIU intelligence, although these appear to be less successful than those initiated from other sources. A positive trend is noticed in relation to the number of ML stand-alone and those with foreign predicate offences.

16. Parallel financial investigations are not conducted systematically but rather on a case-by-case basis. This is evident with the low results achieved when comparing the number of proceeds generating predicate crimes investigated with the number of cases where money laundering was additionally investigated and proceeds seized. ML investigations and prosecutions reflect, to some extent, the risk profile that the country faces, mostly with relation to ML of tax-related crimes and fraud. The penalties imposed in ML gradually have increased. However, they are not fully effective and dissuasive. Poland has not yet achieved convictions concerning legal persons.

17. The confiscation of criminal proceeds, instrumentalities and property of equivalent value is not pursued as a policy objective, although some results have been achieved in ML cases. The courts routinely order the confiscation of assets. However, the lack of meaningful and, in some cases, fragmented information, as well as the lack of any strategic analysis on the effectiveness of the entire repressive system through the deprivation of criminals of illegally acquired property, all prevent the ability to assess the effectiveness of the system. Among the questions that remain unclear are which criminal offences have the provisional measures and confiscation been applied, whether there are measures against proceeds located abroad, to which extent instrumentalities and equivalent value are confiscated, assets recovered and other aspects necessary for evaluating the effectiveness of the system. The absence of a single mechanism for managing/disposing of seized or confiscated property and of a centralised authority in charge of the management of such property negatively impacts the overall effectiveness of the confiscation regime.

18. The effective implementation of the cross-border cash control regime in the non-EU borders has resulted in convictions for fiscal crimes and related penalties of fines for undeclared cash, although the average value of fines is insignificant compared to the value of undeclared cash. When undeclared cash is detected, restraint is limited to the equivalent value of the potential fine for the false/ non-declarations; this is true even in cases of suspicions of ML. Only a few ML investigations have been started on the basis of a cash declaration system. This is not in line with the risks faced by the jurisdiction.

#### ***Terrorist and proliferation financing (Chapter 4; 10.9, 10, 11; R. 1, 4, 5-8, 30, 31 & 39)***

19. The NRA identifies the TF risk in Poland as medium due to its geographical location and the inherent international risks. Beyond this, the understanding of TF risk is not supplemented by good awareness about purely financial activities of individuals, groups and organisations potentially linked with terrorism that could abuse the Polish system of its financing. As a result, there is a limited ability

to trace potentially TF-related movements and transfers, especially using Hawala networks and launching TF investigations that would be more consistent with the country's risks.

20. In the assessed period, two TF convictions of four individuals were achieved, which is a positive outcome. In both conviction cases, the financing of terrorism took place in Poland, and the accused were Polish citizens or had strong ties with Poland. The profile of the convictions is partially in line with the country's risk profile.

21. The main source of potential TF cases for the ISA is intelligence acquired during the course of already initiated terrorism cases. The methods of collecting information include operational and reconnaissance activities, monitoring open sources and analysis of accessible databases. Other sources that might trigger a TF preliminary analysis are information stemming from operational activities and leads from other agencies, including foreign counterparts.

22. Between 2016 and 2020, FIU submitted 237 disseminations to ISA concerning potential links with terrorism, without those being actual TF reports, which in any case should have been filed to the Prosecutor's Office. No TF case was prompted by ISA following those disseminations; nevertheless, in one of the investigations, information from FIU was used (the case is ongoing).

23. It cannot be concluded that the TF investigations are integrated and used to support national counter-terrorism strategies, as Poland does not have a document that would constitute a national anti-terrorism financing strategy.

24. Despite the availability of sanctions, the penalties applied in practice in relation to the two convictions achieved are minimal and not sufficiently dissuasive. In one case, complex TF actions were punished by imprisonment of two years and one month. The second case, apparently less serious, comprised punishments of one to three years. No positive conclusion can hence be drawn on the proportionality of sanctions.

25. FT-related TFS are implemented on the basis of the AML/CFT Law, additionally to the relevant EU Regulations, which are directly applicable in Poland. The Law sets the procedural steps for proposing or listing persons or entities, for considering listing at the request of other states, and for issuing requests for freezing to other countries. However, the authorities do not have uniform procedures or mechanisms for identifying targets for designation / listing, de-listing, and granting exemption.

