

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

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

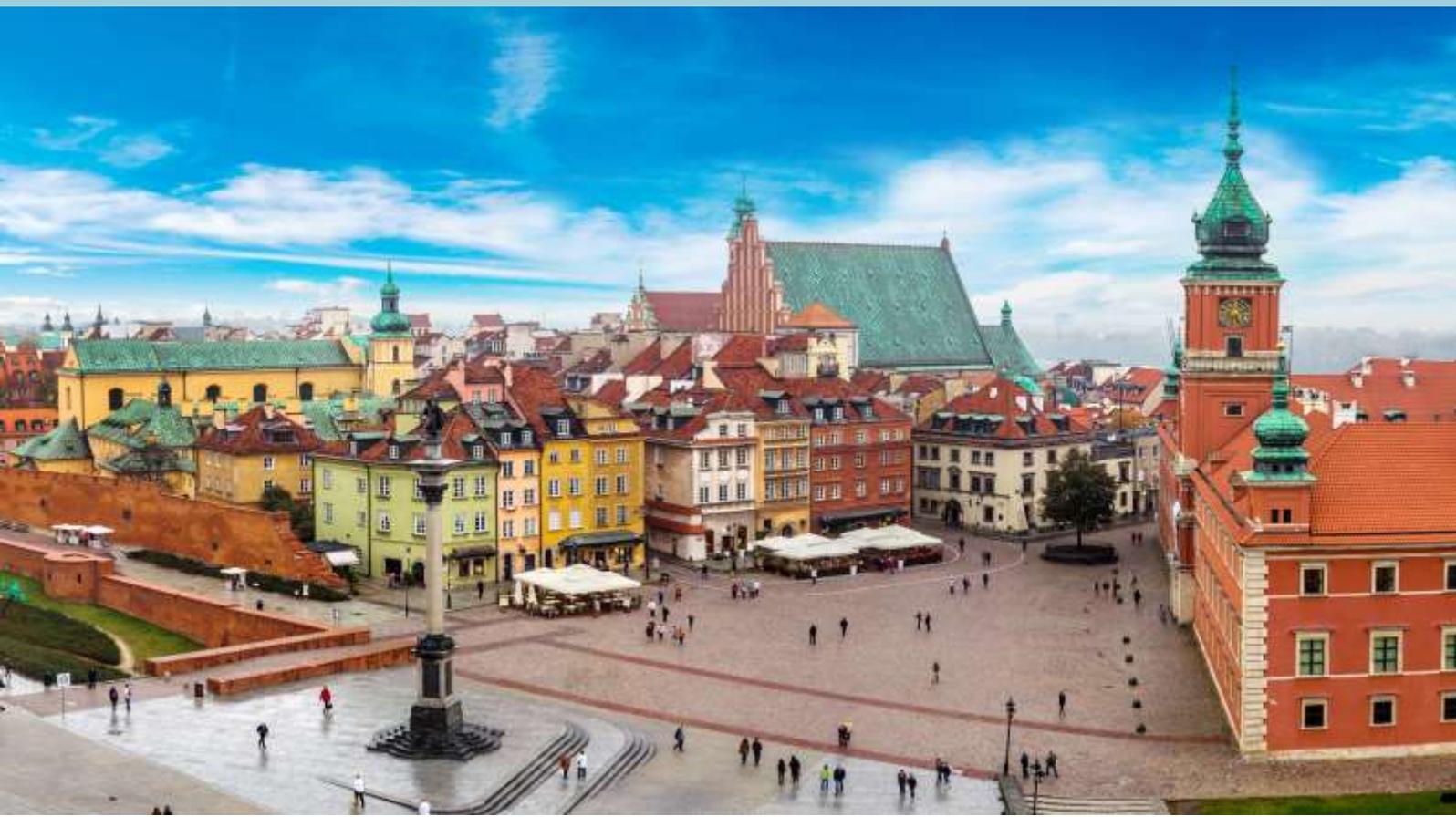
MONEYVAL(2021)25

# Anti-money laundering and counter-terrorist financing measures

# Poland

## Fifth Round Mutual Evaluation Report

December 2021



**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 fifth round mutual evaluation report on Poland was adopted by the MONEYVAL Committee at its 62<sup>nd</sup> Plenary Session

(Strasbourg, 16 December 2021).

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))

## Contents

<b>EXECUTIVE SUMMARY</b> .....	<b>5</b>
KEY FINDINGS.....	5
RISKS AND GENERAL SITUATION.....	8
OVERALL LEVEL OF COMPLIANCE AND EFFECTIVENESS.....	9
PRIORITY ACTIONS.....	17
EFFECTIVENESS & TECHNICAL COMPLIANCE RATINGS.....	19
EFFECTIVENESS RATINGS.....	19
TECHNICAL COMPLIANCE RATINGS.....	19
<b>MUTUAL EVALUATION REPORT</b> .....	<b>20</b>
<b>1. ML/TF RISKS AND CONTEXT</b> .....	<b>21</b>
1.1. ML/TF RISKS AND SCOPING OF HIGHER RISK ISSUES.....	21
1.2. MATERIALITY.....	24
1.3. STRUCTURAL ELEMENTS.....	24
1.4. BACKGROUND AND OTHER CONTEXTUAL FACTORS.....	25
<b>2. NATIONAL AML/CFT POLICIES AND COORDINATION</b> .....	<b>34</b>
2.1. KEY FINDINGS AND RECOMMENDED ACTIONS.....	34
2.2. IMMEDIATE OUTCOME 1 (RISK, POLICY AND COORDINATION).....	36
<b>3. LEGAL SYSTEM AND OPERATIONAL ISSUES</b> .....	<b>47</b>
3.1. KEY FINDINGS AND RECOMMENDED ACTIONS.....	47
3.2. IMMEDIATE OUTCOME 6 (FINANCIAL INTELLIGENCE ML/TF).....	52
3.3. IMMEDIATE OUTCOME 7 (ML INVESTIGATION AND PROSECUTION).....	74
3.4. IMMEDIATE OUTCOME 8 (CONFISCATION).....	90
<b>4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION</b> .....	<b>100</b>
4.1. KEY FINDINGS AND RECOMMENDED ACTIONS.....	100
4.2. IMMEDIATE OUTCOME 9 (TF INVESTIGATION AND PROSECUTION).....	103
4.3. IMMEDIATE OUTCOME 10 (TF PREVENTIVE MEASURES AND FINANCIAL SANCTIONS).....	112
4.4. IMMEDIATE OUTCOME 11 (PF FINANCIAL SANCTIONS).....	121
<b>5. PREVENTIVE MEASURES</b> .....	<b>126</b>
5.1. KEY FINDINGS AND RECOMMENDED ACTIONS.....	126
5.2. IMMEDIATE OUTCOME 4 (PREVENTIVE MEASURES).....	128
<b>6. SUPERVISION</b> .....	<b>146</b>
6.1. KEY FINDINGS AND RECOMMENDED ACTIONS.....	146
6.2. IMMEDIATE OUTCOME 3 (SUPERVISION).....	149
<b>7. LEGAL PERSONS AND ARRANGEMENTS</b> .....	<b>177</b>
7.1. KEY FINDINGS AND RECOMMENDED ACTIONS.....	177
7.2. IMMEDIATE OUTCOME 5 (LEGAL PERSONS AND ARRANGEMENTS).....	180
<b>8. INTERNATIONAL CO-OPERATION</b> .....	<b>205</b>
8.1. KEY FINDINGS AND RECOMMENDED ACTIONS.....	205
8.2. IMMEDIATE OUTCOME 2 (INTERNATIONAL CO-OPERATION).....	207
<b>TECHNICAL COMPLIANCE ANNEX</b> .....	<b>222</b>
RECOMMENDATION 1 – ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH.....	222

RECOMMENDATION 2 - NATIONAL CO-OPERATION AND COORDINATION .....	225
RECOMMENDATION 3 - MONEY LAUNDERING OFFENCE .....	226
RECOMMENDATION 4 - CONFISCATION AND PROVISIONAL MEASURES .....	229
RECOMMENDATION 5 - TERRORIST FINANCING OFFENCE .....	231
RECOMMENDATION 6 - TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING .....	235
RECOMMENDATION 7 - TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION .....	239
RECOMMENDATION 8 - NON-PROFIT ORGANISATIONS.....	241
RECOMMENDATION 9 - FINANCIAL INSTITUTION SECRECY LAWS .....	245
RECOMMENDATION 10 - CUSTOMER DUE DILIGENCE.....	247
RECOMMENDATION 11 - RECORD-KEEPING.....	252
RECOMMENDATION 12 - POLITICALLY EXPOSED PERSONS.....	253
RECOMMENDATION 13 - CORRESPONDENT BANKING .....	255
RECOMMENDATION 14 - MONEY OR VALUE TRANSFER SERVICES.....	256
RECOMMENDATION 15 - NEW TECHNOLOGIES.....	258
RECOMMENDATION 16 - WIRE TRANSFERS .....	261
RECOMMENDATION 17 - RELIANCE ON THIRD PARTIES.....	265
RECOMMENDATION 18 - INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES.....	266
RECOMMENDATION 19 - HIGHER-RISK COUNTRIES.....	269
RECOMMENDATION 20 - REPORTING OF SUSPICIOUS TRANSACTION.....	270
RECOMMENDATION 21 - TIPPING-OFF AND CONFIDENTIALITY.....	272
RECOMMENDATION 22 - DNFBPs: CUSTOMER DUE DILIGENCE .....	273
RECOMMENDATION 23 - DNFBPs: OTHER MEASURES.....	274
RECOMMENDATION 24 - TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS .....	276
RECOMMENDATION 25 - TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS.....	285
RECOMMENDATION 26 - REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS.....	287
RECOMMENDATION 27 - POWERS OF SUPERVISORS .....	291
RECOMMENDATION 28 - REGULATION AND SUPERVISION OF DNFBPs .....	293
RECOMMENDATION 29 - FINANCIAL INTELLIGENCE UNITS.....	296
RECOMMENDATION 30 - RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES.....	300
RECOMMENDATION 31 - POWERS OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES .....	302
RECOMMENDATION 32 - CASH COURIERS .....	304
RECOMMENDATION 33 - STATISTICS.....	306
RECOMMENDATION 34 - GUIDANCE AND FEEDBACK.....	308
RECOMMENDATION 35 - SANCTIONS.....	309
RECOMMENDATION 36 - INTERNATIONAL INSTRUMENTS.....	310
RECOMMENDATION 37 - MUTUAL LEGAL ASSISTANCE .....	311
RECOMMENDATION 38 - MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION .....	313
RECOMMENDATION 39 - EXTRADITION .....	314
RECOMMENDATION 40 - OTHER FORMS OF INTERNATIONAL CO-OPERATION .....	315
<b>SUMMARY OF TECHNICAL COMPLIANCE - DEFICIENCIES.....</b>	<b>321</b>
ANNEX TABLE 1. COMPLIANCE WITH FATF RECOMMENDATIONS.....	321
GLOSSARY OF ACRONYMS.....	328

## 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 TF 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; 10.1, 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, 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; IO.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

---

<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.)

<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.

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 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; IO.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 GIFI 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 accountants 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 GIFI 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, GIFI (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. GIFI (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; 10.2; 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.a.*, 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-operation and 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		

## MUTUAL EVALUATION REPORT

### Preface

1. This report summarises the AML/CFT measures in place as at the date of the onsite visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system and recommends how the system could be strengthened.
2. This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country and information obtained by the evaluation team during its onsite visit to the country from 10 to 21 May 2021.
3. The evaluation was conducted by an assessment team consisting of: Mr Arakel MELIKSETYAN, Head of FIU Armenia, and Mr Andrian MUNTEANU, Deputy director FIU Moldova, Law enforcement evaluators; Ms Vanya ILIEVA, Prosecutor, Supreme Prosecutor's office of cassation, Bulgaria and Dr Balázs GARAMVÖLGYI, Prosecutor, Deputy Head of Department, Office of the Prosecutor General of Hungary, acting as Legal evaluators; Mr Richard WALKER, Director of Financial Crime Policy and International Regulatory Advisor, Office of the Policy and Resources Committee of the States of Guernsey and Mr Gerard PRAST CLAVERO, AML/CFT Supervisory expert UIFAND Andorra, with the support from the MONEYVAL Secretariat of Irina TALIANU, Stela BUIUC, Alexey SAMARIN and Lorena UNGUREANU. The report was reviewed by Ms Jelena ILIC (Serbia), Mr Borislav CVORO (Bosnia and Herzegovina), Ms Catherine ROZAN (Germany). and the FATF Secretariat.
4. Poland previously underwent a MONEYVAL Mutual Evaluation in 2013, conducted according to the 2004 FATF Methodology. The 2013 evaluation and 2017 and 2018 follow-up reports have been published and are available at [Poland \(coe.int\)](https://www.coe.int).
5. That Mutual Evaluation concluded that the country was compliant with 2 Recommendations; largely compliant with 21; partially compliant with 17.
6. Poland was removed from the Follow-up process in 2018.

## 1. ML/TF RISKS AND CONTEXT

1. Poland is located in Central Europe. It shares borders with Lithuania, Belarus, Ukraine, Slovakia, Czech Republic, Germany and Russia's Kaliningrad enclave. The capital city is Warsaw. According to the Constitution of Poland<sup>3</sup>, the official language is Polish. The official currency of Poland is the Polish złoty<sup>4</sup> (PLN). The territory of Poland is divided into 16 voivodeships (provinces); these are further divided into 314 powiats (counties or districts), 66 cities with powiats rights and 2 477 gminas (communes or municipalities)<sup>5</sup>. The total area of the country, according to the administrative division, amounts to 312 679 km<sup>2</sup> (as of 1 January 2021<sup>6</sup>), with a population of 38.1 million people.

2. The Republic of Poland is a parliamentary democratic republic. The Prime Minister is the Head of Government of a multi-party system, and the President is the Head of State and the supreme commander of the Armed Forces. The Government of Poland is the supreme body of executive power. The Government consists of a Council of Ministers headed by the Prime Minister. Legislative power is vested in both the Government and the two chambers of Parliament, the Sejm and the Senate. In light of the recent judicial reform, judicial independence is under scrutiny<sup>7</sup>. Poland's legal system is based on civil law principles.

3. Poland has been a member of the European Union since 1 May 2004 and of the Schengen area since 21 December 2007. The country is also a member of numerous international organisations, such as the Council of Europe (CoE), the Organization for Security and Co-operation in Europe (OSCE), the Organisation for Economic Co-operation and Development (OECD), the North Atlantic Treaty Organization (NATO), the United Nations (UN), the World Trade Organization (WTO), as well as the Visegrad Group (V4: Poland, Czech Republic, Hungary and Slovakia).

### 1.1. ML/TF Risks and Scoping of Higher Risk Issues

#### 1.1.1. Overview of ML/TF Risks

4. According to the most recent National Risk Assessment (NRA), conducted in 2019, Poland is exposed to medium money laundering (ML) and terrorism financing (TF) risks. The ML threat posed by predicate offences is not quantified nor ranked, but some offences are listed and analysed in separate sub-chapters, which implies that they represent a higher ML threat. Poland claims the main proceed-generating ML predicate offences to be 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. With regard to the fiscal offences, which appear to have been identified as one of the main categories of proceed-generating crimes, the most common

---

<sup>3</sup> Constitution of Poland, Article 27: "Polish shall be the official language in the Republic of Poland. This provision shall not infringe upon national minority rights resulting from ratified international agreements".

<sup>4</sup> For the purpose of this report, the exchange rate used is 1 PLN = €22 cents.

<sup>5</sup> Source: [Statistics Poland / Regional Statistics / Classification of Territorial Units / Administrative division of Poland](#)

<sup>6</sup> Source: [Statistics Poland / Basic data](#)

<sup>7</sup> Source: [GRECO \(December 2019\). Follow-up report to the addendum to the Fourth Round Evaluation Report \(Rule 34\) for Poland](#)

modi operandi are carousel fraud, missing trader fraud, fake intra-Community supplies or exports, “straw men”, and transnational VAT fraud.

5. A high risk of money laundering arises from organised criminal groups, both domestic (or with Polish membership/connections) and international.

6. The terrorist threat is assessed by the authorities to be 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; however, as confirmed in the discussions during the onsite visit, the risk of TF is perceived primarily as only a derivative of the risk of terrorism, which is considered low in Poland. 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.

### ***1.1.2. Country’s Risk Assessment & Scoping of Higher Risk Issues***

7. Poland’s first NRA was published in July 2019. Its preparation was led by the GIFI, and the NRA working group consisted of representatives of all competent AML/CFT bodies, including LEAs, supervisory authorities, and other government bodies. The findings of the NRA were discussed with representatives of the private sector prior to adoption. The risk assessment is publicly available<sup>8</sup>.

8. The project for the development of the NRA methodology was launched at the turn of 2016 and 2017, building on the experience gained through the implementation of the Preliminary National Risk Assessment conducted in co-operation with the International Monetary Fund (IMF) in 2012 and the participation in the EU Supranational Risk Assessment carried out by the European Commission since 2015. It is a combination of the risk factor assessment model<sup>9</sup> (with its output defined as the “primary” risk) and the risk scenario assessment model<sup>10</sup> (with its output defined as the “residual” risk), where the final outcome (defined as the “general” risk) is the weighted mathematical sum of the numerical outputs of the mentioned two models. For conclusions related to ML/TF, both models use the notion of probability – as a function of threat and vulnerability and the notion of risk – as a function of probability and consequences.

9. The assessment team considers that the theoretical basis of the NRA methodology is debatable in terms of robustness and coherency for several reasons. First, the formula used to calculate the probability of ML or TF by adding weighted values assigned to the threats and the vulnerabilities would produce an index – but never a probability – of the considered phenomenon. At that, the weights for such values should be equal according to the standard distribution curve (but not 40% and 60% as assigned by the methodology) unless there are

---

<sup>8</sup> [Publications - Ministry of Finance - Gov.pl website \(www.gov.pl\)](http://www.gov.pl)

<sup>9</sup> Which comprises estimates of the asset value subject to ML or being the object of TF, threats of ML/TF-related to products and services offered on the market, quantitative and qualitative information on operations of competent authorities and obligated institutions within the national AML/CTF system, relevant legal provisions and their application.

<sup>10</sup> Which comprises estimates regarding the list of *modi operandi* for ML and TF compiled on the basis of both domestic as well as foreign experiences (similar to the one developed by the European Commission).

statistical series/ empirical data reflecting the correlation between the outcomes and each of the considered variables<sup>11</sup>.

10. Similarly, adding weighted values assigned to the probability and the consequences of ML or TF would produce the index of risk, where any weights for the considered variables other than equal (specifically, 60% and 40% as assigned by the methodology) should be appropriately supported/ justified by statistical series/ empirical data. In exceptional cases, in the complete absence of such data, weights to the variables may be assigned based on expert judgment, which should stem from the findings of comprehensive analyses (as opposed to the statement that one of the variables is more or less “important” than the other). The same is true for the formula used to calculate the “general” risk as a sum of “primary” and “residual” risks (with 33.3% and 66.6% weights, respectively).

11. The work for the conduction of the NRA, mostly covering the period 2016-2019, started in 2017 by the task force established at the inter-ministerial FSC, with the preparation of relevant questionnaires addressed to cooperating units and obligated institutions to collect information. The working groups established at the FSC in the beginning of 2018 played a central role in producing the NRA report submitted for opinion to the FSC and subsequently published on the website of the Ministry of Finance on 18 July 2019.

12. The wide range of data used for the preparation of the NRA has come from financial and non-financial sectors, as well as competent regulatory, supervisory and law enforcement authorities. It appears that the current mechanism for identification and assessment of ML/TF risks in Poland involves a systemic exercise with high-level commitment and nationwide coverage, employs a sustainable structure in terms of the process, and has access to comprehensive data from public and non-public sources. The authorities confirm that the mechanism provides for regular review and update of the risk information as a cyclical exercise.

13. As to the outcome of the risk assessment, upon stating that the risk of ML/TF in Poland is at an average level (i.e. at level 2 on a 4-level scale), the conclusive section of the report speaks of the need to further enhance the national AML/CTF system by means of improving applicable legislative framework, optimizing procedures and ICT systems, as well as developing capacities of all stakeholder agencies and entities in terms of training and information exchange (see Core Issue 1.2 regarding the National AML/CFT Strategy and Action Plan).

14. The analytical value of the NRA report does not seem to be obvious. A large part of the NRA report comprises extensive references to the FATF recommendations and EU regulations, detailed provisions within the Polish legislation, general explanations on the phenomena of ML/TF with little detail and analysis of their specific implications in the context of Poland. Conclusions on the stated level of threats, vulnerabilities and consequences (and, accordingly, the scores assigned to them especially under the “primary” risk assessment model) do not stem from comprehensive analysis of the criteria defined by the NRA methodology. The NRA report lacks qualitative analysis of the available statistics on the numbers of crimes, SARs, domestic and cross-border wire transfers, inspections conducted by competent authorities specifically in terms of their interpretation within the context of the country’s exposure to ML/TF.

15. Accordingly, the product of the NRA does not appear to be a significant contribution to the identification and assessment – and subsequently to the understanding – of ML/TF risks in

---

<sup>11</sup> The probability, i.e. “the likelihood of happening” of an event, can be calculated using the formula  $P(A) = n(A)/n(S)$ , where  $P(A)$  is the probability of the event “A”,  $n(A)$  is the number of favourable outcomes, and  $n(S)$  is the total number of events in the sample space.

the country. This was confirmed during the onsite visit, where numerous competent authorities considered the NRA process a valuable exercise to enhance the general ML/TF awareness; however, they did not confirm its product to be a full and comprehensive description of the ML/TF landscape in the country.

## 1.2. Materiality

16. Poland has emerged as a dynamic market within Europe; it is the sixth-largest economy in the EU<sup>12</sup>. The country performed well during the 2014-2018 period, with the real GDP growth rate generally exceeding 3%. In 2019, Poland's economy expanded by 4.1% (as estimated by the IMF). Despite the Polish economy being among Europe's least affected by the COVID-19 pandemic, its GDP declined by 2.7% in 2020<sup>13</sup>. Poland is classified as a high-income economy by the World Bank<sup>14</sup> and ranks 21st worldwide in terms of GDP (nominal) as well as 40th in the 2020 Ease of Doing Business Index. Poland has a highly diverse economy that ranks 23rd in the 2018 Economic Complexity Index.

17. The largest and most important sectors of Poland's economy are agriculture, industry, wholesale and retail trade, transport, accommodation and food services. Intra-EU trade accounts for 80% of Poland's exports (predominantly to Germany, Czech Republic and France), while outside the EU, 3% of its exports go to both Russia and the United States. The largest part of imports (69%) come from EU Member States (predominantly from Germany, the Netherlands and Italy), while outside the EU, 8% of imports come from China and 7% from Russia. The largest contributors to GDP<sup>15</sup> in 2020 were: services (57.46%), industry (28.16%) and agriculture (2.39%).

18. Poland has the sixth largest banking population in Europe and the second highest number of banks. The country also has the sixth highest rate of banking sector employment in Europe.

19. The art market is the largest segment of the alternative investment market. The advantage of the art market is its low sensitivity to business cycles. In 2019, the value of sales of works of art and antiques amounted to PLN 162.5 million (€35.75 million) and increased by PLN 29.1 million (€6.4 million) compared to 2018. Auction houses, galleries and antique shops operate as intermediaries on the Polish art market.

## 1.3. Structural elements

20. Some of the key structural elements (high-level commitment to address AML/CFT issues; stable institutions with accountability, integrity and transparency; rule of law) necessary for an effective AML/CFT regime are present in Poland to differing extents. However, the independence and efficiency of the judicial system, as well as the political stability, raised concerns<sup>16</sup>.

21. According to the NRA, corruption is also one of the top predicate offences for ML. The Group of States against Corruption (GRECO) has on various occasions<sup>17</sup> expressed its concern

---

<sup>12</sup> Source: [Poland - The World Factbook \(cia.gov\)](https://data.cia.gov/dataset/poland)

<sup>13</sup> Source: [Poland Overview: Development news, research, data | World Bank](https://data.worldbank.org/country/pl)

<sup>14</sup> Source: [WDI - The World by Income and Region \(worldbank.org\)](https://data.worldbank.org/country/pl)

<sup>15</sup> Source: [Poland - GDP distribution across economic sectors 2020 | Statista](https://www.statista.com/statistics/1111111/poland-gdp-distribution/)

<sup>16</sup> Source: Independence of Polish judges (europa.eu)

<sup>17</sup> i.a following an Ad-Hoc Evaluation of Poland on this matter in June 2018

about the increased influence of the legislative and executive branches of power over the functioning of the judiciary, which has left judges increasingly vulnerable to political control and has critically undermined judicial independence. In its Fifth Round Evaluation Report on Poland, GRECO considered the situation similar to the Police and other law enforcement agencies. It stated that the entire chain of criminal proceedings – from investigation to adjudication – was being exposed to risks of political interference, which could ultimately undermine the effectiveness of anti-corruption efforts<sup>18</sup> (particularly in respect of persons with top executive functions).

#### 1.4. Background and Other Contextual Factors

22. Poland is reported to be one of the major amphetamine manufacturers for the European market<sup>19</sup>, where manufacturing and distribution of drugs are handled by local organised crime groups. Due to the large population, Poland also represents a big market for drugs produced both locally and imported into/ transited through the country.

23. Transparency International's corruption perception index ranks Poland 45th among 180 countries in 2020<sup>20</sup>. The perception of corruption in the public sector has been steadily increasing since 2015, when Poland held its highest rank of 29th. Significant risks of corruption have been reported in public procurements, permit issuance and the healthcare sector, among others.

##### 1.4.1. AML/CFT strategy

24. On the 19th of April 2021, Poland adopted the National AML/CFT Strategy, setting out the implementation of specific measures that build upon the findings of the NRA and aim to improve the national AML/CTF system. The implementation of strategic goals was supported by the adoption of an Action Plan based on the National AML/CFT Strategy.

25. The AML/CFT Strategy and the Action Plan set six priority areas. These are: (i) increasing the effectiveness of operations of the FIU and the cooperating units; (ii) adopting the catalogue of obligated institutions and their duties to emerging threats and information needs; (iii) harmonizing and improving the principles of supervision and control over the obligated institutions; (iv) improving information exchange procedures and the scope, quality and access to exchanged information; (v) improving the effectiveness of training programs, producing new guidelines for the FIU, obliged institutions and LEAs and implement an expert forum for all AML/CFT stakeholders; (vi) developing a methodology for the collection of statistical data enabling the effectiveness assessment of the national AML/CFT system.

26. Among national strategies and policies relevant for combating ML/TF, the authorities refer to the 2020 Efficient State Strategy with its Goal 7.2 defined to prevent and combat crime as well as threats to public safety and order; and to the 2015-2020 Program for the Preventing and Combating Economic Crime with its Tasks 6-8 defined to strengthen the coordination of interagency co-operation, prepare draft new regulation in accordance with EU requirements, and coordinate implementation of conclusions of AML assessments. In addition, a National Antiterrorist Program was adopted for 2015-2019.

---

<sup>18</sup> Source : [GRECO Fifth Evaluation Report \(28/01/2019\)](#)

<sup>19</sup> Source: [https://www.emcdda.europa.eu/countries/drug-reports/2019/poland/drug-markets\\_en](https://www.emcdda.europa.eu/countries/drug-reports/2019/poland/drug-markets_en)

<sup>20</sup> Source: <https://www.transparency.org/en/countries/poland>

#### *1.4.2. Legal & institutional framework*

##### *Institutional framework*

27. The institutional framework involves a broad range of authorities. The most relevant ones are the following:

28. The **General Inspector of Financial Information** (GIFI) is Poland's financial intelligence unit, the main coordination body responsible for AML/CFT policy in Poland. The GIFI performs its duties with the assistance of the organisational unit established for this purpose within the Ministry of Finance. The GIFI, together with the Department of Financial Information, functions as the Polish financial intelligence unit. The duties of the GIFI, among others, concentrate on activities connected with conducting the analysis of financial information provided by the obliged institutions as well as co-operation, in particular the exchange of information, with cooperating units and foreign FIUs (see Paragraphs 160-162 on the organisational setup of the FIU). GIFI is competent for the application of specific restrictive measures (i.e. TFS) and performing supervision and control of the fulfilment of AML/CFT obligations stemming from the Act.

29. The **Financial Security Committee** (FSC) is the opinion-making and advisory body in the scope of AML/CFT, which operates at the GIFI, and is created in line with the provisions of the AML/CFT Act (Chapter 3). It provides opinions on the NRA and the AML/CFT Strategy. It also issues recommendations concerning the application of specific restrictive measures and provides analyses and assessments of AML/CFT legal solutions, as well as proposals for amendments of AML/CFT provisions. The FSC is chaired by the GIFI and composed of representatives of all relevant agencies engaged in the AML/CFT system.

30. The **Ministry of Justice** (MoJ) is responsible for the preparation of projects on civil and criminal law, including provisions defining and penalizing money laundering.

31. The **Ministry of the Interior and Administration** is competent for the maintenance of public order and public security, and state border protection. It is responsible for the coordination of the mechanisms enabling governmental administration bodies to cooperate, coordinate and exchange information.

32. The **Ministry of Economic Development, Labor and Technology** is, among others, competent in the area of export control and licensing of international trade in strategic goods.

33. The **Ministry of Foreign Affairs** is responsible for coordinating the implementation of issues related to the application of international sanctions and participates in the MLA.

34. The **Police** have the general power for investigating all offences in Poland, including conducting counterterrorism activities, preparatory proceedings in cases of economic crimes and tasks related to disclosure, identification, protection and recovery of property derived from crime or related to crime.

35. The **Internal Security Agency** (ISA) has powers and competence to recognise, prevent and counteract financing of terrorism and predicate offences that may be linked to money laundering.

36. The **Central Anti-Corruption Bureau** (CBA) is a special service established to combat corruption in public and economic life, particularly in public and local government institutions, as well as to fight against activities detrimental to Poland's economic interests.

37. The **Public Prosecutor's Office** (PPO) is responsible for investigating and prosecuting ML, TF and other predicate offences. Its duties also encompass execution of the MLA requests.

38. The **Komisja Nadzoru Finansowego** (KNF) supervises the financial market in Poland, including AML/CFT area. It exercises oversight of the banking sector, the capital, insurance, pension market, supervision overpayment institutions and payment service offices, electronic money institutions and the savings and credit union sector.

39. The **Narodowy Bank Polski** (NBP) is the central bank of the Republic of Poland, which controls the fulfilment of the obligations imposed by the AML/CFT Act regarding entities operating as currency exchange offices.

40. The **National Revenue Administration** (KAS) operates in the field of collection, control and enforcement of taxes, customs duties, and other revenues of the state budget from public levies, as well as combating tax and customs crime. The heads of customs and tax control offices are empowered to exercise AML/CFT control in relation to obligated institutions controlled within their competence.

41. The **Border Guard** (BG) is responsible for the prevention, identification and prosecution of crimes and offences within its competence.

42. The following authorities are competent to control the AML/CFT compliance:

- **Presidents of Courts of Appeal** in relation to notaries;
- The **National Association of Cooperative Savings and Credit Unions** in relation to cooperative savings and credit unions;
- **Competent governors of provinces** (*wojewoda*) or **governors of districts** (*starosta*) in relation to associations;
- **Competent ministers** or **governors of districts** (*starosta*) in relation to foundations.

#### 1.4.3. Financial sector, DNFBPs and VASPs

43. An overview of the financial and non-financial sectors is provided in the table below.

**Table 1.1: Overview of financial and non-financial sector**

Reporting Entity	Number Licensed/ Registered	Assets Size (PLN billion)
<b>Financial Sector</b>		
Commercial banks (including 1 state bank and 2 affiliating banks)	30	1 780
Cooperative banks	538	150
Payment institutions	38	N/A
Small payment institutions	46	N/A
Payment service offices	1367	N/A
Representative offices of foreign banks and credit unions	8	69
Credit unions, National Association of Cooperative Savings and Credit Unions	26	9
Brokerage houses	38	68
Investment fund management	57	320

companies		
Open pension funds	10	155
Occupational pension funds	2	2
Life insurance undertakings	26	94
Non-life insurance and reinsurance undertakings (personal and property insurance)	33	100
<b>Non-Financial Sector</b>		
Casinos (land based)	51	Total revenue in 2019 PLN 5 838 million (€1 284 million)
Bet making points (bookmaking and sweepstake systems)	2 423	Total revenue in 2019 PLN 6 836 million <sup>21</sup> (€1 504 million)
Real estate agents	19 719	Contribution to GDP in 2019 PLN 110 649 million (€24 342 million) (real estate service)
Notaries	3 617	
Advocates	19 142	N/A
Legal Advisers	45 622	N/A
Foreign lawyers	104	N/A
External chartered accountants	5 620, including 2 878 practising the profession	N/A
External tax advisors	8 963	N/A
Trust and Company Service Providers	N/A	N/A
Bookkeeping services	71500	About 1.7 million companies use bookkeeping services. The estimated value of the market is approximately PLN 5 billion (€1.1 billion)
Postal operators	283	Total revenue in 2019 PLN 10.2 billion (€2.19 billion)
Foundations	28 488	Total revenue in 2018 PLN 10.2 billion (€2.19 billion)
Associations and social organisations	118 389	Total revenue in 2018 PLN 16.0 billion (€3.52 billion)

44. Banks in Poland account for approximately 75.1% of financial sector assets, which reached €6.03 billion in 2018. The vast majority of the assets are managed by commercial banks. At the end of 2018, the Polish financial landscape comprised 30 commercial banks (65%), 538 cooperative banks (5%) and 38 branches of credit institutions (3%). The Polish banking sector

<sup>21</sup> Information on the implementation of the Gambling Law (<https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/raporty/>)

was found to be dominated by foreign-controlled banks with investors from 18 different countries (in particular, Germany and Spain). However, domestic investors controlled all cooperative banks as well as 13 commercial banks.

45. The structure of assets of the Polish financial sector at the end of 2019 in general consists of domestic, commercial banks with foreign branches (65%), investment fund management companies (12%), pension funds (6%), cooperative banks (5%), non-life insurance undertakings (4%), life insurance undertakings (3%), branches of credit institutions (3%), brokerage houses (2%), credit unions (less than 1%). The bureaux de change are mostly Polish-owned and have a limited number of offices across the country per firm since they are mainly familiar businesses managed by individual entrepreneurs. The risk is not considered significant; however, they can provide services in cryptocurrencies exchange, which is the sole reason for considering them with particular care in the context of the present report (see the classification below).

46. The DNFBP sector in Poland comprises casinos (including online casinos), post office operators, legal professions, accountants, foundations and associations, real estate agents and entrepreneurs to the extent to which they accept or make cash payments for goods of the total value equal to or exceeding the equivalent of €10 000.

47. There were 283 postal operators registered in 2019, out of which 143 were active in the provision of postal services. Forty-four postal operators provided services in Poland as well as abroad. The total volume of postal services amounted to PLN 10.2 billion (€2.19 billion). The postal operators do not display particular AML/CFT risks.

48. In 2019, for 51 casinos, 30 licenses for arranging betting (including 2,423 outlets accepting betting) and 18 licenses for arranging betting via the internet were effective. Gambling game revenues reported by entities pursuing activities in the scope of gambling games in 2019 amounted to a total of PLN 22.6 billion (€4.9 billion). Casinos are considered as one of the riskiest DNFBPs.

49. As of November 2020, there were 19 142 active attorneys and 104 foreign attorneys providing legal assistance; 8 963 persons were entered in the list of tax advisers; and 45 622 registered legal advisers exercising their profession. The professions of legal advisor and tax advisor are linked to the profession of attorney. Tax advisory services include providing advice, opinions and explanations regarding tax obligations representing clients in proceedings before tax authorities and before Administrative Courts.

50. Regarding notaries, according to the data of the Ministry of Justice, as of December 2018, 3 617 notaries were appointed in Poland. The legal professions are not considered as risky from the AML/CFT perspective.

51. Regarding real estate trading, intermediaries are obligated institutions. Each entrepreneur may perform intermediation activities in real estate trading subject to holding civil liability insurance for damages caused in connection with the performance of these activities. The data of Statistics Poland (*Główny Urząd Statystyczny*) shows that as of 31 September 2020, there were 20 459 entities registered in the National Official Register of National Economy (REGON), indicating intermediation in real estate trading as their activity. According to the estimations in the NRA, the real estate sector is ranked on the fifth position in terms of risk amongst DNFBPs by the cooperating units, while the private sector does not consider them as being part of the top five risk areas. The AT has no reason to conclude that real estate agents in Poland do not present significant ML/TF risks.

52. According to information from the open sources, 15 cryptocurrency exchanges and 17 cryptocurrency bureaux de change offices offer their services on the internet in the Polish language, but some of them are operated by entities registered abroad. In 2017 the Polish Financial Supervision Authority (UKNF) asked the financial institutions supervised by them to provide detailed information on their customers that appeared to be operating as VASPs. Several virtual currency exchange offices closed their operations or moved them abroad after the UKNF sent in 2018 letters to the banks and PSPs raising awareness about the risks related to cryptocurrencies and requiring the application of EDD measures for their customers acting as VASPs.

53. There are two types of cryptocurrency entities operating in Poland: currency exchangers with physical presence, which exchange FIAT to crypto and vice-versa, and remote operators which provide a wide range of financial services enabling both the purchase and sale of cryptocurrencies, direct payments using cryptocurrencies or using payment instruments (*e.g.* payment cards or apps) via the Internet.

54. More precisely, there are 20 exchange offices allowing the purchases and sales with the physical presence of the client and three online operators (registered as PSPs) allowing the purchase of the most popular cryptocurrencies (BTC, ETH, LTC). In addition, there are three institutions offering exchange of cryptocurrencies via ATMs (called BitMats) with 112 devices spread on the territory of Poland. The sums operated through those devices are limited to: maximum €15 000 per day to be charged in the ATM by the operator and up to €1 000 transactions per customer in a given period of time (usually one week).

55. Pursuant to the Act of 1 March 2018 on Counteracting Money Laundering and Financing of Terrorism (hereinafter referred to as the AML/CFT Act), VASPs are obliged institutions. There are no market entry controls in place with regard to VASPs, which for AML/CFT purposes have been included under GIFI's supervision. In 2019 GIFI conducted a full-scope inspection of one of the largest VASPs (a crypto-currency exchange), while another inspection was carried out by the KAS.

56. Taking into consideration the number of entities providing services related to trading and exchange of cryptocurrency assets, it can be concluded that this sector plays a marginal role in the Polish financial system.

57. The assessors classified the reporting entities (REs) on the basis of their relative importance, given their respective materiality and level of ML/TF risks. The assessors used this classification to inform their conclusions throughout this report, weighting positive and negative implementation issues more heavily for most significant sectors than for less significant ones. This approach applies throughout the report but is most evident in IO.3 and IO.4:

- a) most significant: the banking sector based on the overall market share, as well as known ML/TF cases;
- b) significant: PSP, currency exchangers, casinos and VASPs based on exposure to ML/TF risks;
- c) less significant: other FIs, including insurance, and the rest of DNFBPs.

#### ***1.4.4. Preventive measures***

58. Preventative measures are set under the AML/CFT Act, which came into force on the 1st of March 2018.

59. The main preventive measures provided by the current AML/CFT legislation include the following obligations: conducting risk assessments, applying customer due diligence measures, submitting SARs, having a cash threshold report (CTR), above-threshold transaction reports, maintenance and retention of records of transactions and implementation of AML/CFT compliance program that is reflective of the reporting institutions' ML and TF risk profiles.

60. The AML/CFT Act covers the obligated institutions, including postal operators and entrepreneurs, carrying out activities consisting of making safe deposit boxes available. Furthermore, several types of obligated institutions (*inter alia*: banks, credit institutions) are required to report above-threshold transactions. This additional preventive measure has not been required by the EU legislation.

#### 1.4.5. Legal persons and arrangements

61. According to applicable laws of Poland, the following types of legal persons shall be registered in the National Court Register (NCR): (i) a registered partnership, (ii) a professional partnership, (iii) a limited partnership, (iv) a limited joint-stock partnership, (v) a limited liability company, (vi) a joint-stock company, (vii) the European Economic Interest Grouping, (viii) a *Societas Europaea*, (ix) a cooperative, (x) an association and (xi) a foundation.

62. According to statistics, at the end of 2020, there were 11 537 foundations and 7 227 associations registered in Poland. Foundations, as well as associations, are subject to mandatory entry in the register of associations maintained within the National Court Register. After entry into the register, they acquire legal personality. However, they become obliged institutions only if they accept or make payments in cash of the total value equal to or exceeding the equivalent of €10 000.

**Table 1.2: Numbers of legal persons registered in Poland as of December 2020**

Legal form	Number
Limited liability company	446 732
Joint-stock company	9 546
Professional partnership	2 426
Limited partnership	43 292
Cooperative	10 934
<i>Societas Europae</i>	8
European Economic Interest Grouping	8
Foundations	11 537
Associations	7 227

#### 1.4.6. Supervisory arrangements

63. The AML/CFT supervision framework is consolidated mainly under the AML/CFT Act. GIFI supervises all obligated institutions' compliance with AML/CFT obligations. Given the wide range of obliged institutions, GIFI's controls concentrate on institutions that do not have a prudential supervisor. The coordination of the supervisory responsibilities is done by the GIFI.

64. Under Article 130(2) of the AML/CFT Act and under the terms laid down in separate provisions, control may also be exercised: (i) by the President of NBP over currency exchange

office operators, (ii) by the UKNF over entities supervised by it, (iii) by the National Association of Cooperative Savings and Credit Union (NACSCU) over cooperative savings and credit unions, (iv) by Presidents of Appeal Courts over notaries, and (v) by heads of the KAS over the obligated institutions controlled by these bodies. The control process of those supervisory entities is conducted under the separate provisions of the separate acts, which define the method of operation, including supervisory powers.

**Table 1.3: Supervisory arrangements for financial institutions**

<b>Financial institutions</b>		
<b>Sector</b>	<b>Licensing Body (Market Entry)</b>	<b>AML/CFT Supervisor</b>
Banks	UKNF	UKNF/GIFI/KAS
Payment institutions	UKNF	UKNF/GIFI/ KAS
Payment service agents	UKNF	UKNF/GIFI
Currency exchange offices	President of NBP	President of NBP/GIFI/ KAS
Brokerage houses	UKNF	UKNF/GIFI/ KAS
Collective investments	UKNF	UKNF/ GIFI/ KAS
Investment firms	UKNF	UKNF/ GIFI/ KAS
Insurance companies or intermediaries	UKNF	UKNF/ GIFI/ KAS
E-money institutions	UKNF	UKNF/ GIFI/ KAS
Credit Unions (SKOK)	UKNF	NACSCU/UKNF/GIFI/ KAS
VASPs	N/A	GIFI

**Table 1.4: Supervisory arrangements for DNFBPs**

<b>DNFBPs</b>		
<b>Type of business</b>	<b>Licensing Body (Market Entry)</b>	<b>AML/CFT Supervisor</b>
Land-based casinos	Ministry of Finance	Ministry of Finance
Bet making points (bookmaking and sweepstake systems)	Ministry of Finance	GIFI/KAS
Real estate agents	N/A	GIFI/KAS
Notaries	Presidents of Appeal Courts	GIFI/Presidents of Appeal Courts/KAS
Lawyers	Ministry of Justice	GIFI/KAS
Foreign lawyers	Ministry of Justice	GIFI/ Presidents of Appeal Courts/ KAS

Legal advisers	Ministry of Justice	GIFI/ Presidents of Appeal Courts/ KAS
External chartered accountants	Ministry of Finance	GIFI/ KAS
External tax advisors	Ministry of Finance	GIFI/ KAS
Trust and Company Service Providers	N/A	GIFI/ KAS
Bookkeeping services	N/A	GIFI/ KAS
Postal operators	Office of Electronic Communications	GIFI/ KAS

#### ***1.4.7. International co-operation***

65. Poland has a broadly comprehensive framework for international co-operation. It provides a wide range of mutual legal assistance in all types of investigations, including AML/CFT cases. The Public Prosecutor's Office is the central authority for the receipt of MLA. The provisions on MLA enshrined in the CPC enable courts and public prosecutors to provide legal assistance upon a request of courts and public prosecutors of foreign countries. In case of the existence of an MLA Treaty or other agreement, the mutual legal assistance can be rendered directly by the Prosecution Office or a competent Court. In the absence of any MLA agreement, the Ministry of Foreign Affairs receives the request and directs it to the competent ministry.

66. Apart from regular channels of MLA, the Polish prosecutor's office cooperates with a broad range of international organisations operating on the basis of international agreements in the scope of activities undertaken to combat crime and also uses EU mechanisms, such as Eurojust and European Judicial Network.

## 2. NATIONAL AML/CFT POLICIES AND COORDINATION

### 2.1. Key Findings and Recommended Actions

#### ***Key Findings***

##### ***Immediate Outcome 1***

- a) The current mechanism for identification and assessment of ML/TF risks in Poland involves a systemic exercise with high-level commitment and nationwide coverage, employs a sustainable structure in terms of the process, and has access to comprehensive data from public and non-public sources. Nevertheless, the analytical value of the most recent NRA does not seem to be obvious, and it does not appear to be a significant contribution to the identification and assessment – and subsequently to the understanding – of ML/TF risks in the country.
- b) The authorities have limited understanding of the ML threats emanating from certain types of predicate offences, with conclusions based on statistics available on crime rates, examples of some significant cases, but not on 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. The risk of terrorism financing is perceived primarily as a derivative of the risk of terrorism, and significant further efforts are needed towards appropriate identification and reliable assessment of TF risks.
- c) Whereas the measures stipulated under the priorities of the National AML/CFT Strategy adopted in 2021 would undeniably contribute to the enhancement of the effectiveness of the national AML/CFT system, it is not obvious how these priorities reflect and address the most prevalent threats and vulnerabilities identified through the most recent NRA published in 2019.
- d) The GIFI has taken some measures consistent with the findings of the NRA (e.g. increasing staff by 20%, implementing the list of higher risk areas identified by the NRA into the initial stage of the analytical process and the prioritisation of information exchanges, etc.). Nonetheless, timing and scope of the measures taken by the LEAs and the PPO do not enable a conclusion that they have been informed by the NRA or the AML/CFT Strategy. 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.
- e) Bilateral co-operation mechanisms provided under the AML/CFT Act are adequate. 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, approve risk assessment methodologies, outcomes and actions plans, and provide guidance, but an operative coordination platform or similar arrangements are missing. Moreover, SRBs with functions relevant for AML/CTF are not represented at this (or any other) platform.
- f) Financial institutions and DNFBPs affected by the application of the AML/CFT requirements were involved in the NRA process to a certain extent, and a series

of conferences and workshops were organised to present to them the results of the NRA. Nevertheless, the private sector does not demonstrate practicable awareness of the results of national ML/TF risk assessments, while some of them consider that, regarding their exposure to ML/TF risk, the wording of the analysis in the NRA is rather general/ vague, or that the findings of the NRA are not reliable and accurate.

### ***Recommended Actions***

#### ***Immediate Outcome 1***

- a) Proper analysis should be conducted to arrive at reasonable conclusions on the country's exposure to the risk of ML/TF 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.
- b) Comprehensive assessment should be undertaken to achieve adequate understanding of all aspects of the country's exposure to the risk of TF. This would imply a change in the perception of the risk of terrorism financing, supplemented by good awareness about the actors potentially interested in infiltrating the AML/CFT system, as well as by express ability to trace potentially TF-related cash movements and transfers.
- c) Upon proper analysis and assessment of the national ML/TF risk exposure, the National AML/CFT Strategy and other AML/CFT policies (if any) should be revised to reflect and address – by means of focused and targeted actions – the most prevalent ML/TF risks in the country.
- d) Systemic approach should be introduced, and consistent action should be taken towards alignment of objectives and activities of competent authorities with national AML/CFT 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.
- e) The role of the existing national platforms should be expanded – or new platforms should be established – to introduce mechanisms for co-operation and coordination of issues related to AML/CFT (and where appropriate, to CPF) at an operative level to include, *inter alia*, regular horizontal exchange of information on risks/trends and specific cases. SRBs with functions relevant for AML/CTF should be represented at such platforms.
- f) The private sector should be provided with guidance on the implementation of the recommendations of the NRA, the introduction of specific considerations and amendments into their internal regulations based on the findings of the NRA.

67. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34 and elements of R.15.

## 2.2. Immediate Outcome 1 (Risk, Policy and Coordination)

### 2.2.1. Country's understanding of its ML/TF risks

68. The current mechanism for identification and assessment of ML/TF risks in Poland involves a systemic exercise with high-level commitment and nationwide coverage, employs a sustainable structure in terms of the process, and has access to comprehensive data from public and non-public sources. Nevertheless, as described in the introductory part of this report, the analytical value of the NRA does not seem to be obvious, and it does not appear to be a significant contribution to the identification and assessment – and subsequently to the understanding – of ML/TF risks in the country.

69. 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. All authorities met onsite speak more or less about the same types of the mentioned proceeds-generating predicate offences – in various order of priority – with conclusions that are based on statistics available on crime rates, examples of some significant cases, but not on a comprehensive view of the factual/ detected and potential/ undetected amount of the proceeds of crime generated in or passing through the country, neither by individual offences as defined by the Criminal Code, nor by categories of crimes.

70. The total amount of criminal proceeds in the country is estimated in the NRA as a percentage of GDP within the range of 1.08% to 1.27% as of 2018. This approach does not seem to be reliable mainly for the reason that the mentioned figure is not commensurate with the outcomes of the AML/CFT system in either intelligence (*e.g.* amounts identified in SARs and other alerts, FIU analytical proceedings, disseminations/ notifications to the law enforcement) or law enforcement (*e.g.* amounts involved in investigations, indictments/ prosecutions and convictions; as well as suspended/ blocked amounts, confiscations/ forfeitures) courses of action.

71. Organised crime, cross-border movements of cash and funds, 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.

72. **Organised crime** is an area where deeper insight is needed through the NRA or other nationwide efforts. While general information and case studies provided by the authorities indicate a significant presence of organised criminal groups in the perpetration and commitment of various crimes (including VAT-related fraud, drug and human trafficking, smuggling and others) through abuse of, *inter alia*, services of banks, payment operators and currency exchange bureaus, and NRA concludes that "*the threat stemming from the offences committed by these [organised criminal] groups is not decreasing*", but does not analyse the significance of this phenomenon in the criminal landscape of the country, both in terms of the most prevalent *modi operandi* used by these groups and of reliable estimates regarding the proceeds of crime factually or potentially owned/controlled by them<sup>22</sup>.

---

<sup>22</sup> There is one paragraph in the NRA stating that "according to CBSP data, in 2018, 8,030 persons (in 2017 - 7,113) operating in 880 (in 2017 - 858) organised crime groups, including 742 Polish groups (in 2017 - 735), 128 international groups (in 2017 - 113), 5 Russian-speaking groups and 5 groups composed of foreigners (the same numbers as in 2017)" and that "a considerable part of these groups dealt with drug crime, i.e. 374 (in 2017 - 336) and economic crime, i.e. 292 (in 2017 -

73. With regard to the **cross-border movements of cash**, the NRA has a section<sup>23</sup>, which provides statistics on the total volume of declared cash import into and export from the country within the considered period. The average annual indicators for 2018-2020 are around €260 million for imports and €32 million for exports. The main source and destination countries are Ukraine for incoming cash movements (accounting for more than 70% of imports) and Israel for outgoing cash movements (accounting for more than 30% of exports). Moreover, a total amount of around €6 million in non-declared cross-border movements of cash is reported for the same period.

74. In this regard, the NRA does not provide analysis and conclusions about the economic or other legitimate rationale and, subsequently, the potential of the mentioned cash movements in terms of facilitating possible ML or TF. This is important having regard to the significant number of Polish LLCs incorporated by Ukrainian nationals and the reported scheme of depositing cash on the accounts of such companies for their further transfer to other EU or third countries.

75. As a result of the weaknesses of the NRA, the authorities' understanding of risks related to cross-border cash movements is limited. For example, regarding the significant cash outflow to Israel, the explanation provided by the Border Guard (BG) was that this is done by Israeli currency traders who collect cash in different currencies, physically bring them into Poland, exchange at a favourable rate into shekels and take it back to Israel where they sell the shekels again for PLN at an advantageous rate. This explanation does not seem reasonable and confirms the need for the authorities to improve the understanding of cross-border cash movements and related ML/TF risk exposure.

76. Regarding **cross-border movement of funds** more generally, the understanding of risk is based on a document produced by the UKNF in 2018, which contains statistical data on the number and volume of incoming and outgoing wire transfers with breakdown to source and destination countries, including those considered higher risk for ML and TF. Nonetheless, the document does not analyse the underlying economic or other legitimate rationales of the respective movements of funds, at least to an extent of ascertaining that they are commensurate with external economic activities of the country and ensuring that the significant differences in some positions (e.g. the annual €330 billion difference between incoming and outgoing cross-border transfers not explained by net imports/ exports, direct foreign investments or private transfers) are not due to misusing the financial and other (e.g. real estate) sectors of the economy for layering and integration of foreign proceeds of crime.

77. Among specific predicate offences with the highest potential of generating proceeds of crime, **VAT-related fraud** is the number one crime in the country. The authorities should pursue a much more comprehensive understanding of the significance of the threat emanating from this crime, achieve a reliable estimate on the amounts of involved proceeds of crime, specify the vulnerabilities that create favourable conditions for this type of criminality, and continue taking addressed mitigation measures aimed at suppressing the respective risks<sup>24</sup>. The assessment team considers the VAT taxation system itself, the tax declaration regime, certain features of legal

---

305). Some also carried out so-called multi-criminal activities, i.e. 92 groups (2017 - 81", without any estimates any of the criminal profits generated/ owned/ controlled by such groups.

<sup>23</sup> Namely, the section "Cash circulation" within the subchapter considering the risk areas in the non-financial market

<sup>24</sup> The authorities advise that, among measures aimed at combating VAT-related fraud, certain tools have been implemented, such as introduction of Single Control File (JPK), comparison of data reported in the form of JPK\_VAT with financial flows data in the STIR system, introduction of online cash registers, establishment of the Central Register of Beneficial Owners, implementation of changes in the system of monitoring road and rail transport of goods and trade in heating fuels (SENT system), introduction of the VAT split payment mechanism.

entities are among the main vulnerabilities making the system susceptible to misuse for ML purposes.

78. Another predicate offence, which needs a far better understanding of both the significance of the threat and the scope of the vulnerabilities, is **drug trafficking**. Poland is reported to be one of the major amphetamine manufacturers for the European market<sup>25</sup>, where manufacturing and distribution of drugs are handled by local OCGs. Due to the large population, Poland also represents a big market for drugs produced both locally and imported into/ transited through the country. In this regard, the authorities should develop an understanding of the proceeds of crime, including those from the local production, to arrive at reliable estimates and take targeted action for tracing and disrupting related financial flows. This is important having regard to the very significant amounts of physically seized drugs and the non-estimated amounts that potentially remain undetected.

79. **Corruption** as a predicate offence is another subject that should be appropriately assessed and understood in Poland. Within tens of thousands of corruption offences annually detected by various LEAs, around 70 per cent is document forgery stipulated under Article 271 of the Criminal Code, almost completely related to VAT-related fraud but, when taken individually, not considered in terms of generating and laundering proceeds of crime (under the applicable provisions of the Fiscal Penal Code). As regards the remaining few thousands of detected corruption crimes, the examples presented by the authorities mostly refer to non-significant cases (with up to €20 000 in proceeds) with the involvement of medium level company management or local self-government authorities acting in detriment to private or public interests. This does not appear to be in line with the steadily increasing perception of corruption in the country since 2015<sup>26</sup>, and with the significant risks of corruption reported in public procurements, permit issuance, health care sector, etc.

80. Activities of **professional money launderers** need to be analysed and understood to a much deeper extent, especially in relation to the professions of tax and legal advisers and, more generally, individuals who are in a way or another involved in the business of company incorporation and sale, which is still significant in Poland. Meetings with the competent authorities and the private sector confirm that there is a large number of companies incorporated in Poland, currently estimated to be within the range of 50 thousand (and reportedly being three times more a few years ago), which are a product of the so-called “nests” or “incubators” incorporating dozens of companies daily for their subsequent sale to real owners, both for legal and illegal (mainly VAT-related fraud) purposes. Vulnerabilities in this area are pertinent primarily to the banking system, where additional tools should be implemented for early detection of shell companies, verification of sources of incoming funds, final destinations of outgoing transfers, identification of beneficial owners, etc. Another issue is the lack of interaction between local banks, where funds travel from an account to another with no appropriate communication between the compliance officers.

81. **“Collect” services** wherewith domestic payment institutions use bank accounts for settlement of multiple payments on behalf of unidentified customers<sup>27</sup>, **payable-through or**

---

<sup>25</sup> [https://www.emcdda.europa.eu/countries/drug-reports/2019/poland/drug-markets\\_en](https://www.emcdda.europa.eu/countries/drug-reports/2019/poland/drug-markets_en)

<sup>26</sup> As of 2021, Poland ranks 45<sup>th</sup> in the annual corruption index produced by Transparency International since its highest position of 29<sup>th</sup> in 2015 (<https://www.transparency.org/en/countries/poland>).

<sup>27</sup> The authorities advise that, among measures aimed at mitigating the risk associated with such services, they have been qualified as posing a higher risk of ML/TF, and the obliged entities have been requested to apply enhanced CDD measures with regard to the respective customers.

**nested accounts**, services offered by entities engaged in **cryptocurrency trade**<sup>28</sup> fostering anonymity and similar products or services available in the market are among the subjects that need analysis – much deeper than the descriptions provided and scores assigned under the “*residual*” risk assessment model – to assess threats and vulnerabilities specific to them in the context of Poland, so as to enable design and implementation of targeted measures aimed at the mitigation of relevant ML/TF risks.

82. With regard to the understanding of ML/TF vulnerabilities, the National AML/CFT Strategy adopted on 19 April 2021 identifies several sectors and areas as having the highest level of vulnerability. These include physical cross-border transportation of funds or other assets, telecommunications services related to mobile payments, crowdfunding, and payment services offered by entities other than banks. On the other hand, the authorities met onsite expressed various views on the most prominent ML/TF vulnerabilities in the country, some putting an equation sign between threats and vulnerabilities, others referring to certain products (e.g. virtual currencies, bearer shares, electronic money), delivery methods (e.g. non-face-to-face relationships) and *modus operandi* (e.g. physical cross-border movement of cash, use of Hawala), thus not demonstrating a uniform and comprehensive understanding of the subject matter at national level.

83. The risk of terrorism financing is perceived primarily as a derivative of the risk of terrorism, which is considered to be 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).