26. Generally, the obligated institutions comply with the specific restrictive measures to persons and entities indicated in the lists announced by the GIFI pursuant to the UNSCRs. In case of a hit, the information associated with the freezing of assets shall be provided to the GIFI immediately, no later than two business days following the day of the freezing.

27. Poland identified through the NRA the subset of organisations that fall within the FATF definition of NPOs which include all foundations and associations but did not carry out a specific risk assessment on the NPOs sector exposure to TF risks. The frequency and monitoring of NPOs at risk were not subject to review. Some outreach was reported, mostly for the authorities supervising foundations, but this pertains to the amended provisions of the AML/CFT Act and not to the risk. NPOs (except associations that are not PBO) are subject to a number of transparency and reporting requirements. PBO's financial statements are published on their websites and on the website of the National Institute of Freedom. They are subject to additional scrutiny owing to their tax-preferential status.



28. In relation to TF convictions achieved so far, the applied confiscation measures aimed at depriving the terrorists of the allocated or used instrumentalities, although not always successfully. In one case, out of the total amount of the collected and moved funds and other assets (paramilitary equipment), only €1 900 were seized and subsequently confiscated. Poland has not been reported any freezing under UNSCRs 1267 and 1373.

29. Targeted financial sanctions concerning the UNSCRs relating to the combating of financing of proliferation are addressed through the EU mechanisms, which do not suffer from technical problems in relation to the time of their transposition when it concerns Iran. Individuals and entities had already been listed by the EU when their designation by the UN was made. No case of freezing assets has been registered in Poland related to the PF UNSCRs, up to now. The trade in goods and technologies such as military equipment and dual-use goods, including technologies related to weapons of mass destruction, are subject to control by the state.

### ***Preventive measures (Chapter 5; IO.4; R.9–23)***

30. All REs perform regularly updated risk assessments. Some entities, particularly the banking sector, which is the most material one, demonstrate a remarkable degree of risk understanding. Others (mostly smaller FIs and DNFBPs) adopt a more formalistic approach towards risk assessment, showing a lower degree of understanding of business-specific risks.

31. FIs and DNFBPs are aware of their AML/CFT obligations and implement internal controls and procedures. In the case of larger FIs, who belong to international financial groups, the implementation of group-wide procedures enhances the overall degree of AML compliance due to the requirement to often adopt higher standards.

32. EDD measures mostly consist of incrementing the frequency and intensity of regular CDD measures and, in the case of FIs, also includes ascertaining the source of funds and wealth via external support documentation, amongst other measures. DNFBPs tend to avoid high-risk business relationships, and as a result, the implementation of EDD is limited in practice. Overall, termination or non-acceptance of business relationships is frequent, particularly in such cases in which the entity cannot be satisfied with the identification and verification of the identity of the beneficial owner.

33. FIs establish comprehensive transaction monitoring systems based on alert-generating IT tools. However, there are instances in which a heavy reliance on these systems is placed without fully considering whether the determined risk scenarios are commensurate to the business profile and risks that have been detected. In terms of reporting of suspicious activities, banks amount for the vast majority of SARs, with other FIs and DNFBPs reporting significantly lower numbers, although this is largely commensurate with their materiality and exposure to risks.

34. Regarding VASPs, there is no appetite among FIs to onboard them as customers, a behaviour that is encouraged by the authorities. VASPs themselves implement preventive measures, as AML/CFT reporting entities, but there is a lack of a harmonised approach due to the absence of a regulatory and licensing framework, as well as guidance.

### ***Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)***

35. The UKNF has the most robust entry checks for all obligated institutions, particularly in relation to legal and beneficial ownership. Nevertheless, there are gaps in the controls, particularly in relation to some senior management, and there is also a need to complement staff resources in the licensing department for banks.

36. The framework administered by the NBP in preventing criminal control of currency exchange offices is targeted at legal owners and senior management; currency exchange activity may only be performed by individuals with a clean criminal record. The current legal framework does not allow for the controls to be more developed.