84. According to the NRA, until early 2019, the Internal Security Agency (ISA) identified certain methods of raising funds in Poland for supporting terrorist organisations, such as income from work (legal and illegal), financial support from family members, collections under the guise of charity support (including online), collections conducted on behalf of a terrorist organisation (voluntary and forced), and proceeds from criminal activities (smuggling, fraud, extortion, etc.). Moreover, the ISA has also identified cases of investment in real estate by members and supporters of terrorist groups in Poland.

85. Nonetheless, further discussions on these topics during the onsite did not give a comprehensive view of the intelligence work, which enabled identification of the mentioned methods of and actors in TF, nor did they provide the vision of competent authorities regarding the current situation with the use of the same or different methods by any actors, as well as regarding factual and potential risk of TF unrelated to the perception of the low risk of terrorism in the country. With regard to the presence of Hawala networks, which are popular among certain immigrant communities and national minorities, competent authorities report difficulties in terms of estimating the total turnover in such networks, identifying the persons handling them, locating the directions and purposes of the transfers within the networks. All of these are factors necessitating further efforts towards appropriate identification and reliable assessment of TF risks.

---

<sup>28</sup> The authorities advise that since July 2018, virtual currency service providers are subject to AML/CFT regulations and are therefore required to apply CDD measures.

### 2.2.2. National policies to address identified ML/TF risks

86. After publication of the NRA on 18 July 2019, the authorities developed and adopted the National AML/CFT Strategy, including its Action Plan, on 19 April 2021, setting out the implementation of specific measures that build on the findings of the NRA and pursue improvement of the national AML/CFT system. The National AML/CFT Strategy and Action Plan define six priorities for the way forward, particularly providing for:

- *Increasing the effectiveness of operation of the FIU and the cooperating units* – the measures specified under this priority include optimizing operational analysis (by increasing staff and automating analytical processes); updating analysis and information exchange procedures within the GIFI; preparing a plan for the development of strategic analyses; and assessing financial, human and technical resources of the cooperating units vis-à-vis their tasks in AML/CFT;
- *Adapting the catalogue of the obligated institutions and their duties to emerging threats and information needs* – the measures specified under this priority include supplementing the catalogue of the obligated institutions involving crowdfunding service providers; analysing the feasibility of introducing a threshold for cash transactions; and updating the regulations regarding virtual currencies;
- *Harmonising and improving the principles of supervision and control over the obligated institutions* – the measures specified under this priority include reviewing legal provisions on associations and foundations; developing tools for identification and supervision of entities not subject to registration/ licensing requirements; amending provisions on sector-specific supervision of DNFBPs; introducing provisions on off-site supervision carried out by the GIFI; and amending the legislation to provide for supervision of online currency exchange activities;
- *Optimising the procedure for information exchange and the scope and quality of exchanged information, as well as access to information* – the measures specified under this priority include implementing the Directive (EU) 2019/1153 on the use of financial information; enabling full functionality of the Financial Information System; completing implementation of electronic document templates stipulated by the AML/CFT Act; improving the GIFI access to the databases of cooperating units; improving capacities and use of the GIFI ICT system for information exchange; and proposing amendments to the provisions on the exchange of customer information between obligated institutions, LEAs, supervisors and the GIFI;
- *Organising an effective system for training and for exchange of knowledge and experience* – the measures specified under this priority include developing training programs and producing guidelines for the GIFI, obliged institutions and LEAs; and proposing the development of an expert forum for all stakeholders in the national AML/CFT system;
- *Defining uniform rules for generating statistical data needed to evaluate the effectiveness of the national AML/CFT system* – the measures specified under this priority include developing a methodology for the collection of statistical data enabling assessment of the effectiveness of the national AML/CFT system.

87. All 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 obvious how these priorities reflect and address – by means of focused and targeted actions – the most prevalent threats and vulnerabilities identified through

the NRA<sup>29</sup> and, 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.

88. This first of all relates to the risks emanating from cross-border movements of cash and funds, organised crime, specific, prevalent predicate offences such as VAT-related fraud, drug trafficking and corruption, activities of TCSPs and individuals potentially acting as professional money launderers, Polish shell companies, “collect” services, payable-through accounts, etc. The National AML/CFT Strategy would also need to be updated to incorporate, *inter alia*, analytical feeds on newly emerged risk trends and patterns, regarding the significant time lapse between the publication of the NRA report in 2019 and the adoption of the strategy in 2021.

89. Among national strategies and policies relevant for combating ML/TF, the authorities refer to the 2020 Efficient State Strategy with its Goal 7.2 defined to prevent and combat crime as well as threats to public safety and order; and to the 2015-2020 Program for the Preventing and Combating Economic Crime with its Tasks 6-8 defined to strengthen the coordination of interagency co-operation, prepare draft new regulation in accordance with EU requirements, and coordinate implementation of conclusions of AML assessments. Reference is also made to the 2015-2019 National Antiterrorist Program dealing with the threats of terrorism. Obviously, the above-mentioned documents adopted in 2014-2015 and, subsequently, the activities of competent authorities within their framework do not amount to established practices of developing and implementing national policies to address ML/TF risks identified through national risk assessments, particularly the most recent NRA of 2019, or similar exercises.

90. In terms of monitoring implementation of the current and any future national AML/CFT strategies, it would be beneficial to utilize a mechanism that, in addition to collecting information on the implementation of the measures stipulated by such strategies (as required under Article 32 of the AML/CFT Act), would also use that information to assess the effectiveness of implemented measures so as to revisit, when necessary, the actions, milestones and deadlines established for those measures, and to provide for identification and assessment of undetected/newly emerging risks. The authorities advise that such a mechanism is available under Article 19(2) of the AML/CFT Act, which defines the task of the FSC to perform reviews of the implementation progress of the national AML/CFT strategy. Nonetheless, the assessment team has not been provided information on the (documented) outcomes of the FSC practical work performed so far in that direction.

### ***2.2.3. Exemptions, enhanced and simplified measures***

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

92. Obligated institutions are required to apply enhanced CDD measures in cases when a higher risk of ML or TF is present, with specific examples of possible higher risk scenarios set out under Article 43 of the AML/CTF Act. These examples, in essence, are a replication of the non-

---

<sup>29</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.)

exhaustive list of factors and types of evidence of potentially higher risk set out in Annex III of the Directive (EU) 2015/849, thus unrelated to the findings of the NRA. Further requirements on enhanced CDD measures are set forth under Articles 44-46 of the AML/CFT Act in relation to higher risk third countries, cross-border correspondent relationships and PEPs, with no interconnection or interplay with the results of the NRA. At that, there is no requirement for obligated institutions to take into account the higher risks identified by the NRA or to incorporate information on those risks into their risk assessments.

93. The assessment team has not been provided with any examples on the use of risk assessment outcomes as a basis to justify/ allow exemptions for lower-risk scenarios, support/ require enhanced measures for higher-risk scenarios, or consider waivers of application of certain measures/ requirements based on risk assessments. The authorities advise that work on the NRA and the resulting risk assessment of insurance contracts was the basis for the adoption of the provision in Article 42 of the AML/CFT Act establishing that a lower risk of ML/TF may be evidenced when concluding an insurance contract where the annual premium does not exceed the equivalent of €1 500 or the single premium does not exceed €3 500. Nonetheless, there is no analysis in the NRA regarding the issue of insurance contracts, and the respective provision of the AML/CFT Law has been introduced (1 March 2018) well before the adoption of the NRA (18 July 2019).

#### *2.2.4. Objectives and activities of competent authorities*

94. The assessment team has been provided general information on some measures taken by competent authorities to improve tax administration and combat fiscal crimes (considering that these are the most frequently identified predicate offences for money laundering), to warn the private sector of the risks related to cryptocurrencies, and to improve the practices of detecting and securing the proceeds of crime. Overall, the timing and scope of these measures do not enable a conclusion that they have been informed by the NRA published in 2019 or the National AML/CFT Strategy adopted in 2021.

95. Among such measures, KAS was established under the Ministry of Finance by merging tax administration, fiscal control and customs service in 2017. Over the last 3-4 years, legislation has been drafted to counteract aggressive tax optimization techniques and reduce the VAT gap, the Standard Audit File for TAX (SAF-T) was put in place, the STIR system of the National Clearing House (NCH) was introduced to curb the possibilities of misusing the financial sector for tax fraud, the mechanism of VAT split payment and the online cash register was implemented to control and monitor ongoing taxpayer sales.

96. The GIFI, the UKNF and the NBP published communications on risks related to virtual currency trading. In November 2017, the UKNF sent a request to the banks asking for information on accounts opened by their customers for cryptocurrency exchanges. The responses indicated that such accounts were maintained by both commercial and cooperative banks. Further communication caused termination of business relationships with cryptocurrency exchanges in some cases, while the amendments to the AML/CFT Act made cryptocurrency exchange or bureaux de change obligated institutions.

97. GIFI implemented the list of higher risk areas identified in the NRA into the initial stage of the analytical process, as well as into the prioritisation of incoming requests and spontaneous disclosures from foreign FIUs. The list was also integrated into the electronic form for submission of structured SARs and responses to the GIFI requests by obliged institutions. Between 2019 and

2021, the GIFI increased the staff of analytical and control units by approximately 20%, creating a unit to deal with the increasing volume of requests and spontaneous disclosures from foreign counterparts.

98. The assessment team has not been provided information on objectives and activities of law enforcement agencies, as well as the Public Prosecutor's Office (PPO), specifically building on the findings of the NRA or other risk assessments and aimed at mitigating ML/TF risks identified by such assessments.

99. Whereas the above examples indicate measures taken by the authorities that are in line with the recently adopted National AML/CFT Strategy and relevant for mitigating the ML/TF risks in the country, it appears that 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, 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.

100. Given the fact that the National AML/CFT Strategy and Action Plan were adopted one month before the onsite visit, it is premature to make conclusions as to whether its implementation would result in focused action of the competent authorities consistent with identified ML/TF risks towards better intelligence output and guidance by the GIFI, improved practices of combating major domestic and foreign ML/TF threats by the LEAs, and more effective supervision of obligated institutions' compliance with the AML/CFT requirements by the supervisors.

#### *2.2.5. National coordination and co-operation*

101. With regard to national coordination and co-operation mechanisms available in Poland, there are two platforms<sup>30</sup> considering issues related to AML/CTF. 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.

102. The first platform 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/CFT 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.

103. The mentioned platforms with representatives of the GIFI, law enforcement authorities and other public administration bodies meet regularly. The authorities advise that the first

---

<sup>30</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.

platform has a primary say in matters related to the national AML/CFT system, whereas the second one is more focused on the threats of terrorism, while TF is mostly considered as a “by-product” of terrorism rather than a separate phenomenon to be identified and prevented in the broader context of CTF. In terms of accessibility of information at the national level, an important role is played by the NCR and KCIK<sup>31</sup>, where criminal information is collected and through which additional information can be obtained from other entities bound to submit information to these databases.

104. According to the regulations of the FSC, it meets at least three times annually, adopts decisions through resolutions by simple majority voting (with a justification for each resolution), and produces minutes of its meetings that are endorsed by the FSC. In 2018-2019, the primary task of the Committee was preparation of the NRA. In January 2019, a working group was created within the FSC to finalize the works of the NRA and to produce the NRA report. In the same year, the FSC considered proposals of the Central Anti-Corruption Bureau (CBA) on changes to the relevant regulations enabling access to information on holders of securities, the issue of whether all deficiencies of the national AML/CFT system should be disclosed in the publicly available version of the NRA, and the amendments proposed to the AML/CFT Act to ensure compliance with the Directive (EU) 2015/849.

105. 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, approve risk assessment methodologies, outcomes and actions plans, and provide guidance on policy implementation and follow-up. The assessment team considers that the role of the FSC could be beneficially expanded by introducing mechanisms – both in terms of relevant structures (e.g. working groups within the FSC) and tools (e.g. methodologies, guidelines, etc.) – to coordinate implementation of other tasks, such as collection of statistical data necessary for assessing the effectiveness of the national AML/CFT system (which is now a task assigned to the GIFI under the National AML/CFT Strategy and Action Plan), conduction of topical/ad hoc strategic analyses other than the NRA, arrangement of regular horizontal exchange of information on risks/trends and specific cases, etc.

106. Bilateral co-operation mechanisms provided under the AML/CFT Act, such as notifications from the Public Prosecutor’s Office to the GIFI with regard to decisions on blocking accounts, suspending transactions, initiating proceedings or taking other criminal procedure measures (as stipulated under Article 81), or exchange of AML/CFT-related information between the GIFI and the LEAs (as stipulated under Articles 103-106) are adequate. Nevertheless, the assessment team considers that multilateral co-operation and coordination mechanisms aimed at harmonization of efforts by all competent authorities (and SRBs, as necessary), also in terms of access to information, implementation of joint initiatives at an operational level, and provision of routine feedback on joint actions/ specific cases should be developed to achieve better results in combating ML/TF.

107. The authorities also advise that Poland participates in the Proliferation Security Initiative<sup>32</sup> launched in 2003, considering this platform as a tool to enhance international efforts to counteract the proliferation of WMD. This, however, does not amount to a national platform for the coordination and co-operation of issues related to CPF.

---

<sup>31</sup> The National Criminal Register and the National Consulting and Intervention Center for the Victims of Trafficking

<sup>32</sup> <https://www.state.gov/about-the-proliferation-security-initiative/>

### *2.2.6. Private sector's awareness of risks*

108. Financial institutions and DNFBPs affected by the application of the AML/CFT requirements were involved in the NRA process to a certain extent by way of responding to questionnaires on their perception of ML/TF risks in the country. From among more than 260 questionnaires circulated to the private sector and competent authorities, around 32% of responses came from the private sector, mainly from banks (around 70%), as well as from cooperative savings, credit unions and notaries. This helped identify the products and services in the market, which are perceived to be most vulnerable to misuse for ML/TF purposes.

109. Shortly after obtaining the positive opinion of the FSC on the NRA, it was published on the website of the Ministry of Finance on 18 July 2019. Thereafter, the GIFI organised a series of conferences and workshops for the representatives of financial and non-financial sectors to present the results of the NRA; their unions and associations received letters regarding the NRA publication. Following the publication of the NRA, the UKNF required financial institutions under its supervision to conduct a review of their enterprise-wide risk assessments to bring them in line with the NRA and indicated that this would be verified during onsite visits. The authorities advise that the availability of such assessments and their consistency with the NRA is also verified by the audit function of the obligated institutions.

110. Banks met onsite advised that they would take into account the higher risks identified by the NRA and incorporate information on those risks into their own risk management/mitigation policies and procedures. Nonetheless, they did not provide much detail on how exactly the recommendations of the NRA were implemented or what were the specific considerations and amendments introduced into their internal regulations after the publication of the NRA. Some of the DNFBPs (e.g. notaries) considered that the wording of the analysis in the NRA regarding their exposure to ML/TF risk is rather general/ vague to enable conclusions as to what should be revised in their internal regulations, while others (e.g. casinos) were of the opinion that the findings of the NRA regarding the risk exposure of their activities were not reliable and accurate.

111. With regard to the provision of guidance on risks identified by the NRA, the authorities and the private sector did not advise of specific guidance in the form of STR indicators, red flags, ML/TF typologies and trends particularly developed on the basis of the findings of the NRA and communicated to the obligated institutions for improving awareness of the NRA outcomes.

#### ***Weighting and conclusion***

112. The current mechanism for identification and assessment of ML/TF risks in Poland involves a systemic exercise with high-level commitment, nation-wide coverage, appropriate structure and data access; however, the product of the NRA misses some important constituents to make it a significant contribution to the understanding of ML/TF risk. The authorities have certain understanding of the ML threats emanating from certain types of predicate offences, and the views of individual authorities on ML/TF vulnerabilities generally concur with the NRA findings; however, significant further efforts are needed towards achieving a comprehensive view of the factual/ detected and potential/ undetected amount of the proceeds of crime, uniform understanding of ML/TF vulnerabilities, as well as appropriate identification and reliable assessment of TF risks. The National AML/CFT Strategy sets out specific measures pursuing improvement of the national AML/CTF system; however, it was adopted too shortly before the onsite visit to show tangible results in practice; 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. The private sector has been involved in the NRA process to a certain extent and is generally aware of its outcomes; nevertheless, individual obliged entities do not demonstrate practicable awareness of the results of national ML/TF risk assessments through, *inter alia*, implementing the recommendations of the NRA or introducing relevant amendments into their internal regulations based on the outcomes of the NRA. The IO is achieved to some extent, and major improvements are needed in terms of risk understanding and strategic mitigation measures.

***Overall conclusions on IO.1***

**113. Poland is rated as having a Moderate level of effectiveness for IO.1.**

### 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

#### 3.1. Key Findings and Recommended Actions

##### **Key Findings**

##### **Immediate Outcome 6**

- a) 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. Nevertheless, a significant part of the GIFI resources is used for purposes that, while serving the general interests of the state in combating economic and other crime, are not focused on initiating and furthering ML/TF investigations to trace and confiscate criminal proceeds generated in or passing through the country.
- b) Typologies reported in SARs are generally commensurate with the landscape of prevalent proceeds-generating crimes in the country, but improvements are needed in terms of specific higher risk predicate offences (e.g. corruption). SAR reporting is not consistent with the risk profile of certain sectors (e.g. payment service providers, currency exchange operators and VASPs) and individual players (e.g. particular banks).
- c) Availability of the reporting regime under Article 74 of the AML/CFT Act for lower-level suspicions may (indirectly) stimulate defensive reporting practices, as well as serve to justify the lack of more decisive action by obligated institutions in circumstances potentially related to ML. The GIFI does not have sufficient mechanisms for the provision of general and specific feedback to the obligated institutions on, *inter alia*, their SAR reporting performance.
- d) The GIFI has the necessary infrastructure, including physical and IT security measures, for safe receipt and storage of all reports and other disclosures. 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 conclusions.
- e) Prioritisation of SARs and related analytical proceedings within the GIFI is not sufficiently standardised to ensure mandatory consideration of all relevant descriptors of relative significance, which may adversely affect the selection of cases to be analyzed. Moreover, 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.
- f) There are appropriate legal bases and extensive practice of co-operation between competent authorities to exchange financial intelligence and other information through disseminations and responses to requests on suspicions related to ML, TF and predicate offences. Nonetheless, the lack of effective follow-up mechanisms impedes objective assessment and, subsequently, improvement of the effectiveness of co-operation between competent

authorities, as the available mechanism covers only a small segment of the value chain generated within the AML/CFT system.

***Immediate Outcome 7***

- a) The country has a broad range of LEAs, but none are designated with specific responsibility to investigate ML. Each LEA has the competence to investigate ML in connection to predicate offences, and the competences regarding the latter are non-exclusive, resulting in overlapping and dispersed responsibilities. LEAs' practice is almost entirely focused on the predicate offences with no due attention to the identification of proceeds and the associated ML activities. Overall, the contribution made by the LEAs to ML identification and investigations is disproportionate to the important role that they are required to play with respect to major proceeds generating crimes. Subsequently, there is a mismatch between the number of ML investigations and the number of investigations and convictions of proceeds generating predicate offences.
- b) Half of ML investigations are initiated based on the GIFI notifications, which, however, do not contribute proportionally to ML indictments and convictions. The indictments and convictions in such cases are less successful than in ML cases initiated based on other sources, which raises concerns with regard to the capacity of the authorities to investigate complex ML cases when the link to the predicate criminality is less obvious.
- c) The authorities have demonstrated a low level of proactiveness concerning ML investigations related to cross-border cash, which constitutes a major risk for the country, and have put to limited use the information on ML suspicions included in the MLA incoming requests, despite the inherent geographic ML/TF risk.
- d) The overarching role of the PPO in conducting ML investigations appears to be limited by the fact that the operational activities of the LEAs are not under prosecutorial supervision and by the special unsupervised tax-related crime investigations conducted by the KAS independently. As a result, potential ML is not detected and investigated in all relevant circumstances.
- e) LEAs lack a comprehensive perception of the relevance of parallel financial investigations, which is mirrored by the number of ML investigations achieved when comparing the number of proceeds generating predicate crimes being investigated with the number of cases where money laundering was additionally investigated. No detailed and meaningful guidelines are available for LEAs and PPO on ML investigations which would ensure the quality and the uniform approach towards ML cases among the wide range of LEAs, including through parallel financial investigations.
- f) ML investigations and prosecutions reflect, to some extent, the risk profile that the country faces, mostly in relation to tax and fraud crimes. ML cases investigated and prosecuted do not adequately reflect the cross-border cash transfer's risk.

- g) The authorities have demonstrated effective results in the prosecution of ML in self-laundering ML cases and, to some extent, third-party ML cases. As to stand-alone and foreign predicate offences connected ML cases, a positive trend can be noticed, but the numbers remain behind the ones achieved for self-laundering. This may be attributed to the high evidentiary standard applied in relation to the underlying predicate offence; uncertainty as to the evidentiary requirements in proving stand-alone ML; the general lack of specialised experts in conducting parallel financial investigations (all authorities); the limited expertise in conducting criminal investigations, impacting the quality of the presented evidence before the court (KAS).
- h) The penalties in ML cases have gradually increased, and the range of sentences included more custodial prison sentences instead of fines. Nevertheless, they often remain in the lower range of punishment which is not fully dissuasive. While legal entities are said to be frequently used as a vehicle for ML and the main predicate crimes, in practice, the criminal liability of a legal person is not enforced, and no legal persons have been convicted for ML.
- i) No examples/ statistics have been provided on the criminal justice measures applied in cases where, due to justifiable reasons, it was not possible to secure an ML conviction.

***Immediate Outcome 8***

- a) The legal framework was enhanced, but some of the measures still have a discretionary character (confiscation of instrumentalities), while other provisions fall short of the standard (inability to confiscate all types of property, i.e. intangible assets).
- b) Although LEAs 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 comprehensive statistics on the seized, confiscated and recovered property, which impacts the ability of the Polish authorities to assess the effectiveness of their own system strategically. The new AML/CFT Strategy (2021) does not envisage any priority related to the confiscation regime.
- c) The number of decisions on the seizure of property and the value of the seized property has significantly increased in 2019, compared to the previous years. This illustrates the efforts of the authorities to seize ill-gotten assets. However, these figures are extremely low when compared to the estimated proceeds of crime laundered in Poland.
- d) LEAs could not demonstrate a comprehensive perception of the relevance of parallel financial investigations. In 2019 the National Assets Recovery Office (ARO) was established, but in practice, ARO's activity seems to focus more on facilitating international co-operation and communication with various networks and foreign counterparts.
- e) The effective implementation of the cross-border cash control regime in the non-EU borders has resulted in convictions for fiscal crimes and related fines for undeclared cash. Still, the regime has not demonstrated its effectiveness for

detecting ML/TF-related cash/BNIs. In cases of detected false or non-declaration, the restrained assets concern only the equivalent value of the fine for the fiscal crime and the remaining assets are returned, even in cases of suspicions of ML.

- f) There is no single mechanism for asset recovery/managing/disposing of property and no centralised authority in charge of management of such property, which impacts the effectiveness.

### ***Recommended Actions***

#### ***Immediate Outcome 6***

- a) The GIFI should revisit its resource distribution arrangements to consider whether there is need for reallocation of resources towards activities and tasks directly relevant for AML/CFT; recipients of the GIFI communications should expressly and effectively focus on initiating and furthering ML/TF investigations to trace and confiscate criminal proceeds generated in or passing through the country.
- b) 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. The authorities should act more proactively, applying both supervisory tools of the KNF and analytical efforts of the GIFI, to timely identify low performers in SAR reporting and to take remedial action.
- c) A well-established mechanism is needed – at least for the most important players in the market – to regularly receive, from the GIFI and the supervisors, analyses and conclusions on matters that have key importance in terms of effective implementation of the AML/CFT requirements including, but not limited to, SAR reporting.
- d) The GIFI should further develop and implement a comprehensive set of criteria for prioritisation of SARs and related analytical proceedings, thus also lowering the level of subjectivity related to personal decisions of the management. 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.
- e) A comprehensive follow-up mechanism is to be implemented to provide for regular stocktaking of all information exchanges between the GIFI and the cooperating units. Such mechanism should comprise tools for general and specific feedback on the use of information exchanges both on a regular and ad hoc basis.

#### ***Immediate Outcome 7***

- a) Enhance and formalise the rules for conducting operational activities so that the LEAs properly and proactively consider ML suspicions of major proceeds generating crime even in the pre-investigative stage of proceedings. The PPO

should also analyse the bottlenecks in the criminal procedure that lead to the identified disproportionalities between high-risk predicate offences and ML investigations.

- b) Establish a mechanism to ensure that the cases subject to KAS independent investigation and prosecution in fiscal penal misdemeanours are scrutinized from the point of view of ML and are referred to the PPO for investigation if connected to major proceed generating crimes (e.g. tax fraud).
- c) Specific guidelines on identifying and investigating ML should be developed for the LEAs, including types of ML, specificities for various predicate offences, typologies, professional ML etc. The guidance should be supported with systematic training programs for the LEA officers working on cases of proceeds generating offences.
- d) The PPO should adopt a coherent practice to task selected units of LEAs with ML investigations that have the appropriate knowledge, experience, and resources.
- e) The PPO should bring more ML indictments to the courts in a broader range of proceed generating crimes to develop the jurisprudence on third-party and stand-alone ML and the required level of proof concerning the predicate offences. Prosecutors should consider separating the ML aspect and continue the investigation thereof even after indicting the predicate offence.
- f) Align the ML offence's disposition in the Penal Code with the structure of the Vienna and Palermo Convention's ML definition.
- g) Poland should take steps to enhance the dissuasiveness of sentences and address the lack of ML investigations and convictions against legal persons.

#### ***Immediate Outcome 8***

- a) The authorities should take urgent action (*i.a.*, 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.
- b) Poland should establish a reliable, comprehensive and coherent statistical data gathering regime on seizures, confiscations and asset recovery measures across the whole criminal procedure, including all actors. This will enable the authorities to measure and demonstrate the effectiveness and to take strategic decisions.
- c) The LEAs should continue to expand and reinforce their operational asset tracing and asset recovery capacities (including through training, use of accounting/financial experts and methodological tools) to be able to support and follow up the major proceeds generating crime investigations with in-depth parallel financial investigation.
- d) The current practice concerning undeclared cash and applied fines needs to be reconsidered and brought in line with the threats and vulnerabilities identified in the NRA, as well as scrutinizing ML/TF suspicions.
- e) Poland should establish a coherent system for the handling and management of secured assets as well as the enforcement of confiscation orders.

- f) Amend the general rules on confiscation in the Criminal Code in order to expressly cover the confiscation of laundered property, of any type of assets, including intangible assets, and make confiscation of instrumentalities mandatory.

114. The relevant IOs considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8,9,15,30,31,34,37,38,39 and 40.

## 3.2. Immediate Outcome 6 (Financial Intelligence ML/TF)

### 3.2.1. Use of financial intelligence and other information

#### *Access to information*

115. The GIFI is a key source of financial intelligence and other relevant information in Poland. It has access to a wide range of domestic information sources under Articles 72, 74, 86 and other provisions of the AML/CFT Act; this includes SARs<sup>33</sup> and TTRs<sup>34</sup>, tax and customs databases<sup>35</sup>, land and property registers, company and beneficial owner registers<sup>36</sup>, cross-border cash declarations<sup>37</sup>, criminal records, dedicated databases (e.g. World Check), as well as foreign intelligence provided by counterpart FIUs spontaneously and upon request.

116. The GIFI is empowered to request from obligated institutions additional information without any restrictions (e.g. no need for a prior SAR), set deadlines for the response based on urgency and complexity of the request, and require submission of information in parts where necessary. Accessing information held by obligated institutions is part of the GIFI's routine activities with appropriate legal empowerment and practical implementation; therefore, no separate statistics are kept or presented on that feature of its access to information.

117. 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. A special form has been developed to facilitate request-based information exchanges between the GIFI and the cooperating units.

118. The primary method of making financial intelligence available to the competent authorities is the GIFI notification under either Article 103 (notifying ML/TF-related suspicions to the PPO) or Article 106 (notifying non-ML/TF-related suspicions to other competent

---

<sup>33</sup> Here and hereinafter, the abbreviation "SAR" refers to suspicious activity reports and/ or suspicious transaction reports.

<sup>34</sup> Here and hereinafter, the abbreviation "TTR" refers to the reports on transactions above the applicable threshold (€15 000)

<sup>35</sup> Including general taxpayers register, VAT taxpayers register, list of entities removed from VAT taxpayers register, data from Standard Audit Files for Tax, information on conducted tax audits

<sup>36</sup> Including the National Court Register (NCR), the National Official Register of National Economy (REGON) and the Central Register and Information on Business Activity (CEIDG)

<sup>37</sup> Data is submitted through the electronic communication channel directly to the ICT system of the GIFI.

authorities) of the AML/CFT Act. In case of communication with the PPO, the GIFI differentiates between “*main*” notifications as the original alert sent to it and “*supplementary*” notifications as the additions to the original alert communicating further outcomes of the GIFI analysis (e.g. information requested from obligated institutions or obtained from foreign FIUs). The tables below present statistics on the GIFI disseminations to the PPO and other competent authorities over the period 2016-2020 (excluding the responses to the requests from the PPO and other competent authorities, which are analysed separately):

**Table 3.1: GIFI notifications to cooperating units**

Cooperating unit	2016	2017	2018	2019	2020
<b><i>Under Article 103 of the AML/CFT Act (suspicions of ML/TF)</i></b>					
Public Prosecutor’s Office (PPO), including	402	340	436	578	675
“ <i>Main</i> ” notifications	202	171	184	320	378
“ <i>Supplementary</i> ” notifications	200	169	252	258	297
<b><i>Under Article 106 of the AML/CFT Act (suspicions of predicate offences)</i></b>					
All other cooperating units	644	566	615	276	249
<b>Total 1 (Article 103 (“main”) and Article 106)</b>	<b>846</b>	<b>737</b>	<b>799</b>	<b>596</b>	<b>627</b>
Ratio, Article 103 (“main”) to Total 1	24%	23%	23%	54%	60%
<b>Total 2 (Article 103 (all) and Article 106)</b>	<b>1 046</b>	<b>906</b>	<b>1 051</b>	<b>854</b>	<b>924</b>
Ratio, Article 103 (all) to Total 2	38%	38%	41%	68%	73%

119. Overall, on average, 49%<sup>38</sup> to 65%<sup>39</sup> of the GIFI notifications to the cooperating units within the considered period is unrelated to ML/TF suspicions and pursues mostly investigation and prosecution of predicate offences, which rarely involve consideration of ML/TF. This is confirmed by the statistics on the use of financial intelligence by the competent authorities, as shown in Tables 3.3-3.7 below. Whereas the share of ML/TF-related notifications to the PPO has significantly increased over time (from 24% to 60% counting “*main*” notifications, or from 38% to 73% counting all notifications), this means that with consideration of the responses to the requests received from the cooperating units as analysed further below this section, a significant part of the GIFI resources is still used for purposes that, while serving general interests of the state in combating economic and other crime, are not focused on initiating and furthering ML/TF investigations to trace and confiscate criminal proceeds generated in or passing through the country. This is specifically important given the high level of threats emanating from specific types of criminality, such as VAT-related fraud, drug trafficking, corruption etc. (see the details in the analysis for IO.1).

120. Another method for the competent authorities to access financial intelligence is provided under Article 104 (for the PPO and the courts) and Article 105 (for other competent authorities) of the AML/CFT Act. Through this method, in addition to various sources of information available

<sup>38</sup> Counting all notifications to the PPO

<sup>39</sup> Counting “*main*” notifications to the PPO

under respective sectorial laws (e.g. the Police Act, the Anti-Corruption Bureau Act, etc.), all law enforcement agencies<sup>40</sup>, as well as the PPO, the KAS, the UKNF, the Supreme Audit Office (NIK) and the courts may obtain from the GIFI information based “on a written and justified request” made in the scope of the statutory duties and competences of the mentioned bodies and agencies.

121. In particular substantiated cases, the GIFI may refuse to make information available to the requesting agencies if that could negatively affect its analysis or expose a natural or legal person to disproportionate damage. The authorities advise that the single occasions of the GIFI refusal to provide information (2-3 cases over the period 2016-2020) were technical in nature, e.g. related to the absence of subject names, the period to be covered, the role of a particular subject etc.

122. The table below presents statistics on the requests to the GIFI by cooperating units over the period 2016-2020 and on the responses to such requests:

**Table 3.2: Requests to GIFI by cooperating units under Articles 104-105, and responses to such requests**

Cooperating unit	2016	2017	2018	2019	2020
Public Prosecutor’s Office (PPO)	597	747	737	732	844
National Revenue Administration (KAS)	1 405	834	575	428	317
Police (incl. PCBI)	145	109	108	126	159
Internal Security Agency (ISA) (incl. CTC-ISA)	54	40	72	81	86
Central Anti-Corruption Bureau (CBA)	26	31	27	104	84
Border Guard (BG)	27	29	16	21	36
Military Police	-	-	-	5	15
Military Counterintelligence Service (SKW)	-	4	49	53	37
Courts	1	6	8	9	7
Minister of Finance (supervisor for gambling)	-	-	12	33	33
Komisja Nadzoru Finansowego (KNF)	-	-	1	18	13
<b>Total, requests from cooperating units</b>	<b>2 255</b>	<b>1 800</b>	<b>1 605</b>	<b>1 610</b>	<b>1 631</b>
<b>Total, responses to cooperating units</b>	<b>1 561</b>	<b>963</b>	<b>630</b>	<b>248</b>	<b>247</b>

123. As in the case with the GIFI notifications to the cooperating units, on average, 59% of the requests to the GIFI within the considered period come from the cooperating units other than the PPO and do not focus on investigation and prosecution of ML/TF. The authorities advise that responses to the requests from the cooperating units do not trigger full-scope analytical proceedings and are produced by a dedicated unit responsible for domestic co-operation through a simplified analysis process (see further details in “Table 3.18: Outcomes of GIFI analyses”). In

<sup>40</sup> Including the Police, the Military Police, the Border Guard, the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence Service, the Central Anti-Corruption Bureau, and the Internal Supervision Inspector.

relation to this, the significant difference between the numbers of requests received and responded over the period 2016-2020 needs further interpretation<sup>41</sup>, as there should be a reason for that other than single occasions of the GIFI refusal to provide information and the argumentation that sometimes several requests relate to the same case/ subjects and, therefore, are covered by one response.

124. Two LEAs, namely the CBA and the ISA, have direct access to the TTR database of the GIFI. Moreover, the CBA and the KAS have access through the STIR – the ICT system of the National Clearing House – to information on VAT-paying entities, including records on bank accounts, beneficial owners and transactions. The Police and other LEAs have access to a wide range of information, including data that constitutes a tax, banking and professional secrecy (under court control) and other relevant information. All competent authorities have access to the Central Register of Beneficial Owners (CRBO), which is a publicly available database.

125. As challenges in accessing financial intelligence, some of the competent authorities refer to the unnecessary requirement for a court sanction in order to access bank secrecy in ongoing investigations when charges have not been brought yet against any person; the long response time for financial institutions to provide the requested information; the long waiting time for customs and tax authorities to initiate control activities supporting ML investigations; and the insufficient coordination among various competent authorities impeding more efficient information exchange and investigation. All competent authorities consider the quality of information available or accessible to them as accurate and adequate.

### ***Use of information***

126. There are no comprehensive and accurate statistics on the use of financial intelligence accessed or obtained by the competent authorities from the GIFI and other sources in criminal investigations. Therefore, the assessment team looked at the issue from the standpoint of individual competent authorities based their statistics in an attempt to achieve an all-encompassing view of how the system works.

**Table 3.3: Use of GIFI disseminations by PPO under Article 103 (“main” notifications)**

Indicator	2016	2017	2018	2019	2020
Notifications to PPO	202	171	184	320	378
Refusals to institute criminal proceedings	15	11	11	10	N/A
Notifications attached to ongoing investigations	N/A	7	56	102	N/A
Notifications having triggered new investigations	N/A	153	117	208	N/A
Indictments signed off on completed investigations	N/A	49	46	61	N/A

---

<sup>41</sup> One of the reasons for the said difference might be double counting of the notifications to cooperating units under Article 106 and responses to the requests from them under Article 105 of the AML/CFT Act (as presented in Table 3.4 below). In any case, the lack of consistent and reliable statistics is a serious issue with significant impact on the analysis of various aspects of the AML/CFT system in Poland.

Ratio, notifications attached to ongoing investigations/ notifications	N/A	4%	30%	32%	N/A
Ratio, new investigations to notifications	N/A	93%	91%	95%	N/A
Ratio, indictments to notifications	N/A	30%	36%	28%	N/A

127. Data in the table above shows that from all the GIFI “*main*” notifications to the PPO on ML/TF suspicions, on average, 93% become new investigations, of which 31% become indictments for ML/TF. Importantly, in the considered period, as many as 47 “*main*” notifications of the GIFI to the PPO (data for 2020 is missing) have been refused for instituting a criminal investigation with reference to the lack of justified reasons to suspect that a criminal offence has been committed. As a result, the trend over the considered period is decreasing, from 7% to 3%, and thus positive. Nonetheless, the fact that the share of notifications attached to ongoing investigations has significantly increased up to almost one-third of all notifications to the PPO might be indicative of overextended processes both at the end of obliged entities – related to maintaining business relationships that keep triggering SARs filed with the GIFI and forwarded to the PPO and at the end of the PPO – related to lengthy periods of investigation on the subjects of GIFI notifications (*vis-à-vis* the lack of many complex investigations, which might involve numerous notifications and thus necessitate longer investigation periods).

128. The analysis of the use of GIFI communication with the PPO would be incomplete without considering the number of requests received and responded to on ML/TF suspicions. As shown in Table 3.3, within the considered period, the PPO has made to the GIFI a total of 3,657 requests, or 41% of all requests from the cooperating units. While there are no separate statistics on the number of the PPO requests responded to by the GIFI (and considering the significant difference in the numbers of received and responded requests as shown in Table 3.3), the assessment team reasonably assumes that such a large number of requests for information, which is almost three times bigger than the total number of 1,255 GIFI “*main*” notifications made to the PPO, should have created added value in the form of additional ML/TF investigations initiated by the PPO (or by LEAs with a mandate to investigate ML/TF, should the PPO make requests to the GIFI within investigations initiated by such LEAs). The authorities justifiably argue that in some cases, one or more requests are sent to the GIFI further to the “*main*” notifications made earlier by it, or within the scope of the same investigation (sometimes both by the PPO and by the LEA to which the case has been assigned) and, therefore, every response to a request from the PPO should not account for a separate investigation.

129. Nevertheless, considering that in every single year within the considered period, the number of ML/TF investigations initiated by the PPO has never exceeded the number of the “*main*” notifications made by the GIFI, while the ratio of new investigations to GIFI notifications has roughly remained the same, effective use of the GIFI responses to the PPO requests remains questionable within the context of the overall communication between the GIFI and the PPO (and LEAs, where applicable).

130. Next, the assessment team considered statistics on the GIFI communication (i.e. notifications and responses to requests on suspected predicate offences) with the cooperating units over the period 2016-2020, as presented below (a breakdown of the statistics to individual cooperating units, which would make the analysis more targeted, is not available):

**Table 3.4: GIFI communication with cooperating units under Article 105 (responses to requests) and Article 106 (notifications)**

Cooperating unit	2016	2017	2018	2019	2020
Notifications (under Article 106)	644	566	615	276	249
Responses to requests (under Article 105)	1 561	963	630	248	247
<b>Total</b>	<b>2 205</b>	<b>1 529</b>	<b>1 245</b>	<b>524</b>	<b>496</b>

131. The data in the above table has been compared with that on the use of information as reported to the GIFI by individual cooperating units under Article 14(5) of the AML/CFT Act stipulating provision of feedback on the actions taken with regard to provided information. Such data is available primarily for the KAS and Police (from the GIFI Annual Report for 2020)<sup>42</sup>:

**Table 3.5: Use of GIFI communication by KAS, 2020**

Action taken	Number	Share in total
Attached to ongoing tax and customs control	209	33%
Currently subject to further analyses	203	32%
Forwarded to KAS subdivisions for further processing	67	11%
Initiated tax and customs control	63	10%
Not acted upon/ shelved	56	9%
Used otherwise as part of own statutory activities	26	4%
Forwarded to PPO/ LEAs for initiating criminal proceedings	6	1%
Used for blocking accounts for fiscal crimes	2	0%
<b>Total</b>	<b>632</b>	<b>100%</b>

132. Based on the data in the table above, 43% of the GIFI communication to the KAS is used to initiate tax and customs controls or to supplement existing controls. Another 44% is subjected to further analyses (potentially indicating a large backlog of cases on the recipient's side), on 9% of communication, no further action is taken (potentially indicating the need for better interaction between the GIFI and the KAS to fine-tune the scope/substance of requested data to enhance usability of communicated information), and only 1% is forwarded to the PPO/ LEAs for initiating criminal proceedings (still unclear whether with or without charges of ML). In relation to this, the authorities advise that the KAS follows the principle of the economics of proceedings; their objective is to recover unpaid taxes and to bring the perpetrators to justice. Accordingly, they may refrain from taking action if that objective, in their opinion, cannot be achieved effectively (*e.g.* no transactions, no assets, the owner of the company is no longer in Poland etc.). This confirms the AT's conclusion on the lack of LEA's focus on ML/TF.

<sup>42</sup> Ideally, the figures in this and the next table should be comparable to the sum of the respective figures in Table 3.1 (on the number of the GIFI notifications to the cooperating units) and in Table 3.2 (on the number of requests made by the cooperating units to the GIFI), which is not the case due to the lack of centralized uniform statistics on exchanges of information between competent authorities and on outcomes of using such information.

**Table 3.6: Use of GIFI communication by Police, 2020**

Action taken	Number	Share in total
Currently subject to further analyses	101	59%
Attached to ongoing preparatory proceedings	25	15%
Used otherwise as part of own statutory activities	19	11%
Response indicated lack of information on request subjects	10	6%
Verified negatively (proceedings not initiated)	6	3%
Forwarded to PPO for initiating criminal proceedings	6	3%
Used as part of international exchange of information	3	2%
Forwarded to KAS for further processing	2	1%
<b>Total</b>	<b>172</b>	<b>100%</b>

133. A similar picture is portrayed looking at the outcomes of using the GIFI communication by the next key recipient, namely the Police. Here the share of information subjected to further analysis (59%) is even larger than in the case of the KAS, another 11% is used as part of own statutory activities, and only 3% is forwarded to the PPO for initiation of criminal proceedings not necessarily with ML charges.

134. To conclude the topic on the use of financial intelligence accessed by competent authorities in Poland, summary data provided by the PPO shows the number of criminal investigations initiated based on information received from all domestic and foreign sources:

**Table 3.7: Instigated money laundering investigations, by source of information**

Source of information	2018	2019	Total	Share in total
General Inspector of Financial Information (GIFI)	117	208	325	43%
Public Prosecutor's Office (PPO)	54	68	122	16%
National Revenue Administration (KAS)	18	25	43	6%
Police (incl. PCBI)	18	35	53	7%
Internal Security Agency (ISA) (incl. CTC-ISA)	6	10	16	2%
Central Anti-Corruption Bureau (CBA)	2	4	6	1%
Border Guard (BG)	2	1	3	0%
Courts	4	1	5	1%
Foreign sources	1	3	4	1%
Public administration bodies	1	2	3	0%

Komisja Nadzoru Finansowego (KNF)	1	-	1	0%
National Guarantee Funds	1	-	1	0%
Banks	45	39	84	11%
Cooperative savings and credit unions	2	-	2	0%
Natural and legal entities	40	41	81	11%
<b>Total</b>	<b>312</b>	<b>437</b>	<b>749</b>	<b>100%</b>

135. As one can see in the table above, while the GIFI is a key source of information for initiating ML investigations in the country, the PPO is the initiator of investigations in 16% of cases. A modest share of 6% and 7% of ML investigations is initiated further to notifications to the PPO by, respectively, the KAS and the Police, although these two agencies are the largest “consumers” of information from the GIFI with, respectively, 40% and 50% share of the KAS and 7% and 15% share of the Police as requesters of information and receivers of notifications from the GIFI. A positive aspect is that 11% of the investigations are initiated based on information received from natural and legal entities, which indicates a proactive approach within the society to report potential crimes.

136. The last, but not least, descriptor of the use of financial intelligence by competent authorities is the number of notifications sent to the GIFI on decisions about blocking accounts or suspending transactions, instituting criminal proceedings, bringing charges or indictments in ML/TF cases. Reliable statistics on this is available for the PPO only, which provides feedback to the GIFI under Article 81 of the AML/CFT. The table below presents statistics over the period 2016-2020:

**Table 3.8: Notifications to GIFI by PPO under Article 81**

Cooperating unit	2016	2017	2018	2019	2020
Number of notifications	51	77	90	191	185

137. The PPO has also presented a breakdown of data to the stages of such procedure, as presented in below statistics for the period 2018-2020:

**Table 3.9: Notifications to GIFI by PPO under Article 81, by stage of criminal proceedings**

Stage of criminal proceedings	2018	2019	2020
Instituting preparatory proceedings	28	54	52
Conducting preparatory proceedings	18	39	29
Bringing charges	34	83	82
Bringing indictment	10	15	22
<b>Total</b>	<b>90</b>	<b>191</b>	<b>185</b>

138. Further aspects of the use of financial intelligence and other relevant information to develop evidence and trace criminal proceeds related to ML/TF and predicate offences is presented under the analysis for Core Issue 6.3 (regarding the extent to which FIU analysis and disseminations support operational needs of competent authorities), as well as IOs 7 and 9 (regarding investigation and prosecution of ML/TF).

### 3.2.2. STRs received and requested by competent authorities

#### **Reports and disclosures received from obligated institutions**

139. Obligated institutions file two types of SARs with the GIFI. The first type of SAR is filed under Article 74 of the AML/CFT Act in relation to “*any circumstances which may indicate the suspicion of committing the crime of money laundering or financing of terrorism*” no later than two business days following the day of confirming the suspicion. These SARs are associated with situations whereby the obligated institution does not have much information or arguments to substantiate its suspicions but also cannot assign the respective business relationship to the pool of “*normal*” ones due to certain features (*e.g.* lack of sufficient CDD information, unclear business profile, etc.). The assessment team considers that availability of the reporting regime under this article may (indirectly) stimulate defensive reporting practices, as well as serve to justify the lack of more decisive action by obligated institutions in circumstances potentially related to ML, e.g. in case of business relationships with shell companies widely used in VAT-related fraud and similar crimes (also see the analysis of the data in Table 3.10 on the proportion of SARs filed with GIFI under different regimes).

140. The second type of SAR is filed under Article 86 of the AML/CFT Act immediately upon having “justified suspicion that the specific transaction or specific assets may be associated with money laundering or financing of terrorism”, for which the GIFI has 24 hours to confirm blocking the account or suspending the transaction. These SARs are associated with situations whereby the suspicions of the obligated institution have matured to an extent of considering the application of provisional measures to prevent the flight of funds on suspected accounts. The assessment team considers that the practise under this reporting regime needs to be further improved to secure blocking or suspension of as many funds as possible, especially in the case of accounts used for transiting funds through the Polish financial system (also see the analysis of the respective data in Table 3.19 on assets included in notifications, blocked account balances and suspended transactions).

141. The GIFI also receives notifications from the obligated institutions<sup>43</sup> under Article 89 of the AML/CFT Act on business relationships or transactions that they report directly to the PPO upon “*acquiring reasonable suspicion*” that the assets are proceeds of, or associated with, a crime other than ML, TF, or fiscal crimes. Upon receipt of the respective notification, the PPO has 96 hours to issue a decision on the institution or a refusal to institute relevant proceedings and should immediately notify the obligated institution of such a decision. If proceedings are instituted, the PPO will block the account or suspend the transaction for a period not longer than six months.

142. Another type of report is stipulated under Article 90 of the AML/CFT Act, whereby obligated institutions notify the GIFI on business relationships or transactions that, while having the features of those reported under Article 86, were not blocked or suspended. The reasons for the failure to comply with the requirements of Article 86 are attached to such reports, mainly associated with situations when suspicions arise after the funds are gone—the element triggering the suspicions emerges after carrying out the transaction.

143. The GIFI also receives other disclosures from the obligated institutions not qualified as SAR, mostly related to the provision of supplementary information or other communication on

---

<sup>43</sup> Except for banks, branches of credit institutions, cooperative savings and credit unions

previously filed SARs or GIFI requests. The table below provides statistics on SARs and related disclosures filed with the GIFI by obligated institutions over the period 2016-2020:

**Table 3.10: SARs and related disclosures filed with GIFI by obligated institutions**

Sources of and bases for reporting	2016	2017	2018	2019	2020
SARs under Article 74	2 996	3 211	2 853	3 313	3 172
SARs under Article 86	363	131	153	305	324
Notifications under Article 89	-	-	-	3	3
Notifications under Article 90	-	-	-	63	21
Other disclosures	-	-	-	13	67
<b>Total</b>	<b>3 359</b>	<b>3 342</b>	<b>3 006</b>	<b>3 697</b>	<b>3 587</b>
Ratio, Article 74 SARs to all disclosures	89%	96%	95%	90%	88%
Ratio, Article 86 SARs to all disclosures	11%	4%	5%	8%	9%

144. Hence, 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 to the possibility of – but not features substantiating – ML/TF suspicions. On the other hand, if the data for 2016 is dropped (since the authorities advise that the share of SARs filed under Article 86 is not reliable as it comprises a large number of uniform notifications filed by a single postal operator), the year-on-year proportion of the SARs filed under Article 86 over the considered period shows a slowly increasing dynamics, 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, thus also reducing the work done by the GIFI subsequent to SARs that provide little or no details on the features substantiating ML/TF suspicions.

145. 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 to other competent authorities as a notification on suspicion of other crimes. The SARs which form the basis of the GIFI analysis are filed in the form of a descriptive text document, wherein obligated institutions set out the reasoning of their suspicions. Among obligated institutions, banks keep records of all individuals and companies that have been subjects of their SARs or previous GIFI requests. They monitor the accounts, detect when new contractors appear in the transactions and send follow-up SARs linking them to previous SARs or GIFI requests.

146. Nevertheless, the GIFI observes that some SARs have shortcomings in terms of missing CDD or account information or inadequate justification of the suspicion, which are particularly challenging in case of SARs reported pursuant to Article 86 of the AML/CTF Act due to the 24-hour deadline to make the decision on blocking the account or suspending the transaction. To remedy this shortcoming, the GIFI has instructed obligated institutions to apply all relevant CDD measures first and, only upon having all necessary information and documents, consider filing a SAR with the GIFI. It also provides written materials (handbooks/ typologies) and training aimed at enhancing the quality of SARs.

147. Another parameter of SAR quality is their alignment with the prevalent risks in the country. Whereas the assessment team has not been provided with structured statistics on the typologies underlying SARs filed by the obligated institutions, relevant conclusions can be indirectly drawn looking at the breakdown of the value of blocked accounts and suspended transactions based on SARs, as well as on alerts from the cooperating units, as follows:

**Table 3.11: Breakdown of value of blocked accounts and suspended transactions, by type of suspected criminal activity**

Category	2016	2017	2018	2019	2020
Other fraud/extortion	51 700	14 600	67 500	80 497	69 783
Other penal fiscal offences	39 900	73 200	59 600	40 413	62 160
VAT fraud in international trade	63 300	41 600	50 200	48 845	45 300
Phishing attacks	1 300	5 500	2 000	24 558	4 114
Other	17 900	-	19 800	20 609	111 398
Terrorist activity	-	-	-	18 558	-
Acts to detriment of economic entity	1 400	4 000	6 500	15 055	3 521
Smuggling or illegal trading in other goods	29 900	0	3 700	10 599	7 137
Corruption	-	4 100	3 900	4 112	1 702
Smuggling/drug trafficking	0	2 100	317 700	793	716
Smuggling/trading in tobacco products	1 200	-	-	138	155
Theft	-	-	-	21	1
Other predicate offences	1 800	2 100	29 400	-	1 516
<b>Total</b>	<b>208 400</b>	<b>147 200</b>	<b>560 300</b>	<b>264 198</b>	<b>307 503</b>

148. On average, 35% of the typologies reported in SARs pertain to VAT-related fraud and other penal fiscal offences, 22% to drug trafficking/ smuggling, which is commensurate with the landscape of prevalent proceeds-generating crimes in the country. Nonetheless, SARs with underlying typologies of corruption offences comprise 1% only, which is not consistent with the significance of the threat emanating from this predicate offence, even having regard to its highly latent nature and complexity of methods of laundering the proceeds of crime. In relation to this, the authorities advise that the low level of SARs specifically associated with corruption-related suspicions is “compensated” by the number of the GIFI analytical proceedings concerning corruption, which are then notified to the CBA (overall 375 disclosures as notifications under Article 106 and responses to requests under Article 105 of the AML/CFT Act within the period 2016-2020). Nevertheless, the very low number of ML investigations instigated by the CBA (2 cases in 2018 and 4 cases in 2019) and the lack of statistics on corruption investigations instigated by the CBA further to the GIFI notifications do not enable a conclusion that corruption

offences are appropriately identified, and relevant disseminations of the GIFI are properly used, within the AML/CFT system.

149. The tables below show the concentration of SAR reporting by different types of obligated institutions:

**Table 3.12: SARs filed with GIFI by different types of obligated institutions**

Obligated institutions	2016	2017	2018	2019	2020
Banking sector	2 836	3 104	2 779	3 538	3 345
Cooperative savings and credit unions	33	44	24	5	6
Insurance sector	6	4	14	14	12
Capital sector	18	16	22	22	19
Payment services providers	18	19	30	58	72
Currency exchange sector	21	1	2	4	6
Other financial institutions	13	9	9	20	45
Gambling sector	-	-	9	5	8
High value goods dealers	35	43	77	13	2
Legal professionals	15	20	16	8	3
Tax and accounting advisers	12	12	2	8	17
NGOs	-	-	-	1	2
VASPs	-	-	1	-	50
<b>Total</b>	<b>3 007</b>	<b>3 272</b>	<b>2 985</b>	<b>3 696</b>	<b>3 587</b>

150. According to the data in the table above, on average, 94.3% of SARs come from the banking sector, which is commensurate with its 70% share of the financial sector total assets and diversity of products/ services offered to customers. Nonetheless, certain obligated institutions, such as payment service providers, currency exchange operators and VASPs, given the risk profile of their activities, would be expected to have a more significant contribution in terms of SAR reporting compared to the current practices of, respectively, 1.2%, 0.2% and 0.31% (although in absolute numbers a major increase of SARs filed by VASPs has been recorded, *i.e.* 1 in 2018 and 50 in 2020).

151. Concentration of SAR reporting is also an issue within the bank sector, which is the major contributor of SARs in the AML/CFT system. The table below depicts a sanitised breakdown of SARs reported over the period 2019-2020 by individual banks:

**Table 3.13: SAR reporting by individual banks**

Bank	2019	2020	Average
B509	17.3	15.5	16.4
B1017	16.4	28.3	22.3
B1096	13.7	10.6	12.2

B1230	7.9	5.2	6.5
B7132	4.8	0.0	2.4
B1496	4.5	4.6	4.6
B1085	4.2	7.1	5.6
B541	3.0	3.3	3.1
Others	28.3	25.5	26.9
<b>Total</b>	<b>100.0</b>	<b>100.0</b>	<b>100.0</b>

152. As shown in the table above, the first five contributors of SARs produce 60% of the total number of SARs. This could be considered normal with regard to the size of the banks, as well as their business model, risk profile, consumer base and other relevant characteristics. Nonetheless, meetings during the onsite visits revealed that one of the most significant players in the market providing the whole range of the products and services stipulated by the license and having comparable (or even higher) parameters of activities vis-à-vis the top three reporting banks has been filing around 120 SARs annually over the period 2016-2020. This may suggest inadequate reporting practices in particular banks within the sector.

153. In relation to this bank, the authorities inform to have taken action since 2019, due to which in 2021 penalties were imposed and criminal proceedings were initiated against the staff of one particular branch of the bank responsible for reporting suspicious activity. They advise that the bank has a smaller percentage of corporate and non-resident clients (although the bank confirmed otherwise during the onsite meeting), has well-functioning procedures for customer onboarding (particularly for foreigners and Polish companies controlled by them), thus justifying the low number of cases of identified ML/TF suspicion. In this regard, the assessment team considers that the authorities should act more proactively, applying both supervisory tools of the KNF and analytical efforts of the GIFI to identify low performers and take remedial action promptly.

154. In addition, obligated institutions<sup>44</sup> file TTRs with the GIFI on transactions with a value over €15 000, related to cash deposits to and withdrawals from accounts, transfers of funds<sup>45</sup>, currency exchange transactions and certain notarial operations. Around 30-35 million reports per year are added to the TTR database, which is extensively used for operational analysis conducted by the relevant divisions of the GIFI.

#### *Reports and disclosures received from cooperating units and other sources*

155. Cooperating units are also obligated to “immediately notify the GIFI of a suspicion of committing a crime of money laundering or financing of terrorism”. With regard to the SARs from cooperating units (mostly from the KAS and the Police), these are sometimes follow-ups of previous working contacts related to the contents of a to-be-filed SAR. Accordingly, the GIFI does not face major problems with inadequate justification of the suspicion. Nevertheless, in certain cases, these SARs do not meet the expected quality standard in terms of missing identification data disabling proper identification of individuals or businesses; lack of information regarding

---

<sup>44</sup> Except for currency exchange offices, notaries, attorneys and legal advisers, tax advisers and intermediaries in real estate trading

<sup>45</sup> Except for certain types of intra-institution and domestic transfers

the alleged stage of ML and the related transactions; and very general information about the predicate offence indicating lack of strong evidence.

156. The GIFI also receives disclosures from other sources, such as anonymous whistleblowers, for which the procedure of registration and analysis is the same as for SARs. The table below provides statistics on SARs and related disclosures filed with the GIFI by cooperating units and other sources over the period 2016-2020:

**Table 3.14: SARs and related disclosures filed with GIFI by cooperating units and other sources**

Sources of and bases for reporting	2016	2017	2018	2019	2020
SARs from cooperating units under Article 83	853	796	543	240	143
Other disclosures from cooperating units	-	-	-	53	36
Disclosures from other sources	55	47	97	110	39
<b>Total</b>	<b>908</b>	<b>843</b>	<b>640</b>	<b>403</b>	<b>218</b>

157. Over the period 2016-2020, the number of SARs filed by cooperating units has been steadily decreasing, mainly due to lower levels of reporting by the KAS. This is not commensurate with ML threats emanating from certain types of predicate offences with the highest potential of generating proceeds of crime, wherein VAT-related fraud is the number one offence in the country. On a related note, KAS is not a major contributor to the PPO in notifications to instigate ML investigations (see Table 3.7 in the analysis for Core Issue 6.1), meaning that it does not focus on tracing and confiscating proceeds generated through fiscal crimes.