37. With the exception of credit unions, FIs not subject to the supervision of the UKNF or the NBP, such as non-bank lenders and factoring firms, are not subject to checks to prevent control by criminals. Casino operators are subject to some licensing controls in relation to shareholders, but there are gaps in controls relating to beneficial owners and some senior management positions. The controls in place for legal practitioners and notaries are basic. There are also no developed market entry controls in place for real estate brokers, DPMS and any TCSPs when undertaking activities covered by the FATF. There are no market entry controls in place with regard to VASPs.

38. The understanding of ML risks at individual firm and sector levels in relation to FIs by the GIFI, the UKNF and the NBP is greater than that for DNFBPs and greater for ML risks compared with TF risks. For some years, financial supervisors have risk rated FIs for ML/TF risk; they receive offsite and onsite information and undertake onsite and offsite supervision. Each of the methodologies used has created differentiation of risk between institutions.

39. Supervision by the UKNF and the GIFI includes good elements of risk-based supervision, and GIFI has commenced supervision of VASPs. The NBP also undertakes elements of risk-based supervision and, although there is scope for refinement, it provides the best model in Poland for coordination for organisations with regional offices engaged in AML/CFT. However, there is a significant shortfall in resources at GIFI, which handicaps the extent of its supervision and its ability as the “lead” AML/CFT supervisor to coordinate the overall supervisory engagement of the authorities.

40. There is no supervision of DNFBP sectors that are not subject to registration. Registered DNFBPs are not risk rated, and with the exception of notaries, they are subject to a much lesser degree of supervision. GIFI has been able to undertake some supervision of DNFBPs on the basis of risk-based triggers.

41. GIFI was the only supervisory authority that could, up until July 2018, impose sanctions for AML/CFT breaches and has made recommendations for prosecutions; since then, the UKNF and the NBP also have powers of sanction. The UKNF has imposed a few penalties and has sought to develop a more robust approach since 2018. The NBP has issued fines for some years, including to individuals, although there was a shortfall prior to 2020 compared with the risks of the currency exchange sector. Limited sanctions have been imposed on DNFBPs in recent years, which are not consistent with the risks represented by DNFBPs.

42. GIFI, the UKNF and the NBP have been particularly active and have made substantial efforts to promote understanding by supervised entities of their obligations.

43. Supervision and awareness-raising by supervisors have made a positive difference to the level of AML/CFT compliance by FIs and registered DNFBPs.

#### ***Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)***

44. Poland has assessed elements of the ML/TF risks associated with legal persons. There is a common understanding as to the primary risk of abuse of legal persons (fictitious companies fronted by “straw men” used for VAT fraud and associated ML). A Government-led initiative has been introduced to address the risks of fictitious companies. The number of fictitious companies has

reduced during the last few years as a result of the national initiative aimed at identifying and dealing with such companies.

45. The overall approach to transparency is multi-faceted. There is very good operational exchange of information between authorities. There are elements of coordination and some statistics relevant to considering effectiveness, although overall coordination of the framework as a whole and measurement of effectiveness has yet to be fully developed.

46. Information on the types of legal persons is maintained in the public domain.

47. Basic information is maintained in the National Court Register (NCR). A significant number of applications for registration is refused or dismissed. The wide-ranging checks undertaken by the NCR team prior to registration and also after registration and receipt and review of financial statements provide benefits in addressing the risk of fictitious companies. Court officials are also responsive to information received in ensuring the database is correct. While the data on the register is regarded as being very good quality by the authorities using it, there is some scope to enhance the existing checks to complement the positive activities and outcomes to date.

48. Poland has established a central, publicly accessible register of beneficial owners of legal persons (CRBO), which commenced operation in 2019. The large majority of legal persons have registered information in the register, although almost a quarter of legal persons remain to be registered. The CRBO and other authorities have a positive view of the quality of the data registered to date. In order to ensure that data is adequate, accurate and current, the CRBO team started undertaking a major sampling exercise and strong checks on the data selected. The KAS, the UKNF and GIFl routinely use the information on the register, which has the effect of checking the information used.

49. Poland has also established the National Clearing House (NCH), a database of information provided by banks on owners and beneficial owners of bank accounts and transactions made using the accounts. The NCH team checks the data is complete but does not verify its accuracy. The KAS, the UKNF and GIFl routinely use the information on the NCH, which has the effect of checking it.