**Table 3.15: Breakdown of SARs filed with GIFI by cooperating units under Article 83**

Cooperating unit	2016	2017	2018	2019	2020
National Revenue Administration (KAS)	788	751	479	141	29
Police (incl. PCBI)	55	40	54	94	104
Internal Security Agency (ISA) (incl. CTC-ISA)	4	1	7	2	2
Central Anti-Corruption Bureau (CBA)	4	2	2	3	6
Border Guard (BG)	2	2	1	-	2
<b>Total</b>	<b>853</b>	<b>796</b>	<b>543</b>	<b>240</b>	<b>143</b>

158. The GIFI has the necessary infrastructure, including physical and IT security measures, for safe receipt and storage of all reports and other disclosures sent by obligated institutions and cooperating units. The authorities do not report any instances of a security breach, information leakage or tipping-off caused by or facilitated through to the actions of the GIFI.

159. The GIFI does not have sufficient mechanisms for the provision of general and specific feedback to the obligated institutions on, *inter alia*, their SAR reporting performance. General feedback is delivered through meetings at different fora, such as at the Polish Banks Association, publication of communiques on the GIFI website on issues that need clarification, publication of annual reports, meetings with individual obliged entities, workshops on typologies and trends,

etc. To improve the reporting performance by obligated institutions, a well-established mechanism is needed – at least for the most important players in the market – to regularly receive, from the GIFI and the supervisors, analyses and conclusions on matters that have key importance in terms of effective implementation of the AML/CFT requirements including, but not limited to, SAR reporting. As for specific feedback, this is limited to the GIFI obligation to inform the obligated institutions about making a notification to the PPO further to a SAR filed by them, with no communication on the status of other SARs, including the reasons for their non-escalation to the LEA.

### *3.2.3. Operational needs supported by FIU analysis and dissemination*

160. In terms of legal definition, the Polish FIU is represented by one person – the General Inspector of Financial Information – whom Article 10 of the AML/CFT Act defines as one of the “competent government administration authorities in charge of counteracting money laundering and financing of terrorism” (the other authority is the Minister of Finance). The GIFI is appointed and dismissed by the Prime Minister of Poland at the request of the Minister of Finance after seeking the opinion of the minister competent for coordination of special services’ activities and has the status of the Secretary or Undersecretary of State in the office of the Minister of Finance.

161. The authorities advise that, due to respective arrangements within the Polish legislation, all activities of government agencies are done on behalf of the first person in the agency; consequently, the AML/CFT Act lists all duties and powers of the FIU as those assigned to the GIFI personally. In practice, the GIFI has issued a written authorisation for the Director of the Department of Financial Information (DFI) to perform all these duties and powers except for signing off the NRA, the National AML/CFT Strategy, annual reports, communiques to the private sector published on the GIFI website, as well as representing the national FIU at the Parliament, the Cabinet of Ministers etc. To avoid confusion, all references in this report to the GIFI pertain to the DFI as the structural department within the Ministry of Finance, unless specified otherwise.

162. The DFI has its own structure and internal regulations. Divisions of the DFI fulfil tasks related to the core function of analysis (i.e. the divisions for preliminary, regular and complex analyses with a total of 29 staff positions; the divisions for data processing and modelling with a total of 12 staff positions), receipt and dissemination (i.e. the divisions for national and international co-operation with a total of 18 staff positions), as well as tasks related to support or supplementary functions (i.e. the division for control with 12 staff positions, the team for legal assistance and the team for national risk assessments with three staff positions each).

163. The DFI owns an IT system – the SIGIIF – specifically designed and implemented to serve its functions and tasks. It is separated from similar systems of the Ministry of Finance and is maintained by the IT unit within the DFI. SIGIIF is comprised of the so-called external and internal modules. The external module is used for receiving SARs, TTRs and other communication from obligated institutions, as well as for enabling access of relevant data to obligated institutions and cooperating units. Data is received via a special interface or website, encrypted and signed with a qualified electronic signature. The internal module is used for analytical processing of information with tools for data search, link and statistical analysis. Apart from the SIGIIF, the DFI analysts also have access to other analytical software, such as Data Walk or Clementine.

164. Each SAR received at the DFI is first screened by the Deputy Director overseeing analytical units to determine its priority and urgency and is assigned to the division responsible for preliminary analysis, where the analyst fills in a score sheet assigning points to the case. Cases

that receive points above the pre-determined threshold are qualified as “active” cases proposed to be forwarded for further analysis; those below the threshold remain as “passive” cases. The Deputy Director makes the final decision on the status of the case. Any “passive” case may be forwarded for further analysis whenever there is new information that justifies doing so.

165. In some instances, a case may bypass the scoring stage and be immediately forwarded for further analysis, for example, when obligated institutions send a SAR under Article 86 of the AML/CFT Act seeking the DFI confirmation to block an account or suspend a transaction, or when cooperating units send SARs asking to consider the possibility of blocking an account or suspending a transaction. On the other hand, in some instances, a case may also be qualified as a “passive” one without the scoring stage, e.g. when the obligated entity states in the SAR that LEAs have been informed of the case pursuant to Article 89 of the AML/CTF Act.

166. There is also a third category called “registered” cases, which are neither “active” or “passive” and form the pool of the analytical proceedings triggered by SARs that are not attached to an existing case, are not considered a priority, do not prove positive for links to previous requests or other alerts, and are not associated with higher risk areas (such as trade in drugs and medicines, virtual currencies, cross-border movements of cash etc.). The table below presents statistics on the categories of ML analytical proceedings initiated by the GIFI within the period 2016-2020:

**Table 3.16: Categories of ML analytical proceedings initiated by GIFI**

Category	2016	2017	2018	2019	2020
“Passive” cases	978	883	993	1 057	951
“Active” cases	1 040	901	793	734	663
“Registered” cases	491	782	374	710	643
<b>Total</b>	<b>2 509</b>	<b>2 566</b>	<b>2 160</b>	<b>2 501</b>	<b>2 257</b>

\* Over the considered period, the GIFI also initiated 195 TF analytical proceedings (see the relevant statistics in Table 3.18)

167. To enable relevant comparisons, the assessment team considered the number of all SARs filed by obligated institutions and cooperating units within the same period:

**Table 3.17: SARs and other disclosures filed with GIFI**

Source of SAR or other disclosure	2016	2017	2018	2019	2020
Obligated institutions	3 290	3 272	2 982	3 697	3 587
Cooperating units	853	796	543	293	179
Other sources	55	47	97	110	39
<b>Total</b>	<b>4 198</b>	<b>4 115</b>	<b>3 622</b>	<b>4 100</b>	<b>3 805</b>

168. Comparing the number of analytical proceedings initiated by the GIFI with the number of all SARs filed by obligated institutions and cooperating units within the considered period, there is a significant difference totaling on average 40% of all filings annually. The authorities advise that, at an average 1.65 SAR per case indicator over the considered period, this difference comprises the SARs that are attached to an existing “passive” or “active” case or revitalize an

existing “registered” case sending it to pre-analysis for re-determination of status as “active” or “passive”. Nonetheless, following the principle that each SAR should end up joining one of the specified three categories of analytical proceedings within the GIFI, and considering that responses to requests from domestic and foreign counterparts are not registered as separate cases/ analytical proceedings, this difference most probably comprises either the backlog of SARs awaiting initial screening and prioritisation for subsequent assignment to the respective category of analytical proceedings, or a fourth category of disclosures filed with the GIFI and not explained to the assessment team as far as their further processing and use are concerned. It is also possible that the above-mentioned difference is due to inconsistencies of the system/ software used to generate statistics on the numbers of SARs, analytical proceedings and other deliverables of internal procedures.

169. Prioritisation of SARs and related analytical proceedings is done similarly in the course of preliminary and advanced analysis, considering first whether the SAR requires urgent action in terms of blocking an account or suspending a transaction, concerns TF suspicions, pertains to the higher risk areas identified by the NRA<sup>46</sup>, is related to previous/ ongoing cases or information received from cooperating units, contains information on specific predicate offences, or is specified as a priority by the Director, the Deputy Director or the head of the respective analytical unit. Such prioritisation, while quite reasonable in terms of initial processing of newly arrived SARs, is not sufficiently standardised to ensure mandatory consideration of all relevant descriptors of relative significance, which may adversely affect the selection of cases to be analyzed.

170. To remedy this, the GIFI should further develop and implement a comprehensive set of criteria for prioritisation of SARs and related analytical proceedings, thus also lowering the level of uncertainty related to personal decisions (e.g. prioritisation by the Director or the Deputy Director), which technically cannot be well-informed to due to the large number of SARs received daily (on average 15-16 per working day) and the lack of initial outcomes of analysis to make such decisions (the authorities advise that this process will be further formalised).

171. “Active” cases proposed for advanced analysis are forwarded to the units in charge of regular and complex cases. Throughout the course of the analysis, the analyst decides whether additional information is to be requested from obligated institutions or cooperating units to further the work. Such requests are authorised by the head of the relevant unit upon verification of the legal basis and the scope of information requested. Authorisation is also required for requests to block an account or suspend a transaction, disseminations to the PPO or other competent authorities, requests and spontaneous disclosures to foreign FIUs, and summaries for case closure. Each search in the databases with sensitive information is registered and can be executed only through personal login ID and password. Access to databases is granted only on a “need to know” basis.

172. Outcomes of the GIFI analyses are considered in terms of the notifications to the PPO on ML/TF suspicions and to other competent authorities on suspicions of predicate offences:

---

<sup>46</sup> These areas are mainly defined in terms of high-risk countries and regions (associated with armed conflicts, tax havens, drug production countries etc.)

**Table 3.18: Outcomes of GIFI analyses**

	2016	2017	2018	2019	2020
Analytical proceedings initiated for ML	2 509	2 566	2 160	2 501	2 257
<i>Including, "self-initiated" analyses</i>	54	45	71	27	68
Analytical proceedings initiated for TF	89	37	41	19	9
<i>Including, "self-initiated" analyses</i>	2	-	-	-	-
<b>Total, analytical proceedings</b>	<b>2 598</b>	<b>2 603</b>	<b>2 201</b>	<b>2 520</b>	<b>2 266</b>
Notifications to PPO ("main")	202	171	184	320	378
Notifications to PPO ("supplementary")	200	169	252	258	297
Notifications to other competent authorities	644	566	615	276	249
<b>Total, notifications (with PPO "main" only)</b>	<b>846</b>	<b>737</b>	<b>799</b>	<b>596</b>	<b>627</b>
Ratio, notifications (with PPO "main" only) to analytical proceedings	33%	28%	36%	24%	28%
<b>Total, notifications (with PPO "main" and "supplementary")</b>	<b>1 046</b>	<b>906</b>	<b>1 051</b>	<b>854</b>	<b>924</b>
Ratio, notifications (with PPO "main" and "supplementary") to analytical proceedings	40%	35%	48%	34%	41%

173. The number of “self-initiated” analyses, which are triggered by the requests or other alerts from the domestic and foreign counterparties, is relatively small compared to the number of such requests (see “Table 3.2: Requests to GIFI by cooperating units under Articles 104-105, and responses to such requests” in the analysis for Core Issue 6.1, as well as the respective statistical data in the analysis for IO.2), indicating that the GIFI rarely finds value in information requests to launch its own analysis. The authorities advise that requests often involve SARs/cases already in progress; therefore, initiating a new case on own initiative is not necessary. This, however, should be considered in the broader context of effective use of the GIFI responses to the requests from the cooperating units, as analysed under sub-section “Use of information” above.

174. The ratio of notifications to analytical proceedings, on average within the range of 30%<sup>47</sup> to 39%<sup>48</sup> over the considered period, declined from 33% in 2016 to 28% in 2020 (counting “main” notifications to the PPO, which are the primary triggers for initiating new investigations). The authorities explain this with the argumentation that a notification does not equal a case, and sometimes more than one analytical proceeding can be reported to the LEAs within one notification. As a reason behind this, they present that the links to other proceedings not obvious at the moment of initiating a new proceeding may be identified during the analysis, which appears to conflict with the statement that all SARs are pre-screened for links with previous/ ongoing

<sup>47</sup> Counting “main” notifications to the PPO

<sup>48</sup> Counting all notifications to the PPO

cases. In any case, there still needs to be a reasonable explanation about, for instance, why it would be necessary to have on average three separate analytical proceedings reported to the competent authorities in one notification, why the ratio of “main” notifications to analytical proceedings would decline over time, to demonstrate, for example, that more and more analyses do not end up with a conclusion that there is nothing worth of dissemination to the LEAs, thus indicating either insufficient quality of SARs/ other alerts or inadequate outcomes of analysis to support the needs of competent authorities.

175. Another measurement of the extent to which FIU analysis and disseminations support the needs of competent authorities is the value of assets indicated in the notifications to the competent authorities compared to the value of blocked account balances and suspended transactions on the FIU’s own initiative or further to requests from the competent authorities:

**Table 3.19: Statistics on assets included in notifications, blocked account balances and suspended transactions**

Indicator	2016	2017	2018	2019	2020
Value of assets involved in notifications to LEAs (PLN billion)	18.6	6.2	6.3	11.6	15.4
Accounts blocked, domestic	325	351	302	640	673
<i>Of which, on GIF I's initiative</i>	295	310	233	392	300
Value of blocked domestic account balances (PLN million)	171.3	140.6	430.6	208.0	246.2
<i>Of which, on GIF I's initiative</i>	166.1	107.1	382.1	106.0	57.4
Accounts blocked, foreign	-	-	-	4	1
Value of blocked foreign account balances (PLN million)	-	-	-	13.0	13.8
Transactions suspended	22	21	15	37	32
<i>Of which, on GIF I's initiative</i>	1	2	2	4	13
Value of transactions suspended (PLN million)	31.2	3.0	116.7	31.0	26.7
<i>Of which, on GIF I's initiative</i>	2.1	1.6	0.04	3.7	2.4
Total value of blocked account balances/ suspended transactions (PLN million)	202.5	143.6	547.3	252.0	286.7
<i>Of which, on GIF I's initiative</i>	190.2	129.7	397.1	146.7	91.8

176. Hence, the ratio of the total value of blocked account balances and suspended transactions to the value of assets involved in the GIF I notifications is on average 2.5%. Whereas this indicator might objectively reflect the fact that notifications to the LEAs usually refer to the account turnovers (sometimes overestimated, as the authorities advise), which may be times more than the account balances at the moment of reporting, this also means that, first, the principles for reporting the value of assets involved in in the notifications should be revised to provide a more realistic overview of the subject matter, and second, the efforts of all involved agencies need to

be significantly enhanced to achieve early detection of suspicious business relationships and transactions, thus also preventing multi-million turnovers on such accounts before they are reported through SARs and disseminated to the LEAs upon the GIFI analysis.

177. This is also indicative of potential practices and issues related to: a) on the obligated institutions' side – reporting SARs under Article 74 and waiting for the GIFI reaction while maintaining the business relationship and allowing major turnovers on respective accounts; and b) on the GIFI's side – having a significant backlog of SARs awaiting analysis and resolution or, alternatively, spending too much time on individual case analysis and resolution, which in any case results in belated action towards tracing and securing potential proceeds of crime for confiscation at subsequent stages of applicable criminal procedure.

178. The assessment team has been provided sanitised examples of the outcomes of the GIFI preliminary and advanced analyses, as well as of the disseminations to the competent LEAs, which have proper structure, involve reasonable analysis and convey substantiated conclusions. Notifications to the competent LEAs contain a description of specific schemes of transactions and patterns of activity of the reported subjects, including financial data, beneficial ownership information, supporting documents and assumptions on predicate offence/ ML/ TF.

179. The authorities advise that tasks related to strategic analysis are assigned to various units of the GIFI, including the Data Modeling Division, the NRA Team, the staff responsible for producing annual reports etc. The assessment team has been provided with examples of the outcomes of strategic analyses produced using the database of SARs, TTRs, border-crossing declarations, money remittances etc., exploring IT-powered filtering and visualization tools. While some of the examples seem to be more technical (e.g. identification of errors in TTRs) or operational (e.g. weekly reports on identified TTRs or BCDs linked to previous GIFI notifications to the PPO) in nature, others (e.g. categorisation of cases as per the assigned typology, determination of the preferred method of money transfers in case of laundering proceeds of phishing attacks) can be a useful addition to the typological and other strategic products offered by the FIU.

#### ***3.2.4. Co-operation and exchange of information/financial intelligence***

180. Legal bases for the co-operation between competent authorities to exchange financial intelligence and other information are laid down in the AML/CTF Act stipulating that both the GIFI and the cooperating units are: a) obligated to file and b) entitled to request information on suspicions related to ML, TF and predicate offences (see the details in the analysis for Core Issue 6.1). The GIFI and the cooperating units have elaborated a template request for information along with substantive support (e.g. trainings, phone call clarifications) on the procedure and principles of information exchange under the AML/CTF Act. Information exchanges are subject to confidentiality requirements established by the AML/CFT Act and relevant sectorial laws.

181. In addition, the KAS has approved in 2019 rules of co-operation with the GIFI, setting out provisions and templates for notifications on suspicious activity, communication of control planning and findings, as well as provision of feedback on the use of exchanged information. The Border Guard issued in 2019 an instruction for its structural and territorial units on the procedure of exchanging information with the GIFI. Other competent authorities do not advise having co-operation agreements, instructions, guidelines or similar tools to facilitate the exchange of financial intelligence and other information. There are agreements on co-operation between the GIFI and the ISA, the GIFI and the CBA.

182. The GIFI cooperates with a wide range of competent domestic authorities. Decisions on the mode and extent of co-operation are made internally within the DFI; they need not be consulted by other departments of the Ministry of Finance or with other competent authorities. Co-operation is realised both by formal exchange of information through official documents and by operational interaction through working contacts.

183. A dedicated and secure IT system is used for the exchange of information between the GIFI and the PPO, managed by the latter. It enables the GIFI to promptly send notifications to prosecutors, along with all attached evidence, which is particularly important in cases of requests to block an account or suspend a transaction due to deadlines defined in the AML/CTF Act. The PPO uses this system to send requests for information to the GIFI. For the exchange of information between the GIFI and ISA, a dedicated and secured IT system (CATEL) managed by the ISA is used.

184. Other competent authorities advise using conventional methods (such as e-mail or paper mail) for the exchange of information.

185. As shown in the analysis for Core Issue 6.2, over the considered period, the GIFI has received above 2 600 SARs from cooperating units. These SARs are evaluated in the same way as those from the obligated institutions. If the outcomes of the SAR analysis are disseminated to the PPO, feedback is sent to the cooperating unit (as in the case of SARs from the obligated institutions). When the GIFI receives a SAR from an obligated institution under Article 86 of the AML/CTF Act, before deciding whether to block an account or suspend a transaction, the GIFI contacts the prosecutor or the competent LEA to discuss if it would not have a negative impact on the investigation due to the potential tipping-off of the subjects of investigation.

186. Moreover, the GIFI has received more than 12 000 requests from cooperating units for information concerning around 58.000 subjects. As a rule, the requests seek information on bank accounts and financial transactions of the subjects. In case of the PPO requests in connection with notifications sent by the GIFI, these often look for additional documents and information from foreign FIUs to trace the further flow of money. The requests sometimes trigger “self-initiative” analyses by the GIFI when analytical cases are opened not on the basis of SARs but of suspicious activities identified in the course of preparing responses to requests from cooperating units (see “Table 3.18: Outcomes of GIFI analyses” in the analysis for Core Issue 6.3).

187. Upon receiving the notification of suspected ML or TF from the GIFI, the PPO provides feedback within 30 days on issuing a decision for: 1) transaction suspension or account blocking; 2) institution of proceedings, 3) suspension of proceedings; 4) reinstatement of suspended proceedings; or 5) charging a person with an offence. The PPO also informs the GIFI about indictments, and the GIFI may request a copy of such documents. In tax fraud investigations, there are also cases whereby the prosecutor closes the criminal investigation but forwards the case to tax authorities for relevant proceedings, and financial or administrative sanctions are applied in the end. Other cooperating units are also required to provide feedback to the GIFI on the use of its disseminations.

188. Overall, it appears that there are appropriate arrangements in Poland to provide for co-operation of the GIFI and the competent authorities, including through exchange of financial intelligence and other relevant information. Nevertheless, there is at least one issue – the lack of effective follow-up mechanisms – that impedes objective assessment and, subsequently, improvement of the effectiveness of co-operation. The arrangements under Article 81 AML/CFT Act stipulating for the feedback from the cooperating units to the GIFI cover a small segment of the value chain generated within the AML/CFT system, i.e. feedback is provided only with regard

to decisions about blocking accounts or suspending transactions, instituting criminal proceedings, bringing charges or indictments in cases related to ML/TF. Other than this, the GIFI has no information on the use of the notifications and responses to requests to numerous LEAs, all of which are entitled to investigate and prosecute ML/TF but rarely do so. Accordingly, a comprehensive follow-up mechanism to provide for regular stocktaking of all information exchanges between the GIFI and the cooperating units is necessary, comprising tools for general and specific feedback on the use of such exchanges both on a regular and ad hoc basis.

### ***Weighting and conclusion***

189. 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. Nonetheless, a significant part of the GIFI resources is used for purposes that, while serving the general interests of the state in combating economic and other crime, are not focused on initiating and furthering ML/TF investigations to trace and confiscate criminal proceeds generated in or passing through the country.

190. SAR reporting is not consistent with the risk profile of certain sectors (*e.g.* payment service providers, currency exchange operators and VASPs) and individual players (*e.g.* particular banks). Availability of the reporting regime under Article 74 of the AML/CFT Act for lower level suspicions may (indirectly) stimulate defensive reporting practices, as well as serve to justify the lack of more decisive action by obligated institutions in circumstances potentially related to ML. 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 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. Overall, the IO is achieved to some extent through GIFI's work in accessing, analyzing and disseminating information. Nevertheless, major improvements are needed in the area of using financial intelligence, through focus on initiating and furthering ML/TF investigations to trace and confiscate criminal proceeds generated in or passing through the country.

### ***Overall conclusions on IO.6***

191. **Poland is rated as having a Moderate level of effectiveness for IO.6.**

### 3.3. Immediate Outcome 7 (ML investigation and prosecution)

#### 3.3.1. ML identification and investigation

192. The total number of ML investigations between 2017 and 2019 was 1077, with 321 in 2017, 319 in 2018 and 437 in 2019 (see Table 3.20). Almost half of the investigations resulted from the GIFI notifications, with the other half resulting from other sources. As reflected in Table 3.7. (see IO6), the PPO is the initiator of most of the investigations (based on its own findings), while a modest share is initiated further to notifications to the PPO submitted by LEAs. Other sources include the notifications from the banking sector (concerning other crimes, like fraud), criminal complaints by natural and legal persons and foreign sources (i.e. MLA requests). During the period 2014 – 2019, 10 ML investigations were initiated as a result of the incoming MLA requests.

193. Since 2017, the LEAs have had broad powers and access to various databases already in the intelligence phase (tax, bank or professional secrecy-protected data, insurance, securities investment funds etc.). The access to the secrecy-protected data is tied to judicial permission. In practice, the LEAs often rely on the GIFI to obtain the data available there (essentially financial information kept in the GIFI databases). In cases where the GIFI has sent a notification to the PPO, it can subsequently obtain and provide additional data to the PPO.

**Table 3.20 Number of ML investigations**

	ML investigations			Prosecutions Commenced Cases/ Persons	Convictions Cases/Persons
	Total	ML investigations carried out independently (without prior STR) <sup>a</sup>	ML investigations resulted from STRs		
2020	493	246	247	214/ 926	88/ 191
2019	437	229	208	196/ 664	65/ 123
2018	319	202	117	165/ 591	72/ 160
2017	321	168	153	139/ 541	94/ 234
2016	278	154	124	91/ 234	100/ 251
2015	311	204	107	102/ 384	53/ 123
2014	351	232	119	75/ 269	46/ 121

194. All the LEAs together identify only about 10% of the ML suspicions as the result of their intelligence gathering, which is then translated into initiated criminal investigations (see Table 3.7, IO6). The LEA's contribution, as a whole, is not proportionate to their respective portfolios of major proceed generating crimes.

195. One of the reasons for this shortcoming might be that there are no designated LEAs in Poland with specific responsibility to investigate ML (see R. 30). Each LEA has competence to investigate ML in connection to the predicate offences under their remit and, in practice, whichever authority detects the suspicion of a crime conducts the investigation to the end.

Additionally, the competence of the LEAs shows broad overlaps in the main proceeds generating criminality fields, resulting in cases of similar crimes being investigated by different authorities (*i.e.* tax crimes are investigated by practically every LEA, corruption investigated by Police, CBA, ISA etc.). As a result, the ML and the major proceeds generating predicate crimes investigations are dispersed among the LEAs, with a general lack of focus and specialisation. Overall, the ML offence is regarded as having no real added value in the proceeds generating crime investigations and having no influence on the applied sanction or additional relevance in asset recovery. In addition, no detailed and meaningful guidelines exist as to the steps to be taken for the detection and investigation of potential money laundering<sup>49</sup>. This might explain the limited effectiveness that has been achieved in this regard.

196. Another potential impediment is that no due attention is paid by the LEAs to the identification of illicit proceeds and to associated ML activities. According to LEA explanations, the ML aspect of predicate crimes is investigated during their intelligence-gathering activities. Nevertheless, this claim is supported only by sporadic data, which shows little correlation with the actual results (see IO6, Table 3.7. and Table 3.21) and indicates that a relatively small percentage of investigations of predicate offences develop into ML investigations as well, although some improvements of the number of ML investigations initiated based on notifications to the PPO by certain LEAs can be noticed (Police, including the Central Bureau of Investigation (PCBI) – 35 in 2019, compared to 18 in 2018; KAS – 25 in 2019, compared to 18 in 2018; ISA – 10 in 2019, compared to 6 in 2018).

197. The financial investigation is perceived as a general obligation if the application of forfeiture is prevalent and is seen as an integral part of the “regular” investigation. However, no statistics were provided as to how many such investigations are conducted annually<sup>50</sup>.

198. Forensic expertise is routinely called upon in financial and economic crime cases, potentially supporting the ML aspect of the case as well. The PPO itself possesses analytical capacities at the regional level offices but also tasks the KAS with analytical objectives and makes use of the capacities of the Institute of Economic and Financial Expertise which was established in 2018. Likewise, the internal analytical capacities of the Police are used to support the financial investigations (financial and billing analyses).

199. While acknowledging the above, these investigations/analyses do not significantly contribute to the initiation of new ML investigations. They are not systematically conducted by specialised teams of financial investigators and do not include a full enquiry into the financial affairs related to criminal activity, with a view to identifying the extent of criminal networks and the scale of criminality.

200. This might explain the low results achieved when comparing the number of proceeds generating predicate crimes being investigated with the number of cases where money laundering was additionally investigated, and proceeds seized (see IO8).

---

<sup>49</sup> Guidelines on the rules of conducting preparatory proceedings in cases of offences related to the procedure of extortion of undue reimbursement of value added tax (VAT) and other fraudulent losses of this tax (2017) and Guidelines on the principles of conducting preparatory proceedings for financial crimes committed to the detriment of many wronged parties using financial instruments and banking activities (2016).

<sup>50</sup> See FATF Guidance on AML/CFT-related data and statistics (2015), page 58 - <https://www.fatf-gafi.org/media/fatf/documents/reports/AML-CFT-related-data-and-statistics.pdf>

201. When investigating predicate criminality, ML is not considered systematically in all relevant circumstances. According to the available criminal statistics, the following pattern can be established throughout a longer period of time: annually, there are approximately 400.000 registered potential predicate offences (excepting the high number of tax crimes investigated by KAS), about half of these fall into the category of major proceed generating crime-types, perceived as the main threats for ML, while yearly there are about 200 new ML investigations started, resulting in about 100 indictments, and 50-60 convictions (see Tables 3.21 and 3.22.).

**Table 3.21 Number of registered predicate offences and ML**

	Number of registered predicate offences (without KAS)	Number of registered ML	
2014	N/A	N/A	N/A
2015	N/A	N/A	N/A
2016	398695	301	0.0008%
2017	406119	365	0.0009%
2018	380254	462	0.0012%
2019	393368	1263	0.0032%
2020	N/A	N/A	N/A

**Table 3.22 Number of ML cases (without a prior GIFI notification)**

	ML/TF investigations without prior GIFI notification	Indictments Cases/ persons	Convictions Cases/ persons
2020	246	177/ 722	71/ 153
2019	229	135/ 449	57/ 81
2018	202	119/ 431	60/ 130
2017	168	90/ 309	120/ 327
2016	154	62/ 129	79/ 164
2015	204	60/ 209	33/ 70
2014	232	45/ 162	30/ 94

202. Likewise, when comparing the numbers of the achieved convictions for the predicate offences, which are among the major proceeds generating crimes and threats for the country (tax and drug-related crimes), with the number of ML investigations with the same underlying predicate offence, the ratio is not proportionate (see Table 3.23), which indicates that the system misses opportunities to identify ML cases. Notwithstanding, the positive feature of the ML investigations initiated in connection to a predicate crime is the relatively high indictment and convictions rate (about 50%), compared to the lower rate noticed in the ML investigations resulting from the GIFI notifications (see Table 3.24).

**Table 3.23 ML investigations compared to the number of convictions for tax and drug-related crimes (2014-2018).**

	Convictions for predicate offences (persons)	Number of ML investigations in relation to predicate offences
Tax-related crimes (direct/indirect taxes, customs and excise duties and taxes)	22 245	560
Drug-related crimes	9 167	51

203. In relation to tax-related crimes, which mainly fall into the competence of KAS, a few ML cases are investigated, despite the high number of yearly tax crime investigations. According to the data available, KAS conducted preparatory proceedings related to ML: 6 cases in 2017, 10 in 2018, 12 in 2019 and 10 in 2020, which is low in comparison to the volume of their tax crime-based portfolio.

204. One of the reasons for such modest results in detecting potential ML cases in relation to a crime that is perceived as posing the highest ML threat to the country is the limited capacity of the KAS staff. There are no specialised ML experts to conduct such preparatory proceedings, and the available expertise concerns only tax-related matters. This was also confirmed by the judges the AT met onsite, in relation to the quality of the evidence presented before the courts. KAS officials claimed that they look into the ML aspect even if the legal qualification according to Art. 299 of Penal Code is not registered. Nevertheless, the above results do not fully mirror this claim.

205. According to the Police statistics, in 2020 only, 638 operational activities in ML allegations were conducted, and already in the first three months of 2021, further 235 cases. In comparison to the same year, 2020, the number of the relevant predicate offences handled by the Police was about 210.000, which roughly means that the ML aspect is considered in every 3 000<sup>th</sup> proceed generating crime case. This is a low ratio even considering that many predicate crimes, by their nature, might not warrant an ML investigation.

206. The number of ML investigations initiated by the prosecutor based on Police findings (which includes the PCBI) is only a fraction of the overall predicate cases, leading to the conclusion that, even if some scrutiny exists to a limited extent, potential ML cases are not brought to the PPO for starting the actual criminal investigation on a regular basis.

207. In corruption cases investigated by the CBA, the ML aspect is rarely taken into account. According to the available statistics, only in less than 1 % of the corruption-related investigations is the ML aspect considered. The number of ML indictments in such cases is negligible (2 in 2018; 2 in 2019), with no final convictions. In relation to the ML investigations connected to other types of predicate offences, since its establishment (between 2007-2021), only 160 such investigations have been carried out by the CBA.

208. Although not part of the main type of activity, the powers of the ISA include the investigation of financial crimes when they are considered to jeopardize the security of Poland. Yearly, ISA conducts about 100 such ML-related operational activities (107 in 2014, 111 in 2015, 102 in 2016, 117 in 2017, 111 in 218, 108 in 2019). Nevertheless, few of these result in initiating a criminal investigation on ML (6 investigations in 2018 (5%); 10 investigations in 2019 (9%)).

209. With regard to the source of ML investigations, as described above, almost half of the investigations resulted from the GIFI notifications. Still, the PPO and the LEAs make limited use of such information for initiating ML investigations (see IO.6). The PPO's refusal to initiate an

investigation based on the GIFI notification may be appealed by the latter. This routinely happened in the past, usually resulting in the court overturning the refusal as premature. Nevertheless, the increasing number of the GIFI notifications and the decreasing number of the PPO refusals to initiate investigations based on such notifications is a positive development (10 refusals in 2020, compared to 26 in 2015).

210. Overall, the ML investigations initiated as a result of the GIFI notifications appear to be less successful than those initiated from other sources (about 27% indictment rate and 10% conviction rate, compared to a 50% rate for indictments and convictions) (see Tables 3.24 and 3.22). These results, together with the number of refusals to institute criminal investigations by the PPO, over the period 2015 – 2019 (due to lack of justified reasons to suspect that a criminal offence has been committed), presumably derive from the less obvious connection to a predicate offence, the limited capacity of the authorities to investigate more complex and standalone ML cases and the concerns raised with regard to the quality of financial intelligence in general (see IO6).

**Table 3.24 Number of ML cases (based on a prior GIFI notification)**

	Investigations initiated based on GIFI notifications to PPO	Indictments in cases based on GIFI notifications	Judgments passed in cases based on GIFI notifications	Persons indicted – convicted
2020	247	37	17	204/ 38
2019	208	61	15	215/ 42
2018	117	46	12	160/ 30
2017	153	49	13	232/ 69
2015	107	33	20	148/ 53
2014	119	30	16	107/ 27
Total	951	256	93	1066/ 259
Percentage	100%	27%	10%	

211. Few cases, if at all, were initiated as a result of cross-border declarations of cash. This raises concerns as to the level of proactiveness of the competent LEAs (KAS and BG Service) and PPO and the lack of guidelines in this area. The described cases by the competent authorities in relation to undeclared/ declared cross-border cash (see IO.8) indicate that, as a practice, even in cases of ML suspicions, the ML investigation is not initiated.

212. Incoming international requests regarding proceeds generating criminality are sporadically used to start ML investigations. The authorities presented statistics on the ML cases initiated as a result of incoming MLA requests, which indicates that, during 2014 – 2019, ten such ML investigations were initiated (eight resulted in indictments and two convictions). This is a commendable result. However, there is no mechanism in place for proactively harvesting the incoming MLA requests (see IO2).

213. Based on the principle of legality and *ex officio* mandatory action, which is a fundamental principle of the Polish criminal law and procedure, each potential crime must be investigated in an equal manner, which impacts the prioritisation of ML cases. One way of prioritising the ML investigations is by assigning them to hierarchically higher prosecution units – the regional and circuit Prosecutor’s Office, and the Public Prosecutor’s Office, depending on the seriousness of the

case, with about 10% of the ML cases being prioritised and carried out by the local division of the Department of Organised Crime and Corruption of the PPO (most complex/ serious cases).

214. The ML criminal investigations are under the control of the prosecutor who conducts the investigation and who can task any law enforcement agency (LEA) with the execution of investigative steps and measures. Therefore, the PPO is the obvious focal point and would be in the best position to foster the inclusion of the ML aspect in the investigations of those predicate offences which are regarded as the main threats for the country. This role appears to be limited by the fact that the operational activities of the LEAs are not under prosecutorial supervision, and as a result, potential ML might pass undetected.

215. In the pre-investigation (or operational, intelligence) stage, all the LEAs, comprising the Police, KAS, CBA, ISA, BG, are entitled to conduct intelligence gathering, including in ML cases, with no prosecutorial oversight, based on their respective laws (e.g., Act on the Police, Act on the Central Anti-Corruption Bureau etc.). Thus, it is up to the LEAs to bring the results of their operational activity to the prosecutor who can institute the ML investigation, according to the CPC.

216. The KAS is vested with the power to directly 'prosecute' fiscal offences described in the Fiscal Penal Code, *without* the oversight and control of the prosecutor, if these are not in conjunction with the crimes codified in the Penal Code. This might have a deteriorating effect on ML detection and investigation in connection to tax crimes since this 'fast track' option would not be available if the ML suspicion is also a part of the investigation. The Polish authorities clarified that these powers refer only to minor violations (where the amount of a depleted/ exposed to depletion public liability or the value of the object of the act does not exceed five times the minimum wage – about €5 000) and that in case of ML suspicions there is an obligation to notify the PPO, but no statistics were provided on such notifications.

217. In light of the above-described circumstances, the use of methodological guidelines on ML investigation/ prosecution is of key importance for ensuring the quality and the uniform approach towards ML cases among the wide range of LEAs with such competences. However, insufficient guidelines were issued by the PPO. The two existing Guidelines of 2016 and 2017 on the principles of conducting preparatory proceedings for financial crimes and for tax crimes marginally tackle the ML aspect.

218. Domestic joint investigation groups, including prosecutors and law enforcement officials, are used to enhance the effectiveness of investigations. Such investigations groups are created in complex cases, mostly related to economic crimes. Between 2016 and 2019, 66 such groups were established at the national level and 50 at the regional level, 37 of which were set up to investigate money laundering alongside predicate crimes.

219. Poland was a member of 45 JITs established between 2015-2020, out of which 5 included suspicions of ML (see IO.2). Given the size and geographical position of the country and the typical cross-border and organised crime nature of JIT cases, these figures are rather modest, but there is an upward trend in the application of this judicial co-operation tool, with significantly more JIT agreements concluded in the past two years. The cross-border movement of illicit assets connected to the offences investigated in these cases would merit an emphasized inquiry into ML, though.

220. Poland participates in the European Money Mule Actions (EMMA) organised by Europol, which since 2017 has led to the identification of hundreds of individuals, bank accounts and thousands of transactions in a growing number. The results of this LEA co-operation do not seem

to have made an impact on the number of ML cases and are yet to be translated into investigations (and convictions).

### ***3.3.2. Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies***

221. According to the Polish NRA and the general consensus of the authorities met with onsite, the highest ML threats are tax crimes (especially VAT-related fraud), investment and other fraud, drug-related crimes (including crimes against the pharmaceutical law), cybercrime and smuggling of goods and connected excise crimes. The most likely means and methods of ML identified in the NRA are through the use of: natural persons as money mules for cross-border transportation of cash; Hawala networks; purchase or top-up of SIM cards or use of online payment services to transfer funds.

222. The 2021 AML/CFT Strategy does not target specific predicate offences or types of ML, and the AT has not been provided with information on objectives and activities of law enforcement agencies, as well as the PPO, specifically building on the findings of the NRA or other risk assessments and aimed at mitigating ML/TF risks identified by such assessments (see also IO.1).

223. ML investigations reflect, to a certain extent, the risk profile of Poland. The statistical breakdown of the ML investigations demonstrates that the tax crimes, frauds and drug-related offences find their correspondence in the most numerous ML cases (e.g. 2017-2019 – 41 drug-related ML investigations, 312 tax related, 313 in relation to crimes against property). On a less positive note, there are no data on the other types of predicated; hence an analysis cannot be done in this respect.

**Table 3.25 The underlying predicate offence in ML investigations (PPO)**

	2017	2018	2019
Offences against fiscal obligations and settlements of donation or subsidy	110	89	113
Offences against property	106	100	107
Offences against the credibility of documents	27	29	51
Offences against the Law on counteracting drug addiction	19	8	14
Offences against business turnover	11	6	16
Offences against public safety	N/A	4	2
Offences against the Act on trading in financial instruments	1	2	2
Offences against freedom	2	2	7
Offences of corruption	4	2	3
Offences against the Law on bonds	N/A	1	1
Offences against the Rights of Persons Pursuing Paid Work	N/A	1	N/A
Offences against the Act of pharmaceutical Law	17	1	5
Offences against the Law on author's rights and related rights	2	1	1
Offences against the Industrial Property Law	2	1	N/A
Offences of human trafficking	2	1	1
Offences against the Payment Services Act	3	N/A	N/A
Offences against the Act on the manufacture of alcohol and tobacco products	2	N/A	N/A
Offences against the Act of Energy Law	1	N/A	N/A
Offences against the Gambling Act	1	N/A	
Offences against the Circulation of Money and Securities	N/A	N/A	1
Offences against the Act on restrictions on conducting certain business activities by persons holding public office	N/A	N/A	1
Offences against the Act on the protection of certain services provided by electronic means	N/A	N/A	1
Offences against the Act on banking Law	1	1	N/A
<b>Total</b>	<b>311</b>	<b>249</b>	<b>326</b>

224. As highlighted by the statistics below (Table 3.26), in practice, from 2017 to 2019, around a third of the ML investigations were connected to fiscal crimes, with a decreasing trend during this period. Another third of the ML investigations is represented by offences that can be put under the umbrella of “frauds” (see Table 3.25), while the drug trafficking-related ML investigations represent 4.6%. Although no data was provided regarding their successful prosecution, this appears to be largely in line with the country's risk.

**Table 3.26 ML investigations in connection to fiscal crimes**

	Total number of initiated ML investigations	Total number of ML investigation initiated due to or in combination with fiscal crimes	Proportion of fiscal crime cases in ML investigations
2020	493	119	24%
2019	437	123	28%
2018	319	91	28%
2017	321	112	35%
2016	278	189	67%
2015	311	68	21%
2014	351	104	29%

225. The authorities provided some successful examples of convictions reflecting the main ML proceeds generating threats, namely tax-related crimes and frauds (see the Case studies described below).

**Box 3.1: Case studies in line with threats and risk profile**

**Case 1. The Scrap metal case – VAT fraud (Autonomous ML)**

The investigation covered money laundering committed by entrepreneurs operating on the steel trade market.

The identified predicate offence was VAT fraud committed by representatives of two companies, CMC and HK. They underreported their tax obligations for the period of 2006-2011 by introducing into their accounting systems numerous VAT invoices certifying fictitious purchases of scrap metal. The invoices were issued by the companies IZ (owned by Sebastian C.) and ZP owned by (Tomasz A.). The approximative amount of proceeds was PLN 34 865 047 (€7 705 175). The proceeds of the VAT fraud were then transferred by CMC and HK to the bank accounts of IZ and ZP companies. Next, Robert B. - the leading perpetrator in the case - commanded Sebastian C. and Tomasz A. to transfer the money to their private bank accounts and then withdraw it in cash. The role of Joanna S. - the second perpetrator in the case - consisted in receiving money from Sebastian C. and Tomasz A. and handing them over to Robert B. The investigations revealed that Joanna S. was to receive proceeds of tax fraud in the total amount of PLN 1 584 736 (€350 227). The Court of Gliwice sentenced, on 26 September 2018, Robert B. to two years and six months of imprisonment, and Jolanta S. to one year and two months of imprisonment with a probation period of four years.

In addition, the court ordered the forfeiture of equivalent benefits in the amount of PLN 34 865 049 (€7 705 176) for Robert B.

**Case 2. The Money Mules case – Cyberattack fraud (Autonomous ML)**

The investigation covered the activity of an organised criminal group between 2014 and 2015. Twenty-two citizens of various countries (Poland, Nigeria, Senegal, Cameroon and the United

Kingdom) were charged with participation in organised criminal activities and aggravated money laundering.

Foreigners were the main members of the identified criminal group, and they were specialised exclusively in laundering proceeds issued from criminal activities committed outside Poland. A clear division of roles and tasks has been revealed during the investigations: some members came to Poland to open numerous bank accounts in their own names using forged identity documents. Ten Polish banks submitted 25 SARs to the FIU. The Prosecutor then issued 34 decisions on blocking the accounts to which the stolen funds were transferred. The main underlying predicate offences were identified as cyberattack frauds (Business Email Compromise) and unlawful interference with IT systems committed against natural and legal persons.

The modus operandi was to send victims incorrect information on the beneficiary's bank account numbers to which they were supposed to transfer payments to their business partners. The money would arrive to the perpetrators, who then transferred it to subsequent bank accounts. Finally, the money was withdrawn at cash desks and ATMs in Poland, other EU countries and in Africa.

During the investigations, it was revealed that the value of damages resulting from the underlying crimes, and thus the total of laundered funds, was established in Poland at around PLN 10 761 029, €495 386 and US\$1 379 809.

Property was seized for an amount of approximately PLN 2 000 000 (€442 000). The value of forfeited property amounted to approximately €100 000. Out of the 22 perpetrators involved, 18 were convicted for money laundering and sentenced to penalties ranging from one year and two months to two years of imprisonment, to which fines and forfeiture of the benefits of the crime were added.

The remaining four perpetrators were prosecuted in separate investigations due to their hiding from LEAs after concluding the main investigation. All of them were convicted.

### **Case 3. The Amber Gold case – Fraud (Self-laundering)**

The investigation was conducted by the District Prosecutor's Office in Łódź and covered the activities of the shareholders and managers of AG Ltd. Between 2009 and 2012, they misled their clients to dispose of their property against their interest, with damages amounting to a total of PLN 850 640 168 (€187 991 477).

The clients entrusted their funds to the perpetrators with the objective of purchasing certified precious metals (gold, silver, platinum), which would later bring profit as a result of trading. However, the purchase certificates did not reflect the actual purchases made, and the company did not undertake any actions aimed at making profit.

The identified predicate offence was fraud in a scheme called the "pyramid on the financial market", forgery of documents and use thereof and presenting false data. Collected funds were then laundered by multiple transfers between bank accounts held by AG Ltd and other entities belonging to the „AG Group” as well as to natural and legal persons. The transfers were mainly made to a German-based company operating in the aviation sector (PLN 299 306 556 / €65 847 442). They also covered current operations of the AG Group (PLN 212.165.276 / €46 676 360), consisting mainly in purchasing of real estate, vehicles, computer software, paying employees' salaries, taxes, advertisement payments and donations.

In 2019, two persons were sentenced. The first was sentenced to 15 years of imprisonment (out of which 8 years for ML), a fine of 530 daily rates of PLN 300 (€66); while the second was sentenced to 12 years and 6 months of imprisonment (out of which 4 years for ML), a fine of 450

daily rates of 300 PLN (€66). Both were banned from running a business for ten years, with an obligation to restore damages. No forfeiture measures were applied.

226. Based on the country's risk profile and the perception of the authorities, drug-related criminality is a major concern, both as a transit country and a source of synthetic drugs. The country still must develop a comprehensive understanding of the proceeds of drug crimes (especially the local production), which would enable the authorities to arrive at reliable estimates and take targeted action for tracing and disrupting related financial flows. This is important because of the significant amounts of physically seized drugs and the non-estimated amounts that potentially remain undetected (see also IO.1).

227. There is still a gap between the number of convictions in drug-related crimes and the drug-related ML investigations (see Table 3.23), but proportionally, in the overall number of ML investigations, the drug-related predicates are ranked in high positions. On a less positive side, the authorities were unable to provide examples of ML convictions (nor investigations for that matter) connected to domestic drug production proceeds.

228. According to the authorities, the recent ML drug-related investigations indicate a shift in the modus operandi by means of post parcels, bank transfers and use of cryptocurrencies, which implicates the need to investigate the role of the alleged money launderers who were not involved in committing the drug crime. The AT was provided with one such case at the stage of investigation, which is a positive outcome, but no actual convictions have been achieved at this stage.

229. ML cases investigated and prosecuted do not adequately reflect the cross-border risk. The detection of undeclared cash results rarely in ML investigations, and a generally low level of proactiveness in this was observed. As a result, there appear to be missed opportunities to investigate ML in relation to cross-border cash, even in cases where ML suspicions were present (see the description under Core Issue 7.1). Nevertheless, as a recent positive development, the authorities presented a case example of ML investigation in relation to a large amount of undeclared cross-border cash, which were seized. The investigation and the information received as a result of international co-operation via Europol indicate that the potential illicit source of cash is criminal activity connected to smuggling, human trafficking and tax evasion.

### ***3.3.3. Types of ML cases pursued***

230. Effective results in the prosecution are achieved mostly in self-laundering cases and third-party ML cases. No "professional ML" convictions were reported apart from one ongoing investigation (see BOX 8 under IO2). Although the numbers remain behind the ones achieved for self-laundering, a positive trend can be noticed on stand-alone ML convictions (7 convictions in 2014, compared to 18 in 2019).

#### **CASE BOX 3.2. - The Phishing case – Cyberattack fraud (Third-Party ML)**

The investigation covered the activity of an organised criminal group that operated in Poland between 2011 and 2016. Some of the suspects were charged with third-party money laundering since they were not involved in any underlying predicate offence.

The investigation covered the participation of 14 Polish citizens in an organised criminal group committing crimes against property, mainly breaching IT security, breaking into the electronic banking systems and stealing funds. The proceeds of crime were then laundered by electronic transfers to accounts opened in Poland and other EU countries and controlled by the group members, and subsequently withdrawn in cash. Then, the cash was transferred to non-EU countries via money remittance services.

The underlying predicate offences were identified by Polish banks, which received information from foreign banks about unauthorised transactions made on the victims' accounts.

In 2019, all suspects were sentenced to imprisonment for a period ranging between 1 and 3 years, with fines ranging from PLN 1 000 to 12 000 (€220 to €2 655).

For 12 out of the 14 perpetrators, the court ordered the forfeiture of the proceeds of crime amounting to between PLN 100 to 30 000 (€22 to €6 630).

231. The analysis of the statistics indicates a significant increase in ML cases connected to foreign predicate offences (nil in 2014, compared to 23 in 2019), which is a positive development (see Table 3.27). However, when looking at the volume of the international co-operation requests and the geographical position of the country, more emphasis is expected to be placed on this category.

**Table 3.27 Convictions by type of ML**

	Total number of ML convictions (persons)	Self-laundering (%)	Third-party laundering (%)	Stand-alone laundering (%)	ML connected to a foreign predicate offence (%)
2020	N/A	N/A	N/A	N/A	N/A
2019	123	66 (54%)	39 (31%)	18 (14%)	23 (19%)
2018	160	126 (79%)	23 (14%)	11 (7%)	21 (13%)
2017	234	201 (86%)	18 (8%)	15 (6%)	53 (23%)
2016	251	222 (88%)	17 (7%)	12 (5%)	14 (6%)
2015	123	82 (66%)	29 (24%)	12 (10%)	2 (2%)
2014	121	109 (90%)	5 (4%)	7 (6%)	0 (0%)

232. At the pre-trial stage, self-laundering is the most prevalent form of ML in practice (cc. 50-60% of the cases), but other forms (third-party and stand-alone ML) are also present, in varying proportion (see Table 3.28).

**Table 3.28 Investigations by type of ML**

<b>Types of ML investigations</b>	<b>Total new ML investigations</b>	<b>Self-laundering (%)</b>	<b>Third-party and Stand-alone laundering (%)</b>
2020	N/A	N/A	N/A
2019	156	99 (63%)	57 (37%)
2018	128	75 (59%)	53 (41%)
2017	126	59 (47%)	67 (53%)
2016	76	32 (42%)	44 (58%)
2015	109	56 (51%)	53 (49%)
2014	102	49 (48%)	53 (52%)

233. The majority of ML investigations and prosecutions are tied to their predicate offences. In this respect, reportedly, the high evidentiary standard in relation to the underlying predicate offence poses impediments in pursuing ML cases. This is confirmed by the high proportion of discontinuations and acquittals (the number of the decisions on discontinuation of ML investigations is almost the same as the number of ML indictments; the number of acquittals – almost 10% of the indictments). According to the prevailing court interpretation, the predicate offence must be proven to the exact legal qualification; thus, the unspecified criminal origin or behaviour is not considered enough basis for a conviction for ML. Also, the actual connection of the illicit assets to the predicate crime has to be proven, e.g., in a drug trafficking case, the trafficking, the amount of drugs and the amount of illicit gains from the crime. The Polish authorities claim that these standards set by the judicial practice do not impede ML prosecutions, although this is not reflected in the achieved results.

234. Notwithstanding the above, there are examples of the courts stepping away from the high evidentiary standards, but this jurisprudence is usually connected to foreign predicates investigated abroad (see Case Box 3.3).

#### **CASE BOX 3.3 - The French case – (Autonomous ML)**

The case was initiated based on a notification to the Prosecutor’s Office by a commercial bank. In fact, the commercial bank received a request from a French commercial bank for the return of funds in the amount of €196 000, which had originated from a phishing offence and had been transferred to the account held by the Polish company at the Polish commercial bank and later transferred to the account of a Chinese company, in China. Four days later, another request was made by the French commercial bank regarding the return of funds in the amount of €227 166. The funds were returned to the applicant before being credited to the account of the Polish company. On the same day, another transfer was made to the account of the Polish company in the amount of €292 700 originating from another French commercial bank. Based on suspicions that the account of the Polish company was being used for phishing offences, the Polish commercial bank blocked the account (June 2014). In September 2014, the applied measures were waived, and the funds in the amount of €292 700 were returned to the account of the French company.

To prove the illegal source of the money, the Polish LEA used a notification from the French authorities certifying that the transfer was undue and the operation was a fraud. The Polish

judges accepted the evidence. One person was convicted for aggravated ML and sentenced to three years imprisonment in 2018.

235. According to the PPO, the length of the investigations in ML cases can expand to several years. Although the investigation phase's initial 3-month limit can be extended by the prosecutor (and further on by the senior prosecutor), without an absolute maximum, these cycles of extensions and the need for justification thereof puts a certain pressure on the authorities. In complex, time-consuming cross-border cases, especially if the ML aspect has been included only at a later stage of the investigation, this might also lead to the loss of evidence and thus to discontinuation of the criminal proceedings.

236. The number of sentences pronounced by the Polish courts is consistently only about half of the filed indictments per year, which indicates a cumulating backlog and obstructs the development of jurisprudence concerning ML.

237. The lingering technical deficiencies on the criminalisation of ML (see R.3) may have an impact on the legal practice, although some appear to have been addressed. For example, with regard to the potential limitations of the wording laundered property (the illicit assets '*obtained from the benefits derived from a committed prohibited act*'), the established interpretation of the Supreme Court enables indictments/convictions concerning direct gains obtained from the predicate offence in self-laundering cases. On a less positive note, the over-restrictive result-based intentional element requires additional efforts from the authorities. This may potentially impact the ability to effectively pursue ML cases and achieve convictions, as the *lack of criminal intent* is among the main reasons for the high number of discontinuations and acquittals. Apart from the technical deficiencies, the system would benefit from the incrimination of the negligent form of ML, which would prevent situations in which the absence of enough evidence to substantiate, with high certainty, the criminal intent would lead to the discontinuation of the criminal proceeding.

#### ***3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions***

238. Money laundering is punishable by up to eight years of imprisonment pursuant to the Criminal Code. A maximum prison sentence of ten years is foreseen for aggravating money laundering. The maximum sentence prescribed for ML is proportionate to other economic crimes, e.g. fraud - eight years, corruption - eight years (aggravated corruption, up to 12 years), embezzlement - three years (aggravated embezzlement, up to ten years).

239. The courts determine the appropriate sentence based on the individual facts of the case considering both the seriousness of the offence and the personal circumstances of the offender. The sentences are based on a wide range of elements relevant to each individual case, and do not always record what effect the ML activity specifically has on the final penalty. It is therefore not always clear the extent to which conviction for ML leads to an additional sanction.

240. The penalties imposed in ML cases since 2013 have gradually increased, and now the range of sentences passed for money laundering prosecutions has included more custodial prison sentences instead of fines. Nevertheless, they often remain in the lower range of punishment which is not fully dissuasive.

241. In practice, the minimum prison time imposed is systematically six to eight months. Starting 2018, in some of the major cases, more dissuasive sentences have been applied (nine years imprisonment in one case).

242. The average prison time imposed in ML cases in 2018 and 2019 was one year and six months and one year and five months of imprisonment, respectively, which is a slight increase from the previous period (e.g. one year and two months in 2017). Looking at the average of prison time pronounced in ML cases, coupled with the minimums and the harshest penalty, the AT concludes that the sentences can be, and at least sometimes are, imposed in a proportional manner. Imprisonment sanctions are accompanied by fines and forfeiture of benefits of the crime, instrumentalities or substitute value.

243. The sentences for ML can be an important factor underlying the decisions on whether there is value in prosecuting offenders for money laundering, in addition to pursuing prosecution for predicate offences. In many cases, the LEAs see a greater impact from the penalties applicable to the predicate offences, and the general mindset is that ML has little added value in this respect.

244. There are no sanctions applied against legal persons in ML cases, although, according to the opinions expressed by the authorities, in financial crime, tax crime and fraud, the perpetrators almost always exploit the involvement of legal entities. According to the Polish authorities, the reason for this is that these legal entities are almost always shell companies with no assets and legal activity. Polish authorities also indicate that legal entities which were used in criminal conduct are routinely stripped of their VAT registration in an administrative procedure of the KAS, effectively rendering them useless for further activities. According to their perception, this sanction ensures that the ranks of legal entities are kept as clean as possible. The available data indicates that, between 2017 and 2020, more than 415.000 entities (individuals and legal persons) were deleted from the VAT register. Nevertheless, the lack of any convictions for legal persons cannot demonstrate that effective, proportionate and dissuasive sanctions are applied.

### ***3.3.5. Use of alternative measures***

245. According to the authorities, Poland considers applying alternative criminal measures in cases where an ML investigation has been pursued but where it is not possible, for justifiable reasons, to secure an ML conviction. Initially, reference was made to forfeiture measures applied on the basis of a ruling on conditional dismissal of proceeding (e.g. death, insanity or other substantial criminal law or procedural law obstacles). During the onsite visit, the authorities mentioned that, in practice, when ML offence cannot be included in the indictment due to justifiable reasons, they prosecute for other offences. Nevertheless, this has not been demonstrated by case examples or relevant statistics.

### ***Overall conclusions on IO.7***

246. Poland has a broad range of LEAs, but none are designated with specific responsibility to investigate ML, which impacts their appetite to venture into an ML investigation. Overall, ML cases are not fully prioritised, and the number of ML investigations remains behind the number of convictions for proceeds generating predicate 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 several 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 were not fully effective and dissuasive, but the practice proved proportionality.

**247. Poland is rated as having a Moderate level of effectiveness for IO.7.**

### 3.4. Immediate Outcome 8 (Confiscation)

#### *3.4.1. Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective*

##### ***Policy through legislation/procedures***

248. Although LEAs have achieved some results, especially in cases of ML, the confiscation of criminal proceeds, instrumentalities and property of equivalent value is not pursued as a policy objective. This is supported by the lack of comprehensive statistics on the seized, confiscated and recovered property. This aspect was not considered in the context of the NRA and impacts the ability of the AT to assess the effectiveness of the system.

249. At the strategic level, the new AML/CFT strategy (2021) does not envisage any priority related to the confiscation regime. The Polish authorities argue that the AML/CFT Strategy in Priority VI targets to enhance the *“rules for generating statistical data needed to evaluate the effectiveness of the national AML/CFT system”*. However, this pertains only to keeping statistics, not to the confiscation regime as such. In addition, due to the recent adoption of the Strategy (during the onsite visit), its content has no impact on effectiveness.

250. Seizure and confiscation, in theory, are defined objectives and - through to the legality principle-based criminal procedure - a legal obligation in the ML cases and criminal procedures in general (Art 297 CCP and Art 202 of the Rules on internal procedures of the PPO (RIP)). In ML cases, forfeiture of benefits and indirect gains from an offence is mandatory according to Art. 299 para 7 and Art. 44 of the Penal Code, and the court may give detailed explanation on the grounds of the judgment. The confiscation of instrumentalities has a discretionary character. In case there is a victim of the crime, reparation takes precedence.