50. The basic and beneficial ownership registers and the NCH are complemented by information held by banks, notaries and lawyers. A considerable number of legal persons are subject to CDD by more than one obligated institution. Almost all legal persons have a bank account. There are very positive aspects to banks' approaches to beneficial ownership, and the UKNF, GIFl (as supervisor and FIU) and the KAS have found information held by banks to be generally reliable. Banks' approaches to obtaining information have improved and continuing to develop.

51. The team administering the CRBO has commenced an approach to sanctions. However, notwithstanding some very positive aspects, the overall sanctions framework for the system as a whole (noting also the relevant aspects of IO.3 and IO.7) is not comprehensively dissuasive.

52. GIFl (as an FIU) has interrogated all of the financial intelligence it holds on legal persons and compared it with the NCR and CRBO. Mismatches have been advised to the relevant registry team.

53. The KAS undertakes sophisticated and multi-faceted analytical and investigative activity relevant to combatting misuse of legal persons and ensuring the adequacy, accuracy and currency of basic and beneficial ownership information. Risk scoring has allowed the KAS to target the risk of VAT fraud (i.e. fictitious companies) and use its resources in a risk-based way.

54. The KAS prevented a significant number of legal persons from registering on the VAT register and has struck off a significant number of companies from the register. It has also increased VAT receipts. It has tangibly addressed the issue of use by fictitious companies, and statistics indicate it is being effective. The Court has initiated a substantial number of proceedings as a tool to generate the production of information. It has also imposed some fines (although statistics are not kept on the number and level) and also struck off a substantial number of companies (including fictitious companies).

### ***International co-operation (Chapter 8; IO.2; R.36–40)***

55. Polish legislation sets out a comprehensive framework for international co-operation, enabling the authorities to provide assistance concerning ML/TF and associated predicate offences. The MoJ acts as the central authority for the incoming and outgoing MLA requests. Its role is particularly important with regard to the international co-operation with non-EU countries, as the mechanism is different from the one concerning the co-operation with EU countries, where there is direct co-operation between the authorities.

56. International co-operation is an essential component of Poland's AML/CFT system, given its geographical location at the crossroad of Europe's main communications routes. Its status as a transit country for illegal immigration, drug trafficking, smuggling and other forms of organised crimes exposes the country to an increased outside ML/TF risk.

57. Poland proactively interacts with foreign counterparts from EU countries and has demonstrated, through various case examples, effective co-operation with other EU MS. Nevertheless, this applies, to a much lesser extent, to co-operation with non-EU countries, some of which pose a high risk for the country from an AML/CFT perspective. The lack of comprehensive statistics, including a breakdown by jurisdiction, also prevents the authorities from demonstrating if the co-operation is used constructively to address ML/TF threats of international nature faced by the country.

58. The management and monitoring of the quality and timeliness of the execution of foreign MLA requests are fragmented with no centralised case management system. This impacts the ability to assess the timeliness of the provided assistance and the prioritisation mechanism.

59. The GIFI has a broad legal basis for international co-operation and proactively and constructively interacts with its foreign counterparts by exchanging information on ML/TF. The assistance provided by the GIFI upon request or spontaneously is considered effective in terms of the quality and timeliness of its foreign counterparts.

60. LEAs proactively exchange information with their foreign counterparts and have demonstrated their ability to establish Joint Investigative Teams. The feedback received from the international community illustrates that LEAs provide timely and high-quality assistance to their foreign counterparts. Nevertheless, in the absence of comprehensive statistics, i.e. incoming/outgoing requests; breakdown based on the predicate offences, jurisdictions, it is difficult to assess the volume, dynamic and the area of co-operation, although some successful examples of co-operation in relation to ML cases have been provided. The absence of such data also prevents the Polish authorities from following up and assessing the effectiveness of international exchange of information, and measuring the extent to which these information exchanges result in successful investigation and prosecution of ML and TF using MLA, and where not, if country-specific impediments exist to prevent such anticipated results.

61. The supervisory authorities (other than the GIFI) regularly exchange information with their foreign counterparts, but not for AML/CFT purposes.
62. Polish authorities provide and respond to foreign requests for international co-operation in identifying and exchanging basic and beneficial ownership information of legal persons registered in Poland. Such requests are usually part of more general inquiries. Several examples were presented, which demonstrated positive feedback to the assistance provided.

### Priority Actions

- a) The authorities should take urgent action (i.e., through strategic and methodological documents and guidance) to ensure that the confiscation of criminal proceeds, instrumentalities and property of equivalent value is pursued as a policy objective. A consistent practise should be developed to enhance the asset tracing, seizing and recovery aspect of the investigations to substantiate motions for application of every form of forfeiture. (IO8)
- b) The authorities should take steps to collect and maintain meaningful, comprehensive and comparable statistics, mainly on seized, confiscated, shared and returned assets for all proceeds generating offences and all forms of international co-operation, based on which a strategic document should be adopted to address the shortcomings and allocate resources. (IO8, IO2)
- c) Proper analysis should be conducted to arrive at reasonable conclusions on the country's exposure to the ML/TF risks due to, inter alia, organised crime, specific predicate offences with the highest potential of generating proceeds of crime, cross-border movements of cash and funds, as well as due to activities of professional money launderers and availability of certain higher-risk products/ services. Comprehensive assessment should be undertaken to achieve adequate understanding of all aspects of the country's exposure to the risk of TF (IO1)
- d) A systemic approach should be introduced, and consistent action should be taken towards alignment of objectives and activities of competent authorities with national ML/TF policies by means of incorporating risk assessment outcomes into their roles and priorities, adjusting agency-level policies with risk assessment outcomes, implementing institutional and operational changes driven by a focus on identified/emerging risks. (IO1)
- e) The GIFI should further develop and implement a comprehensive set of criteria for prioritisation of SARs and related analytical proceedings, to enhance the support of the operational needs of competent authorities in ML/TF cases; efforts of all involved agencies need to be significantly enhanced to achieve early detection of suspicious business relationships and transactions, thus also preventing large turnovers before they are reported to the GIFI and disseminated to the LEAs. (IO6)
- f) The practice of reporting under Article 86 of the AML/CFT Act for higher-level suspicions should be improved through guidance aimed to secure blocking or suspension of as many funds as possible, especially in case of accounts used for transiting funds through the Polish financial system. (IO6)

- g) Procedural and institutional measures should be undertaken to ensure that ML is detected and investigated in all potential cases, including by: i) enhancing and formalising the rules for conducting operational activities and adopting a coherent practice for tasking LEAs with ML investigations; ii) pursuing ML as a priority and prosecuting a wider range of ML offences, including autonomous ML, for criminal activity which is in line with the ML threats and risks of Poland; iii) ensuring the financial aspect is systematically explored by all LEAs and that detailed guidelines are available to them on ML and parallel financial investigations; iv) enhancing the mechanism for detecting ML/ TF suspicions as a result of false or non-declarations of cross-border cash and ensure proactive investigation of such cases. (IO7, IO8)
- h) The authorities should take measures to clarify that the TF is a stand-alone crime and not a byproduct of terrorism both in terms of risk and criminalisation, and the technical deficiencies under R30 and 32 should be addressed. The border cash control mechanisms should be strengthened by providing a legal basis to administratively stop and restrain terrorist and FT suspicious assets. (IO9)
- i) A specific risk assessment on the NPO sector's exposure to TF risks should be conducted, and more targeted measures should be applied for those entities which are more vulnerable to TF abuse. (IO10)
- j) A supervisory system on PF-TFS must be urgently put in place. The authorities should perform awareness-raising activities to enhance the knowledge and understanding of some authorities (Border Guard) and entities of the private sector (especially DNFBPs) on PF-related TFS obligations. (IO11)
- k) Poland should address the gaps which exist for FIs, DNFBPs and VASPs in relation to preventing criminal control of obligated institutions and provide resources to allow for the comprehensive exercise of those controls and comprehensive risk-based supervision. This should include additional coordination and monitoring by GIFI to ensure supervision by each supervisory authority is risk-based and effective. (IO3)
- l) Poland should develop the NRA to undertake a comprehensive risk assessment and understanding in relation to legal persons and ensure that the Financial Security Committee undertakes robust coordination of risk-based activities by the authorities so that basic and beneficial ownership information held in Poland is adequate, accurate and current. (IO1, IO5)

## Effectiveness & Technical Compliance Ratings

### Effectiveness Ratings

Note: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE level of effectiveness.


<b>IO.1 – Risk, policy and coordination</b>	<b>IO.2–International co-operation</b>	<b>IO.3 – Supervision</b>	<b>IO.4 – Preventive measures</b>	<b>IO.5–Legal persons and arrangements</b>	<b>IO.6 – Financial intelligence</b>
ME	SE	ME	SE	SE	ME
<b>IO.7–ML investigation &amp; prosecution</b>	<b>IO.8 – Confiscation</b>	<b>IO.9–TF investigation &amp; prosecution</b>	<b>IO.10–TF preventive measures &amp; financial sanctions</b>	<b>IO.11 – PF financial sanctions</b>	
ME	LE	ME	ME	ME	

### Technical Compliance Ratings

Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.

<b>R.1 - Assessing risk &amp; applying risk-based approach</b>	<b>R.2-National co- and operation coordination</b>	<b>R.3-Money laundering offence</b>	<b>R.4 - Confiscation &amp; provisional measures</b>	<b>R.5 - Terrorist financing offence</b>	<b>R.6 - Targeted financial sanctions – terrorism &amp; terrorist financing</b>
PC	LC	LC	LC	PC	LC
<b>R.7- Targeted financial sanctions - proliferation</b>	<b>R.8 -Non-profit organisations</b>	<b>R.9 - Financial institution secrecy laws</b>	<b>R.10 - Customer due diligence</b>	<b>R.11 - Record keeping</b>	<b>R.12 - Politically exposed persons</b>
PC	PC	C	LC	LC	LC
<b>R.13 - Correspondent banking</b>	<b>R.14 - Money or value transfer services</b>	<b>R.15 - New technologies</b>	<b>R.16 - Wire transfers</b>	<b>R.17 - Reliance on third parties</b>	<b>R.18 - Internal controls and foreign branches and subsidiaries</b>
PC	LC	PC	LC	PC	PC
<b>R.19 - Higher-risk countries</b>	<b>R.20 - Reporting of suspicious transactions</b>	<b>R.21 - Tipping-off and confidentiality</b>	<b>R.22 - DNFBPs: Customer due diligence</b>	<b>R.23 - DNFBPs: Other measures</b>	<b>R.24 - Transparency &amp; BO of legal persons</b>
PC	PC	LC	PC	LC	LC
<b>R.25 - Transparency &amp; BO of legal arrangements</b>	<b>R.26 - Regulation and supervision of financial institutions</b>	<b>R.27 - Powers of supervision</b>	<b>R.28 - Regulation and supervision of DNFBPs</b>	<b>R.29 - Financial intelligence units</b>	<b>R.30 - Responsibilities of law enforcement and investigative authorities</b>
LC	PC	LC	PC	C	LC
<b>R.31 - Powers of law enforcement and investigative authorities</b>	<b>R.32 - Cash couriers</b>	<b>R.33 - Statistics</b>	<b>R.34 - Guidance and feedback</b>	<b>R.35 - Sanctions</b>	<b>R.36 - International instruments</b>
LC	PC	PC	PC	PC	LC
<b>R.37 - Mutual legal assistance</b>	<b>R.38 - Mutual legal assistance: freezing and confiscation</b>	<b>R.39 - Extradition</b>	<b>R.40 - Other forms of international co-operation</b>		
LC	LC	LC	LC		

All rights reserved. Reproduction is authorised, provided the source is acknowledged, save where otherwise stated. For any use for commercial purposes, no part of this publication may be translated, reproduced or transmitted, in any form or by any means, electronic (CD-ROM, Internet, etc.) or mechanical, including photocopying, recording or any information storage or retrieval system without prior permission in writing from the MONEYVAL Secretariat, Directorate General of Human Rights and Rule of Law, Council of Europe (F-67075 Strasbourg or [moneyval@coe.int](mailto:moneyval@coe.int))



© MONEYVAL

[www.coe.int/MONEYVAL](http://www.coe.int/MONEYVAL)