251. Since 2017, the CC features extended forfeiture (Art 45 para 2 and 3), which makes it possible for the court to confiscate elements of property if the perpetrator gained benefit even indirectly from a more serious offence (at least five years imprisonment upper limit or organised crime or benefit of significant value) based on a presumption that any asset obtained in the five years before committing the offence was illicit. Any such asset transferred to third parties can be subject to forfeiture as well. The scope of this legal instrument is fairly broad, and authorities claim to apply it, especially in drug-related cases. However, there is no policy level mechanism to incentivise the LEA or prosecutors in applying this tool. The PPO informed that an order was issued in March 2017 requiring prosecutors to pay special attention to the issue of forfeiture envisaged by Art. 45 of the CC. Nevertheless, the Polish authorities did not demonstrate how often extended forfeiture is used in practice and whether it has been applied in ML cases.

252. Although in April 2017, a special form of confiscation was introduced to the CC, namely the forfeiture of an enterprise (in case the perpetrator directly or indirectly obtained material benefits using the enterprise), its application is still discretionary. The authorities maintained that such confiscation has been ordered by the Courts in some cases, but there is no data on the number of instances, value of assets, or crime(s) for which it was applied.

253. A significant policy-level difficulty resides in the fact that the temporary seizure of the suspect's property is not mandatory. The temporary seizure is applied only in cases where the LEA can establish a risk of removal of assets, which conduct may impede the execution of the fine, forfeiture or other monetary sanction imposed in the final judgment. For the LEAs to apply a temporary seizure, the prosecutor must take the formal decision on property securing, and the

decision can be appealed in court. This puts an unnecessary burden on the LEAs and dissuades them from the timely application of the provisional measures, a conclusion confirmed by the weak results obtained in terms of actual seizures and confiscations achieved in Poland globally, as described under the Core Issue below.

### ***Methodological tools and institutional measures***

254. The legal provisions on provisional measures and confiscation have been supported since 2018 with the Methodology on the seizure of property (hereafter the Seizure Methodology) developed in the context of the “Program for preventing and combating economic crime for 2015-2020” and supplemented by other guidelines issued by the PPO. While most of the guidelines focus on specific types of criminality (e.g., financial crimes, fraud, tax offences), the one issued on 31 March 2017 addresses the asset recovery topic, reinforcing the obligation to apply any means to deprive the perpetrator of illicit assets, instructing prosecutors to require the LEAs to do an in-depth search for these. While the adoption of such methodological tools is commendable, the limited results obtained in terms of asset recovery suggest that those remain optional and no control or peer pressure measures have been put in place to enforce their application (e.g. including the asset tracing/recovery in the yearly appraisal of prosecutors LEA, monitoring of preventive measures imposed etc.).

255. The Seizure Methodology appears to be a comprehensive document, including a description of activities preceding the issuance of seizure orders (such as collecting data on assets) and activities aimed at determining the property profile of the suspect. It contains a description of the information detained by GIFI and modalities of obtaining it. To improve its content, the authorities already conducted an updating process led by the PPO and comprised of prosecutors, judges, representatives of LEAs and ministries, to include the extended confiscation, forfeiture of an enterprise and to give guidance on the practical aspects of seizing cryptocurrencies. Nevertheless, at the time of the onsite visit, the revised version was not available.

256. According to the PPO, in order to respond to the emerging trends concerning cryptocurrencies, the Seizure Methodology was updated, aiming to strip the perpetrator of access to the wallets and convert cryptocurrencies into FIAT money, and such, to channel the assets back to traditional procedural steps. There is no specific legislation on these procedures yet, and the AT was not presented with case examples to demonstrate the practical application and the broad interpretation of the legal provision (“items”), which would include the virtual assets.

257. There are further plans to update the Methodology, which will also take into consideration the new EU rules on freezing orders.

258. Although available, not all LEA met on site were aware of the content of the Seizure Methodology nor used it systematically in their work which negatively impacts effectiveness.

259. In December 2008, following the EU Council Decision 2007/845/JHA, the National Assets Recovery Office (ARO) was established at the HQ of the National Police with the aim to serve as the only contact point for international exchange concerning asset recovery, facilitating the tracing and identification of proceeds of crime, using the Europol SIENA channel within the EU, CARIN channels in the Camden Network. Beyond this mandate, ARO provided trainings on asset recovery to field units and, in some large cases, performed actions concerning asset tracing.

260. In April 2019, in addition to the central ARO office, permanent Regional Asset Recovery Units and Teams were established at the Voivodship Police HQs’ Economic Crimes Departments

for the purpose of operatively supporting police investigations. According to the information provided by the Polish authorities, at the time of the onsite visit, the personnel of the structure was a total of 91 officers, of which ten are allocated in the National Police Headquarter (central ARO). Due to this rather limited capacity, the main activity of the ARO structure is coordination and counselling, and to a limited extent, in some cases, operational support. Prosecutors are not satisfied with the ARO's activity and want it to be more oriented towards parallel financial investigation, assets tracing and recovery.

261. Parallel to the above structure, the commander of the Police Central Bureau of Investigation (PCBI) on 26 June 2019 issued an internal order to streamline and coordinate PCBI's own efforts in the field of disclosure and securing of property within the PCBI. As a result, 70 coordinators at the central and local levels were appointed, dealing with the disclosure and securing of property (assistance in complex cases, conducting trainings, issuing opinions on documentation in connection with the co-operation with the GIFI, etc.).

262. Next to the Police, KAS plays a significant role in seizing and securing assets. Since April 2019, the KAS took the policy measure to establish designated asset recovery units with a central and 15 regional Centers for Tracing and Asset Recovery (CUOM). CUOM has a task to support asset tracing and recovery efforts of KAS units but also serves as an international co-operation unit as well in tax and customs-related matters.

263. Based on the Polish Tax Ordinance Act, as a result of risk analysis, including the suspicion of tax fraud, with the aim of securing tax income, the head of KAS can block a bank account for 72 hours which can be extended up to three months.

### ***Policy through practice***

264. Since April 2017, through amendments to Police Act and the Internal Security Act, the LEAs – next to the various relevant databases and registries – was given broad access to property-related databases, including banking, tax or other professional secrecy protected ones, where they can collect information on the property status of the person under investigation. At the request of the LEAs, the holder of such secrecy-protected data (e.g., financial institutions, tax authorities) must disclose them. Institutions, governmental or municipal bodies and entrepreneurs active in public services are obliged by the law to comply with these requests. The exchange flows on electronic channels seem to be an effective step to speed up asset recovery efforts, especially in financial crime areas. In the case of a 'hit' in the databases, the LEAs take steps to temporarily seize the assets, with all the procedural burden as described above, as an obligatory judicial decision must be obtained to secure the asset.

265. In asset tracing, the LEAs routinely use information from GIFI and conduct analysis of cash flow and turnover of assets, check the registers, in some cases try to obtain additional background information from informants, and since 2017, they are allowed to use special investigative techniques for asset tracing as well.

266. In practice, and as described under IO6, an important part<sup>51</sup> of the GIFI notifications to LEA is unrelated to ML/TF suspicions and pursues mostly investigation and prosecution of predicate offences, which is still relevant for this Immediate Outcome. In addition to various sources of information available under respective sectorial laws (e.g. the Police Act, the Anti-

---

<sup>51</sup> On average 71% to 83%

Corruption Bureau Act, etc.), all law enforcement agencies<sup>52</sup>, as well as the PPO, the KAS, the UKNF and the Supreme Audit Office may obtain from the GIFI information based “*on a written and justified request*” made in the scope of the statutory duties and competences of the mentioned bodies and agencies. Although not formalised through a written document, this practice can be considered at policy level as confirmed by the statistics on the use of financial intelligence (see Tables 3.3-3.7 under IO6) and the interviews onsite.

267. The value of seized property seems to be on the rise (in 2019), at least in the investigation phase. The Polish authorities recently started to emphasise asset recovery, and while the amended legal environment supports this, and asset recovery specialisation started to take shape in the major LEAs, the impact of these changes is yet to be seen in practice. The fragmented nature of statistical data gathering on asset seizure and recovery hinders the Polish authorities from demonstrating the actual effectiveness of the current system in place.

### ***Parallel financial investigations***

268. LEAs could not demonstrate a comprehensive perception of the relevance of parallel financial investigations, which are not considered as a separate, specialised item, but more a part of the “regular” investigations. While this approach may not be problematic, treating the financial part of the crime as any other component points to the absence of financially specialised investigators/analysts. Another fact that indicates the lack of effectiveness of this “integrated approach” is the recent and repeated attempt of the Polish authorities to create specialised units (ARO, CUOM, property securing coordinators within the PCBI) for assets tracing/recovery.

269. Apart from the Seizure Methodology, there are no measures taken at the policy level to encourage LEA and prosecutors to conduct financial investigations and to pursue the proceeds of crime systematically and as a matter of priority. The lack of focus on the detection and securing of proceeds of crime in the pre-investigative proceedings, together with the absence of *de facto* support to pursue financial evaluations from a dedicated agency, leaves the AT unconvinced that confiscation is pursued as a policy objective in Poland.

270. The AT has not seen any parallel financial investigations so far in relation to TF cases (see under Immediate Outcome 10).

### ***3.4.2. Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad***

271. It must be mentioned from the outset that the depth of the analysis under this Core Issue is seriously affected by the lack of statistical data, as the AT was not given any meaningful information as to what criminal offences have been represented in the statistics on the performance of the confiscation and provisional measures regime, whether there were measures taken against proceeds located abroad, to which extent instrumentalities or equivalent value were confiscated etc... There was a general and absolute lack of information regarding the confiscations, while only partial figures were provided in the area of the provisional measures, which were too fragmented to draw substantiated conclusions. The analysis below is based on and structured according to the type of data available.

---

<sup>52</sup> Including the Police, the Military Police, the Border Guard, the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence Service, the Central Anti-Corruption Bureau, and the Internal Supervision Inspector.

272. On the positive side, the legal framework on provisional measures and confiscation of proceeds of crime and instrumentalities has been improved since the 2013 evaluation. The new provisions enable the confiscation of instrumentalities even if they do not belong to the offender and of the enterprise used for the commission of a crime. Some of the measures still have a discretionary character (confiscation of instrumentalities), which may impact the effectiveness, while other provisions fall short of the standard (inability to confiscate all types of property, i.e. intangible assets). Regarding the latter, the AT was informed that the judicial practice adopted a broad interpretation of the legal provision to encompass virtual assets. Nevertheless, the assessors were not presented with the respective Court decision and hence, are unable to confirm this statement.

**Table 3.29 Seizures and Confiscations in ML cases**

	Property seized (€)	Number of cases	Property confiscated <sup>53</sup> (€)	Number of cases
2020				
2019	383 232 977	172	9 432 780	31
2018	84 094 702	129	22 769 508	50
2017	117 846 700	N/A	23 112 585	68
2016	49 344 055	75	16 055 128	48
2015	65 818 610	71	9 327 510	33
2014	84 470 385	81	1 793 697	12

273. When looking at the overall value of the table above, a positive conclusion can be drawn on the effectiveness of the system in ML cases, as in some years, notable sums appear to have been confiscated (2017 and 2018). Nevertheless, the AT was not provided with statistics on the assets actually recovered. Another disturbing finding was that only in about half of the total ML cases year by year were confiscation measures applied (e.g. 65 ML convictions were pronounced in 2019 (see Table 3.1. under IO7), while in the same year, confiscation was imposed in only 31 cases). This means that in 34 ML cases, no confiscation measure was imposed whatsoever.<sup>54</sup>

274. An increasing trend can be noted between 2014 and 2017, with a stable level sustained in 2017 and 2018. A significant decrease is observed in 2019. This was explained by the authorities as a mere coincidence whereby that year, the courts simply heard cases in which less property had been seized at the stage of the investigation. The AT encourages the authorities to consider such strategic analyses more carefully to identify trends and features that may lead to better or poorer results in specific circumstances.

275. During the preparatory proceeding in the fiscal-penal cases, the KAS is seizing and secures assets in a steadily growing value, while statistics on applied forfeiture only exist because the 'prosecution' is also done by KAS itself. The figures show a tendency that the share of tax crimes connected to asset recovery by KAS decreased from 2015 to 2018 from 98% to 72%, with a slight increase again to 78% in 2019.

<sup>53</sup> On the basis of courts' decisions of first instance. No data on the actually recovered property.

<sup>54</sup> In 2020, in 38 ML cases out of the 88 ML convictions, no confiscation measures were imposed.

276. However, the applied forfeiture as a sanction in fiscal penal cases seem to be very low in comparison, with 6, 2 and 2 % in value of the total secured assets in 2018, 2019 and 2020, respectively. The reason for this wide gap between secured and forfeited assets is unclear, as the Polish authorities did not provide an explanation on the outcome of more than 90% of the secured assets in these cases.

**Table 3.30 Seizure and forfeiture in KAS cases**

	Value of seized/secured assets (in PLN)	Percentage of assets secured in connection of tax crimes	Forfeiture applied by courts in fiscal penal cases	Percentage of assets forfeited to secured assets
2020	236.726.380	N/A	5.363.794	2%
2019	319.916.579	78%	7.782.938	2%
2018	160.842.822	72%	9.526.623	6%
2017	129.011.321	71%	N/A	
2016	108.840.846	78%	N/A	
2015	109.488.915	98%	N/A	

277. On the other hand, instead of or in addition to forfeiture, fines are also applied to a much higher number in penal and fiscal-penal cases prepared by KAS. There is no breakdown to the nature of crimes in question, but from the above figures, it can be subsumed that the majority has been tax crimes. It is also not clear whether these fines are enforced from the secured assets.

**Table 3.31 Applied fines in penal and fiscal penal cases**

	Total amount of fines (in PLN)	Number of convicted persons	Average amount of fine (in PLN)
2020	104.978.106	23782	4414
2019	240.378.307	37343	6437

278. The Border Guard seizes illicit assets they encounter during their activities; the value of secured assets between 2014 and 2021 varies between PLN 2.8 million (€0.6 million) and PLN 137.6 million (€30.2 million) per year. Due to the nature of their competence, the fluctuation is natural, as a single significant case can have a major impact on the data. The fact that in 2019 the Border Guard seized a value of about 40% of the seizure of KAS in the same year is an achievement, even if it can be attributed to one case.

279. There was no data made available to the AT on the asset recovery results of the other LEAs.

280. The courts order forfeiture to a high number and value, with the majority applied to financial gains. The Polish authorities presented statistics only on first instance court decisions and only for 2020.

**Table 3.32 Forfeited assets in 2020**

<b>Data on forfeiture 2020, first instance courts</b>	
Number of cases	30 195
Number of persons subject to forfeiture	33 739
Value of forfeiture ordered (in PLN)	442 596 217 (€97 371 167)

281. The execution of forfeitures applied by the courts' decisions is a task of the KAS enforcement offices and is considered a negligible part of their portfolio. The enforcement is carried out in an administrative procedure; in 2020, the KAS fiscal offices received 9 610 judgments brought in criminal cases for execution of forfeiture, of which 5 047 were executed in an average timeframe of 90 days. It is not clear how the rest of the pronounced forfeiture orders are handled if only a third of the judgments are forwarded for execution to KAS. There are no specific statistics on ML cases.

282. Overall, Poland has not demonstrated how much of the seized assets were actually confiscated. The data kept by the Ministry of Justice on the total value of the confiscated assets regards only the decisions of the first instance courts (not final decisions). In relation to the *de facto* recovered property, it appears that no aggregated data is maintained by the KAS, which is in charge of the administrative execution of the court decisions, including those on forfeiture.

283. There is no single mechanism for managing/disposing of seized or confiscated property and no centralised authority in charge of management of such property, which negatively impacts the effectiveness.

#### ***3.4.3. Confiscation of falsely or undeclared cross-border transaction of currency/BNI***

284. 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 (e.g. 216 convictions in 2020, with the amount of imposed fines of PLN 514 332 / €113 153). Still, the regime has not demonstrated its effectiveness for detecting ML/TF-related cash/BNIs.

285. Cash-control is only established at the non-EU borders (Ukraine, Belarus and Russia), plus in the international airports. The declaration threshold is €10 000. There is no mechanism available to counter cash couriers entering through the EU internal borders.

286. There are no statistics available on the confiscations of false or undeclared currency or BNI, hence the AT based its analysis on case studies and on discussions held onsite with the responsible agencies.

287. In practice, the main sources of influx of declared cash are Ukraine and Israel. The explanation provided by the authorities for this trend is that Ukrainian citizens use the cash to buy goods in Western Europe (e.g., used cars, mobile phones), which will then be taken back to Ukraine. Concerning Israel, the authorities maintain that Israeli citizens arrive with cash in different foreign currencies, exchange these into PLN and/or purchase luxury goods, then return to Israel on the same day. The supposed rationale beyond this currency exchange tourism is the favourable difference in the exchange rates. No ML suspicion has been raised in these cases. While not contradicting the authorities' conclusion, the AT is of the opinion that there are

unexplored areas of risk related to this type of cross-border movement of cash that need more attention from the responsible bodies.

#### **CASE BOX 3.5. – The fake diplomatic passport case**

In 2018 the Border Guard authorities identified a person travelling from Dubai into Poland who declared carrying cash in value of over €330 000 in various currencies (PLN, CHF). The search performed on the person revealed several luxurious goods (watches, shoe wear). A closer inspection of his documents revealed a fake diplomatic passport. The subsequent investigation concluded that his main activity was buying luxurious goods for re-selling and that he was a frequent traveller. As a result, the penalty in the form of a fine was applied for non-declaration of the luxury goods. The rest of the money/goods were released back to the person.

288. Undeclared cash is handled according to the provisions of the penal fiscal code, resulting in a fine. The proportion and volume of fines imposed seem to be very low, their dissuasiveness being questionable. In cases of detected false or non-declaration, the restrained assets concern only the equivalent value of the fine for the fiscal crime and the remaining assets are returned, even in cases of suspicions of ML (see case boxes 3.5 and 3.6.). Only a few ML investigation has been started based on undeclared cash.

#### **CASE BOX 3.6. – Undeclared cash**

The Polish authorities discovered undeclared cash (€12 000) on a traveller from China to Poland. As a result, they initiated fiscal and criminal proceedings. There were well-grounded suspicions established in relation to the person: he indicated the source of money as “gains in a casino” but was unable to produce any justification/document, the other goods he possessed were cheap, and the investigation also revealed that his main activity was selling goods in a third country (not the country of origin nor Poland). His activity involved a frequent cross-border movement of cash. The result of the investigation was the application of the fine for non-declaration. The rest of the money was released back to the traveller. The GIFI was informed about the case in compliance with general reporting obligations. No follow-up measures were taken.

289. The total and the average value of fines (approx. €500 on average in the last year) seem to be insignificant in comparison to the value of undeclared cash, which is clearly not proportionate and dissuasive. This is a particularly significant shortcoming, especially in light of the NRA, which identified cross-border cash movements as one of the main concerns. Also, according to the figures, the majority of undeclared cash stems from only a few cases with more than €50 000 (23 in 2018, 22 in 2019 and 15 in 2020), which points to large sums being moved through the Polish border unreported.

**Table 3.33 Fines imposed on undeclared cash transporting**

	Number of cases	Total amount of unreported cash in PLN	Total amount of fines in PLN	Average fine per case in PLN	Percentage of fines to the value of unreported cash
2020	216	16 142 020	514 332	2 381	3%
2019	366	36 491 326	582 935	1 593	1.6%
2018	197	24 267 857	431 070	2 188	1.7%
2017	150	71 523 296	292 000	1 947	0.4%

290. Concerning cash couriers, the LEAs treat the phenomenon as an indication of ML with unknown predicate offences, which connects with the issues raised in IO7. Although Poland has participated in the European Money Mule Actions (EMMA) organised by Europol since 2017, there is no data on how the results were taken into account to start and conclude ML investigations. According to the reporting tables, perpetrators acting as money mules, organisers, move of funds through bank accounts have been identified in a higher number; this is not reflected in ML investigations.

291. The overall lack of data prevented the Polish authorities from demonstrating the effectiveness of the cash/BNI control system, and the available data raises concerns about its usefulness.

#### ***3.4.4. Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities***

292. The number of decisions on seizure of property and the value of the seized property significantly increased in 2019, compared to the previous years (€877 mln in 2019, compared to €245 mln in 2018 or €286 mln in 2017). This illustrates the efforts of the authorities to seize ill-gotten assets. However, these figures are low when compared to the estimated proceeds of crime laundered in Poland. Additionally, in the absence of the breakdown of data on seizures and confiscations for specific predicate crimes, the AT is not in a position to assess if these measures are in line with the main ML threats and risks.

293. The NRA identified risks are based on law enforcement experiences, typology of cases and assets they encounter in actual cases. As already expressed under other IOs, there is no data on the damages caused by crimes or the volume of actually laundered assets, and the authorities indicated that they do not collect such data. The NRA estimates the volume of laundered assets as high as cc. 1% of the GDP, which would amount to 22 billion PLN (6 billion US\$) as of 2018. At the onsite visit, both GIFI and KAS stated that this figure is a realistic estimation.

294. In comparison, the secured and forfeited assets' overall volume is dwarfed. Due to the lack of comprehensive statistics, the AT could not establish an overarching conclusion on the efficacy of the system and on how aligned the practice is with the NRA and major proceed generating crimes. The absence of statistics also indicates the lack of an internal strategic analysis on the effectiveness of the entire repressive system through the deprivation of criminals of illegally acquired property.

295. The KAS, partly due to its extended powers to 'prosecute' fiscal offences directly, is an important factor in asset tracing and recovery. The value of assets seized in fiscal-penal cases is

steadily rising, with a vast majority coming from tax-related crimes. On the other hand, the value of confiscated assets based on these measures remains low. (See Table 3.30 Seizure and forfeiture in KAS cases above)

296. There is no established system to preserve and manage seized assets other than the provisions of the Criminal Procedure Code and the Rules of Internal Procedure of the PPO, which is based on the nature of the seized items (e.g., evidence, prohibited items, objects of artistic or historical value, perishable objects, etc.).

### ***Overall conclusions on IO.8***

297. 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 the predicate offences, which negatively impacts the authorities' ability to assess the effectiveness of the system and to take targeted policy measures to address the weaknesses. There was a general lack of information regarding the confiscations (except for ML), while only partial figures were provided in the area of the provisional measures, which were too fragmented to draw any positive conclusion. There is a total absence of information on assets actually recovered. In cases of detected false or non-declaration, the restrained assets concern only the equivalent value of the fine for the 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. **Poland is rated as having a Low level of effectiveness for IO.8.**

## 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

### 4.1. Key Findings and Recommended Actions

#### ***Key Findings***

##### ***Immediate Outcome 9***

- a) The Counter Terrorism Centre of the Internal Security Agency (CTC-ISA) is the main LEA responsible for identifying and investigating TF cases, which in practice are exclusively conducted in connection with a terrorism offence. Two convictions of four individuals were achieved in the assessed period. 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, as explained under 9.1.
- b) The prosecution and LEA did not adopt methodological guidance or instructions for TF investigations, nor did they develop a system to prioritise all potential TF cases. The AT is concerned about the general understanding and prioritisation of TF among the responsible institutions, which might create blind spots in the system.
- c) TF investigations are conducted and supervised by the specialised Local Divisions of the Department for Organised Crime and Corruption of the Public Prosecutor's Office. In the case of the convictions achieved so far, the TF consisted in the collection and movement of funds (about €8 500) and other assets (paramilitary equipment), as well as in the use of funds (€200) and other assets (mobile phones, clothes).
- d) The main challenge in effectively prosecuting TF cases, even when financing elements are present, is the impossibility of proving the commission of or the link with a terrorist act. This is an area of concern, especially in the context of the technical deficiencies described under R.5. While in one of the TF convictions, the TF was proved through the membership of the perpetrators to a terrorist organisation, one of the culprits who participated in the financing act was acquitted due to the fact that he was not a member of the said organisation.
- e) TF investigations are not integrated and used in support of national counter-terrorism strategies, as Poland does not have a separate document that would constitute a national anti-terrorism financing strategy.
- f) The sanctions applied 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. Hence, no positive conclusion can be drawn on the proportionality of sanctions.

##### ***Immediate Outcome 10***

- a) The Polish TF TFS system is a combination of solutions and legal provisions provided at the domestic and EU level. Under the national designation regime, the competence to identify and propose persons to the relevant United National Security Council (UNSC) committees is given to the Financial Security

Committee, a collective body composed of 23 authorities at the national level, including the GIFI and the ISA.

- b) Poland did not propose any designations to date nor received third-party requests. While this is largely in line with the country's TF risk profile, it must be mentioned that the authorities do not have uniform procedures or mechanisms for identifying targets for designation/listing, de-listing, and granting exemptions. Some authorities, ISA, GIFI would use the same sources as for any investigation/SAR analysis; other members of the FSC were less clear how this would work in practice.
- c) The UNSCRs sanctions lists are promptly published and updated on the FIU's website, where newsletters are also available. Upon subscription, the REs receive prompt notifications on any changes in the lists.
- d) No funds related to TF TFS have been frozen, and no false positives have been reported. This is largely consistent with the country's risk. Guidance has been provided to REs on FT-related TFS by providing e-learning courses on the FIU's website. Nevertheless, the overall communication approach adopted by the authorities is not yet sufficiently targeted.
- e) FIs, particularly in the banking and insurance sectors, have a good understanding of their freezing and reporting obligations, developed their own automated screening systems to check clients and other participants to the transaction against sanctions lists. The awareness of the FT-related TFS obligations of the DNFBP sector varies.
- f) Poland did not carry out a specific risk assessment on the NPO sector's exposure to TF risks. The NPOs are obligated entities when performing transactions in cash exceeding €10 000, which is a risk mitigation factor. The NRA outlines some FT risk scenarios which may concern NPOs, but those are rather general and not connected with the Polish realities. Several controls have been carried out on NPOs since 2016, but they are not conducted risk-based and are rather oriented to technically identify NPOs that are obliged entities and report respective cases to GIFI.

#### ***Immediate Outcome 11***

- a) PF targeted financial sanctions are addressed through EU legislation explicitly to DPRK and Iran, which displays elements of an effective system. The national AML/CFT legislation does not provide PF requirements, and as a result, no supervisory duties are entrusted to any domestic authority or body.
- b) No case of freezing assets has been registered related to the respective UNSCRs, which is largely in line with the country risk seeing the geographical position of the country and their main trade partners.
- c) The trade in special commodities and technologies, such as military equipment, dual-use goods and technologies related to weapons of mass destruction, is subject to control by the state. The Ministry of Economic Development, Labor and Technology (minister competent for economy) is active in the area of export controls and licensing the international trade in strategic goods, thus

participating in a wider mission of counter-proliferation. The FSC and the FIU have no competences in countering PF; therefore, they are not involved in the licensing process, which indicates a lack of coordination and prioritisation at the national level.

- d) The financial sector demonstrated a sound understanding of their obligations under the PF UNSCRs, as well as the necessary steps to be taken to apply the freezing mechanisms. However, the lack of targeted guidance and communication from the state bodies coupled with the lack of supervision shows that PF is not regarded as of serious concern among the authorities.
- e) The DNFBPs have a limited understanding of their PF preventive obligations under the UNSCRs. It appears that insufficient measures are taken to detect funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities.

### ***Recommended Actions***

#### ***Immediate Outcome 9***

- a) The authorities should take measures, procedural, methodological, or otherwise, to clarify that the TF is a stand-alone crime and not a byproduct of terrorism both in terms of risk and criminalisation.
- b) The ISA should be given the authority to investigate TF offences that are not targeting the Polish state's security.
- c) Internal and external EU border cash control mechanisms should be strengthened by providing a legal basis to stop and restrain terrorist and FT suspicious assets administratively (see R32). The identification of such assets should be supported by developing specific indicators and typologies.
- d) Authorities should undertake measures to enhance and formalise the rules for conducting operational activities so that all LEAs properly and proactively consider TF suspicions when needed to avoid TF aspects being overlooked.
- e) Measures should be taken to ensure that financial investigations are carried out not only in terrorism-related cases but also in cases of suspicions about the legality of the funding and/or the destination of funds.
- f) Training and awareness-raising initiatives should be put in place for other authorities (such as prosecution or Border Guard) for them to acquire sufficient knowledge to start and conduct a TF case on their own initiative (e.g. based on an MLA request received from a foreign counterpart or suspicious activity at the border).
- g) The technical deficiencies identified under R.5 affecting the full criminalisation of financing of terrorism as required by the standard should be remedied.

#### ***Immediate Outcome 10***

- a) Provide to all obligated institutions regular training on implementation of FT TFS, emphasising DNFBPs sector.
- b) Conduct a detailed risk assessment of the NPO sector to identify those at risk of FT abuse. The risk assessment process should engage representatives of the NPO sector.
- c) Adopt a targeted risk-based approach to the supervision of the NPO sector.

***Immediate Outcome 11***

- a) A supervisory system on the application of the PF-TFS must be urgently put in place in Poland, which shall include an effective and dissuasive sanctioning regime for non-compliance with the PF TFS requirements.
- b) The authorities should perform trainings and awareness-raising activities in order to enhance the knowledge and understanding of some authorities (Border Guard) and some entities of the private sector (especially DNFBPs) on PF-related TFS obligations.
- c) The authorities should issue guidance for the private sector in the application of the PF UNSCRs.
- d) A domestic coordination mechanism on PF matters should be established to enhance the country's capacities to prevent sanctions from being evaded and to develop and implement policies and activities to combat the financing of proliferation of WMD.

298. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5-8, 30, 31 and 39 and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

## **4.2. Immediate Outcome 9 (TF investigation and prosecution)**

### ***4.2.1. Prosecution/conviction of types of TF activity consistent with the country's risk-profile***

299. The Polish NRA divides the risk of terrorist financing between the “risk on the territory of Poland”, which is based on the terrorist threat itself and estimated as low, and the “overall risk of terrorist financing”, which was estimated to be at the medium level. The NRA<sup>55</sup> recognises the country as an attractive place for logistics bases and the transfer of money and other assets for terrorist purposes; hence it can be assumed that the difference between the two is the external TF risk which brings the “overall” risk from low to medium. As expressed in the Introductory part and in the context of IO1, the AT has reservations regarding the accuracy of the NRA, especially due to questionable methodological tools used.

300. At the operational level, the TF is seen by the authorities as a byproduct of terrorism, somehow linked to it when assessing the risk. Beyond this, the understanding of TF risk is not supplemented by good awareness about purely financial activities of individuals, groups and

---

<sup>55</sup> See page 736

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 to launch TF investigations that would be more consistent with the country's risks.

**Table 4.1. Number of preliminary proceedings carried out by ISA (TA and TF)**

	2016	2017	2018	2019	2020
Terrorist acts	19	19	15	10	8
TF	2	3	5	3	4
Total number of pending cases	21	22	20	13	12
Number of charges related to terrorist and TF preliminary investigations	1	3	2	1	3

301. The ISA is the main LEA responsible for identifying and investigating TF cases, which in practice (and as a result of the understanding of risk explained above) are exclusively conducted in connection with a terrorism offence. In the last seven years, ISA handled three TF cases that ended with indictments. Further on, 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, as further explained below.

**CASE BOX 4.1. - The Caucasian Emirate**

The case was initiated in 2014 by ISA as a result of covered operations. The suspects were Taus G., Zaur G, Alvi Y. and Shamkhan A., foreign citizens who in 2007-2009 came to Poland, where obtained subsidiary protection status (Shamkhan A., Taus G.) or tolerated stay (Zaur G. Alvi Y.).

The four suspects lived in Łomża, where they made contact with the "Salvation" Foundation providing assistance to people from a sensitive community. In 2014, the suspects began to collect funds with the intention of transferring them to Caucasian extremists fighting as mercenaries in Syria. The collection was made among certain nationals by referring to the principles of Islam and the obligation of voluntary alms. Some of the donations came from abroad. The collected cash was handed over to a courier (nicknamed Abu-Askhab), who physically transported it to the war zone through Germany, Austria and Turkey. The funds so transferred amounted to at least €8 500.

In 2014, the perpetrators also facilitated medical care for Vakha K., an Islamic fighter who suffered a gunshot injury in Syria. The suspects enabled his arrival and stayed in Poland and organised an operation to remove a bullet from his chest, after which Vakha K. left for Turkey.

In May 2014, the accused began purchasing commonly available paramilitary equipment (tactical backpacks and headsets) acquired on the internet using the accounts of the employees of the "Salvation" Foundation. They handed over the purchased equipment to their spouses, who sent it to Turkey.

In 2016 the four suspects were indicted with terrorism financing and participation in an organised group with terrorist purpose charges, and the case was sent to District Court in Białystok. In August 2017, Taus G. Zaur.G and Shamkhan A. were found guilty, as the Court established that they provided material support and financing of terrorist acts in their capacity of members of a terrorist organisation. They were sentenced to two years and one month of imprisonment. The Court ordered the confiscation of PLN 1000 and EUR1700 (approximately EUR 1900) due to the financial standing of the perpetrators who did not have any property.

Alvi Y. was acquitted as the Court concluded that although the accused was aware that the money was collected, moved and used to finance a terrorist organisation, the evidence did not conclude that he was a member of an organised criminal group.

The investigation concluded that the Foundation was abused, and no collusion between perpetrators and its employees was found.

On January 16, 2018, the judgment was upheld by the Court of Appeal in Białystok.

302. Some conclusions can be drawn from the two convictions described under Box 4.1 and 4.2 and their consistency with the country's risk. In both cases, the financing part was quite basic, consisting mostly in handling and transportation of cash and a serious/complex parallel financial investigation into TF was not needed/undertaken. The risk related to the physical transportation of cash is well known and understood by ISA and is in line with the country's risk profile. However, this is less acknowledged by other authorities potentially involved in TF cases such as the Border Guard.

303. Turning to investigations, the authorities presented the AT with some ongoing cases that appear to be more in line with the country's risk than the convictions, as they include potential financing of ISIS foreign fighters, use of Hawala system, MTSs and even bank accounts. This suggests an improving understanding of TF risks at the LEA level over time (the ongoing investigations are more recent than the convictions). The investigations also demonstrate the ability of GIFI to meaningfully contribute to an ongoing investigation, although no case is triggered by a GIFI report/dissemination.

#### **CASE BOX 4.2. - The Arson case**

The investigation was initiated by ISA on the basis of a report filed by a third party and concerned Tomasz S., Adrian M. and Michał P., all three supporters of nationalist organisations in Poland.

At the beginning of January 2018, a German journalist, Manuel O. made contact with Michał P. via Facebook and floated the idea to attack a cultural centre of a national minority in Ukraine. Michał P. agreed to this proposal, and Manuel O. sent Michał P. €500 by post. Michał P. recruited Tomasz S. and Adrian M. and gave them PLN 1 000 (€220) to cover the travel expenses to Ukraine, and equipped them with cell phones, SIM cards and clothing. The two travelled to Ukraine through Slovakia.

On the night of 3-4 February 2018, Tomasz S. and Adrian M. went to the building of a national minority cultural NPO, drew a swastika on the facade and set the building on fire. Michał P followed the acts through video. The next day, the perpetrators returned to Poland through Slovakia and met with Michał P., who gave them PLN 1 000 (€220) each as a reward. On February 7, 2018, Michał P. met Manuel O., who gave Michał P. compensation of €1 500 for the acts.

The investigation consisted of interviewing witnesses, searching the perpetrators' flats and securing the content of text messages and conversations. The ISA determined the itinerary of the perpetrators by tracing their cell phones. The Border Guard determined whether and when the suspects were crossing Polish borders.

There was close international co-operation between the Polish and Ukrainian prosecutor's offices, and a JIT was established, enabling evidence exchange without any further formalities.

In March 2020, Michał P. was sentenced to 3 years of imprisonment for TF. The Court also imposed a fine amounting to PLN 15 000 (approximately €3 000) and forfeiture of equivalent benefits of PLN 8 000 (approximately €1 500).

Adrian M. was sentenced to two years of restriction of liberty and obliged to perform unpaid community work. The Court forfeited the equivalent of benefits gained by Adrian M. of PLN 2 000 (approximately €450). Tomasz S. was sentenced to one year of imprisonment and a fine of PLN 4 000 (approximately €900) together with the forfeiture of the equivalent of benefits gained by Tomasz S. (approximately €450). The court obliged all three convicts to redress damage incurred by the NPO and forfeited mobile phones used as instrumentalities to commit the crime. The sentences were not TF-related but for publicly committed incitement to hatred based on national and ethnic differences.

Manuel O. absconded, which led to the decision to exclude the evidence against him from the Arson case and initiate (also in 2018) a separate investigation in which Manuel O. was charged with TF in December 2018. The investigation was suspended due to the hiding of the suspect. In connection to a parallel investigation concerning the involvement of Manuel O. in the Arson case carried out by the German authorities, the Polish authorities initiated negotiations for transferring the proceedings to Germany. The up-to-date information of the whereabouts of Manuel O. implies the death of the suspect.

304. Turning to other risk indicators, the AT was informed that there were five TF-related MLA requests received by the Polish authorities from foreign counterparts in 2019. The MLA requests were executed by the District Prosecutor's Offices in Katowice, Rzeszów, Gdansk and Warsaw, and none gave grounds to launch a criminal investigation by the Polish authorities. While three of the MLA requests included mostly hearing of witnesses, the other two had more substantive links with Poland. In one of the cases, 19 Polish companies, their owners, founders, CEOs, accountants and other employees were involved, and in the second, business activities were carried out in Poland by the person investigated in the foreign jurisdiction. The absence of follow-up might be caused by the legal gaps in the application of the criminal liability of legal persons (see also R5), but in any case, it is hardly in line with the actual country risk, as far as the legal entities are concerned.

305. Apart from the actual cases (including MLA), in the course of its work, ISA identified certain methods of fundraising for supporting terrorist organisations, such as income from work (legal and illegal), financial support from family members, collections under the guise of charity support (including online), collections conducted on behalf of a terrorist organisation (voluntary and forced), and proceeds from criminal activities (smuggling, fraud, extortion, etc.). Moreover, the ISA has also identified cases of investment in real estate by members and supporters of terrorist groups in Poland. This is partially in line with the country's risk profile and with the constituent elements of the two convictions.

306. Since 2014, when there was an increase in Europe of cases involving foreign terrorist fighters, the ISA has been actively monitoring the foreign fighters and returnees who were Polish citizens or linked to Poland. However, there are no TF cases regarding returnees, and it cannot be concluded that this threat is adequately reflected in TF cases investigated.

307. The analysis above, coupled with the NRA statement that Poland might be an attractive place for logistics bases and the transfer of money and other assets for terrorist purposes and with the shortcomings with regard to the TF offence, reflected in the TC Annex (R.5), raise additional concerns about the possibility of a full and effective investigation into a TF case.

308. Another TF vulnerability identified in the NRA and confirmed by the convictions is the movement of cash. In this context, the finding of the TC Annex (32.8) that the customs do not have the specific power to stop and restrain currency at the borders in order to ascertain whether evidence of TF may be found is of particular importance. This raises concerns about the ability of the authorities to identify and initiate TF enquiries at the borders.

309. Overall, the AT considers that the TF convictions and even more the ongoing investigations lead to a positive conclusion as they reflect certain elements of the country's risks. Nevertheless, a clear statement that the results achieved in the period under review are fully consistent with the country's risk profile is difficult to make in the absence of a more significant number of prosecutions and convictions and taking into account the shortcomings.

310. The assessment team takes comfort in the fact that the ISA is systematically involved in a number of TF cases that appear to be quite well-grounded in their substance. However, this is a double edge observation which, coupled with the number of TF MLAs requests received in 2019 and other trends identified by ISA, suggests that a more comprehensive TF risk assessment is needed to address all the different types of potential TF activity (e.g., collection, movement and use of funds or other assets) (see also IO1). The absence of cases initiated other than through the ISA's work suggests that other authorities (including the prosecutors) lack sufficient knowledge and/or coordination to start a TF case on their own initiative (e.g. based on an MLA request received from a foreign counterpart). The GIFI's contribution to the initiation of the TF cases remains marginal.

#### ***4.2.2. TF identification and investigation***

311. The identification of TF cases has so far been carried out only by the Counter-Terrorism Centre of the ISA, which also ensures the communication between other the LEA potentially involved in the performance of national security tasks (such as terrorist actions but not TF), on the basis of the Act on the ISA and the Intelligence Agency of 24 May 2002.

312. ISA conducted nine TF investigations since 2016, out of which three were finalised with an indictment and two sentences were pronounced. At the time of the onsite visit, one case was still under investigation, and the investigation of another case was suspended (due to an outgoing MLA request and the flight of the key witness in Syria). The capabilities of the other bodies to conduct terrorism-related financial investigations remain virtually unused as they consider the terrorism-related matters as being in ISA's remit.

**Table 4.2. – TF investigations conducted by ISA**

Data		2016	2017	2018	2019	2020	Until v.2021
Number of investigations conducted in cases under Art. 165a of the Polish Criminal Code.		2	3	5	3	4	1
Number of investigations initiated		1	2	3	0	2	0
Number of investigations terminated		1	1	2	1	3	0
by	bringing charges	1	0	1	0	1	0
	termination	0	1	0	0	1	0
	Suspension	0	0	1	1	1	0

313. The specifics of the TF investigations, as introduced to the assessors, appear to demonstrate both the applicability of the legal framework and the ability of the Polish authorities to cooperate among themselves and with foreign counterparts. As described under the sub-chapter above, the convictions are related to the collection and transfer of funds (domestic and from abroad), and the funding was linked to a specific terrorist act, activity or organisation.

314. The main source of potential TF cases for the ISA is intelligence acquired in the course of already initiated terrorism cases. The methods of collecting information include operational and reconnaissance activities, monitoring of 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.

315. A tool designed to be used to pro-actively initiate a TF or a terrorism case consists in the Catalogue of incidents of terrorist nature<sup>56</sup>, which was distributed to several agencies by ISA. Group 11 of the Catalogue refers to TF and covers incidents related to the introduction of the circulation of assets from illegal or hidden sources. No information was provided on identified TF cases or investigations resulting from an incident report under this Catalogue.

316. Between 2016 and 2020, FIU submitted 237 disseminations to ISA concerning potential links with terrorism. These were not TF notifications that, in accordance with the AML/CFT Act, should be provided to the PPO. 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).

**Table 4.3. - Information exchange between ISA and GIFI**

Year	2016	2017	2018	2019	2020
<b>Terrorism Financing:</b>					
Requests to GIFI	24	9	15	11	38
Notifications from GIFI	103	45	53	25	11

<sup>56</sup> Approved through the Directive of the Minister of the Internal affairs and administration of 22 July 2016

317. According to ISA, each FIU dissemination, like any other disclosure, is subject to an operational investigation. Such verification includes a preliminary financial analysis and verification against all available information: the police databases; international databases (Europol, Interpol); open sources (Companies Register, Trade Register, Real Estate Register, etc.) mainly to determine whether it can be linked to any terrorist activity.

318. The AT is unable to ascertain how the GIFI disseminations were used by ISA, but no grounds were identified to report the case to the PPO. The assessment of the sufficiency of the data as a potential TF (or any other crime) case belongs to ISA and not to the prosecution.

319. The PPOs are not formally involved in the operational phase of the TF cases unless the LEA (ISA in this particular case) opens a formal criminal investigation. Therefore, there is no independent legal body to review ISA's decisions when a case is discontinued at the operational level.

320. The ways in which potential cases of TF are examined have been closely scrutinised by the AT. ISA generally presented its methods for a proactive approach - exchange of information on extremist groups; social media monitoring; co-operation with foreign and local counterparts, although no specific examples were presented. The ISA applies the reactive approach in work on the study of the GIFI reports. The means of gathering information on suspected terrorists are mainly operational and intelligence activities (HUMINT); opensource monitoring (OSINT); co-operation with partner services (local or foreign); analysis of records included in accessible databases.

321. There is no established practise for ISA to send feedback to the GIFI on the actions taken and the final decision on each notification received. This raises concerns about the effective coordination and communication between the ISA and the FIU in the field of countering terrorism and its financing.

322. The view of the Polish authorities that TF offence is an element of the crime of terrorism has several interlinked factettes. On the one hand, it is a matter of practice, as all the TF cases are strictly connected with a terrorism case. On the other hand, there is a theoretical understanding of the crime referred to in Article 165a CC (TF) as a preparatory stage into a specific terrorist act or activity rather than a separate crime. It is possible that this understanding by practitioners is influenced by academia<sup>57</sup> and the judiciary. The latter shared their opinion that the intention of the perpetrator of the TF to finance a specific terrorist act is essential for the recognition of the features of TF. Thirdly, from the risk perspective, the TF analytical part in the NRA is focused almost entirely on the risks of terrorism and not so much on TF, which in any event is linked to terrorism. Finally, from the technical perspective, and as presented in the TCA (R30.1), the ISA lacks formal competences in investigating TF offences that are not endangering the Polish state's security (through a terrorist act).

323. The ISA investigation unit and the Prosecutor's Office use all possible means to gather evidence during TF investigations. Interrogations of witnesses are cited as the most important evidence of the intentional element in the TF crime. Secret operations, including wiretapping, are widely used. When necessary, searches of people and premises, seizure of property, examination of telephones are carried out. The help of phonoscopy experts and translators is used.

---

<sup>57</sup> Thus, the NRA (p. 727) quote Prof. Alicja Grześkowiak, who considers TF "as a crime in the foreground of the respective terrorist crime, representing a stage of preparation for this type of act".

Information from payment institutions on TF cases is obtained without difficulty within two weeks to two to three months.

324. On a positive note, in the course of one of the ongoing investigations, ISA provided expertise on the structure and operational rules of ISIS and the potential roles played by suspects. The authorities pointed out (and the AT agrees) the value of the analyses elaborated by the ISA for the TF investigations. Officers of the mentioned unit undergo specialist analytical trainings, which is a commendable undertaking.

325. TF investigations are conducted and supervised only by the specialised Local Divisions of the Department for Organised Crime and Corruption of the PPO. With regards to the convictions achieved so far, the TF consisted in the collection and movement of funds (about €8 500) and other assets (paramilitary equipment), as well as in the use of funds (€200) and other assets (mobile phones, clothes).

326. The prosecution and LEA did not adopt methodological guidance or instructions for TF investigations, nor did they develop a case management system to prioritise potential TF cases. In fact, ISA has a monopoly on TF cases that have been handled from the beginning to the end exclusively by them; therefore, and seeing the limited number of cases, a case management system is not needed. While this can be considered somehow positive in terms of centralisation and specialisation, it leaves all the other authorities in Poland unconcerned by the TF, which might result in blind spots in the system. This is confirmed by the lack of reaction to all five TF MLA requests received in 2019 (see analysis in previous core issue) in terms of domestic investigations/analysis/measures which could have been triggered by those notifications. The AT is concerned about the general understanding and prioritisation of TF among the responsible institutions, especially in cases where the financing has no direct link with Poland.

327. The authorities stated that the main challenge in effectively prosecuting TF cases, even when financing indications are present, is the impossibility to prove the commission of or the link with a terrorist act. While in one of the TF convictions, the financing element was proved through the membership of the perpetrators to a terrorist organisation, one of the culprits who participated in the financing act was acquitted due to the fact that he was not a member of the said organisation. This confirms the four factettes concerns expressed in paragraph 323 above.

#### *4.2.3. TF investigation integrated with –and supportive of- national strategies*

328. It cannot be concluded that the TF investigations are integrated and used in support of national counter-terrorism strategies, as Poland does not have a document that would constitute a national anti-terrorism financing strategy. Poland applies the provisions of the 2005 EU Counter-Terrorism Strategy, Directive 2015/849 and Directive 2019/1153.

329. Until 2019, the "National Antiterrorist Program for 2015-2019" was in force, which contained some general priority actions of legislative nature, aiming at implementing the previous MONEYVAL assessment report recommendations on TF offence, but no other pertinent strategic objectives/ actions in relation to countering TF were envisaged.

330. It should also be noted that the programme has identified GIFI as the main competence in counteracting TF, as it deals in the area of collection, gathering, processing and analysing financial information, and is responsible for taking action in this field, including through its co-operation with foreign FIUs. However, the GIFI's notifications to ISA are not TF-related from the outset, in

which case they should have been disseminated to the PPO. No TF disseminations to the PPO have been reported.

331. The new AML/CFT Strategy (2021) lacks priority measures in connection with countering TF (among the six generally defined priorities), or at least they are not addressed by means of focused and targeted actions that would integrate and be supported by the results of the TF investigations.

#### *4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions*

332. The Polish legal framework provides for a dissuasive sanctioning regime for TF crimes, with the exception of acts provided by Art.165a (3) CC (see analysis under R5). The offences covered by the two convictions achieved in the period under review and analysed in the sub-chapter above do not fall within this exception.

333. Despite the availability of sanctions, when looking at the penalties applied in practice in relation to the two convictions achieved, they 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.

334. Regarding the reasons for this difference in the imposed penalties, AT got acquainted with the motives for one of the sentences and the individualisation of the punishment. It turns out that for the Court, the amount of funding found in the investigations plays a more significant role in terms of punishment than the level of danger that the funded act may cause. Based on these data, no positive conclusion can be drawn as to the appropriateness and dissuasiveness for TF crime.

335. The possibility of imposing a fine and confiscation for the crime of TF, in addition to imprisonment, means that the Polish courts have additional legal remedies to punish the perpetrator accordingly. Unfortunately, their actual implementation is limited, including the small number of investigations leading to convictions.

#### *4.2.5. Alternative measures used where TF conviction is not possible (e.g. disruption)*

336. Even in theory, the possibility to use criminal, regulatory or other measures when it is not possible to secure a conviction for TF is very limited. The application of confiscation under Art. 45 of the CC is the only possible measure to be taken in the absence of a conviction.

337. There is no possibility in these cases (when for some reason a conviction cannot be secured) to impose a sanction or other restriction on a related legal entity, as, by law (Act of 28 October 2002 on liability of collective entities), it is bound by the existence of a convicted person.

338. In practice, the authorities have never applied alternative measures in lieu of proceeding with FT charges.

#### *Overall conclusions on IO.9*

339. 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. However, there are still some technical shortcomings (commented on in the TCA) that also affect efficiency. 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 prosecution and other LEA have not adopted methodological guidelines or instructions for TF investigations, nor have they developed a case management system to prioritise TF cases. None of the FIU reports to ISA on potential links to terrorist financing triggered a case of TF; however, information from the FIU was used in one of the 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 they are not dissuasive or proportionate. The IO is achieved to some extent as the authorities demonstrated that TF convictions could be achieved, and ISA has competences in relation to TF. Nevertheless, major improvements are needed to ensure full effectiveness of TF investigations capacities and integrate the TF investigations in the national counter-terrorism strategies.

340. **Poland is rated as having a Moderate level of effectiveness for IO.9.**

### **4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)**

#### ***4.3.1. Implementation of targeted financial sanctions for TF without delay***

341. 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 sanctions lists are published on the GIFI's website immediately after the decision of the United Nations Security Council, and the lists are automatically updated based on changes on the website of UN Committees. The implementation of sanctions stemming from resolution 1373 takes place without delay as at the national level, the decision of the GIFI concerning listing is enforceable with immediate effect (Article 120 (7) of the AML/CFT Act). Therefore, the implementation of TFS and freezing of property values of persons and entities designated by the UNSCR is made without delay.

342. To support the application of the TF TFS, in 2018, GIFI and KAS published communications on their website, regarding the specific measures to be taken, including and the obligation to freeze and prohibition to make property values available. These communications include the legal framework governing the TF TFS, the measures to be taken in this regard and contain links to the sanctions list on the UN website.

343. Moreover, the authorities developed a communication mechanism to notify relevant competent authorities and all obligated institutions of new designations: upon subscription, a newsletter is available on the GIFI's website for the entities to receive prompt notifications on the updates of the lists. GIFI provides a tool available to be uploaded from its website, allowing access to updated lists in format. Over 1,000 subscriptions have been reported since the initiative was launched in mid-2019. The authorities clarified that the tool is intended for small, obligated institutions as large FIs use automatic updates delivered in their software. GIFI did not provide any information on the percentage of the obligated institutions that subscribed to the newsletter, but seeing the overall number of RE in Poland, this type of outreach, although a commendable initiative, is an area for further strengthening. The lists are published on the GIFI's website and are available in MS Excel format too.

344. Poland does not have any cases to prove the implementation of TFS pursuant to UNSCRs 1267 and its successor resolutions and 1373; neither has it designated persons or entities that meet the designation criteria under the mentioned Resolutions.

345. The provisions of the AML/CFT Act give the competence for listing (at the national level) and making proposals for listing (to UNSC) to the Financial Security Committee, composed of representatives of more than 20 national authorities<sup>58</sup>. The Law sets the procedural steps to be taken 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.

346. Motions from competent national authorities to propose a person or entity to be recommended for listing can be submitted by any member of the FSC as a result of potential targets being identified in the execution of their duties. According to the AML/CFT Act, based on the recommendation from the FSC, GIFI may submit (through the MFA) a designation request to foreign institutions and international organisations (including the UN). This is not a formal obligation for the GIFI, but in practice, since the FSC is a consultative and advisory body for the GIFI, it should be expected that the recommendation of the Committee would result in the GIFI making an application to foreign authorities. The FSC recommendation should contain the justification for the proposal, as well as information and documents confirming the circumstances grounding it.

347. Similarly, the requests from foreign countries shall be received through the MFA, which is a member of the FSC. Based on the justified motion, after considering all the collected information and documentation, the FSC shall decide and may recommend entering a person or entity into the national list of persons and entities against which the financial sanctions shall be applied.

348. Recommendations of the FSC on the listing are made collectively, by analysing all circumstances of the case, according to specific criteria provided by the law<sup>59</sup>, which cover the standards set forth in UNSCRs. Based on the recommendation of the FSC, the GIFI issues the listing decision, which is enforceable with immediate effect, and which amends the national sanctions list immediately.

349. The system described above has never been tested in practice, as no listing proposals have been made to the FSC for consideration. This is largely in line with the country's risk profile as no attacks have occurred, and there are no reasons to believe that potential targets might be present on its territory. The authorities maintain they had a "*dry run*", an exercise, to test the system.

350. To identify potential targets, various authorities would apply different approaches depending on their main activities. For example, GIFI would base their initial analysis on a potential candidate for listing on information received from REs and conduct the same type of analysis to determine the grounds for listing, as in the case of any SAR. The ISA would use the

---

<sup>58</sup> Ministry of Internal Affairs, the Ministry of Justice, the Ministry of Foreign Affairs, the Ministry of National Defence, the Ministry of Economic Development, Labor and Technology, the Ministry of Finance, the minister competent for computerization, a member of the Council of Ministers competent for coordinating the activities of special services, the Chairperson of the KNF, the President of the NBP, the Chief Commander of the Police, the Chief Commander of the Military Police, the Chief Commander of the Border Guard, the Public Prosecutor, the Head of the Internal Security Agency, the Head of the Central Anti-Corruption Bureau, the Head of the Intelligence Agency, the Head of the Military Intelligence Service, the Head of the Military Counterintelligence Service, the Head of KAS and the Head of the National Security Bureau.

<sup>59</sup> Art. 121 of AML/CFT Act

information they have in the terrorism-related cases, and they would inform the FSC at the indictment, while the PPO would collect their suspicions on the potential listing from their ongoing cases and would inform the FSC the moment they would press charges against the respective individual or entity. Other FSC members were not clear what procedure they would apply to identify potential targets.

351. 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.

352. Obligated institutions are aware of their TF-related TFS obligations and of the requirements to freeze funds/assets of designated individuals/entities. They have systems in place that allow the swift implementation of TFS by automatic screening of customer database as soon as they become aware of new designations (e.g. by checking updates on relevant UN sources or upon receipt of a notification from the GIFI).

353. Banks, insurance companies and money or value transfer services rely on a range of well-known commercial databases to screen their existing and potential customers against the sanctions lists. Clients are checked against the TFS lists at the stage of establishing the business relationship and on every occasion when transactions are carried out. Regular checks of the client database are automatically performed daily, on average. (For detailed analysis on categories of FIs and DNFBPs, see also IO4.)

354. The FIs proved a complex understanding of the sanction's evasion risk, including potential use of complex legal structures and activity on behalf of designated persons by associates. They have a good perception of the need to identify and screen not only customers and BOs, representatives/signatories of the legal person, but also all subjects of the ownership structure, in fact, all parties to a transaction.

355. DNFBPs proved variable levels of understanding of legal provisions and measures to be taken on the implementation of TF-related TFS. Sectors with greater legal knowledge (notaries and lawyers) are more aware of restrictive measures that would have to be implemented in case of a positive match, which would include notification to the GIFI and the PPO, blocking of the provided funds and the non-provision of services. Notaries, casinos, auditors, lawyers and real estate agencies conduct manual checks on sanctions lists provided by the GIFI through its website. Other sectors (real estate) understand the concept of "lists" in a broad sense and would equally treat matches in any list (PEPs, sanctions, high-risk jurisdictions, etc.). In the case of casinos, the screening measures are applied to the clients on a very large number of different lists including, UNSCRs.

356. As described above, the private sector has been provided with some online guidance on FT-related TFS. The GIFI and other supervisors make TFS information available on their websites and keep contact on a case-by-case basis with the representatives of obligated institutions. However, the overall communication approach adopted by the authorities is not yet sufficiently targeted, and obligated institutions need to seek TFS-related communication mostly out of their own initiative. Most of the trainings are more of a general AML/CFT nature, and only a small part

is dedicated to TFS<sup>60</sup>. As a result, the DNFBPs had difficulties in describing details related to TFS, being limited only to general knowledge in this regard.

#### **CASE BOX 4.3 – Case-by-case feedback**

GIFI has a dedicated e-mail box to which obligated institutions send inquiries regarding the implementation of obligations resulting from the application of TFS. Institutions ask, for example, which lists are to be used, is there a national sanction list, which entities are to be checked against the sanction lists (whether their clients or clients' contractors). Approximately 130 e-mails have been received to this inbox.

357. Supervisory authorities test the screening mechanisms of obligated institutions, verify possible business relationships with the sanctioned persons and assess how partial matches with lists identified as false positives would be resolved. AT was not provided with any confirmation on the detection of significant deficiencies in the area of TF-related TFS compliance, and thus, no remedial measures have been taken in relation to breaches of TF TFS-related provisions.

#### *4.3.2. Targeted approach, outreach and oversight of at-risk non-profit organisations*

358. 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. Not being based on a risk analysis, the subset of NPO considered as falling under the FATF definition is quite broad.

359. A separate chapter of the NRA is dedicated to the analysis of the “Activities of NPOs”, but as described under the Introductory part and under IO1, the value of the assessment is very limited. Most of the “analysis” speaks about generalities such as the definition of NPOs, legal requirements applicable to NPOs, the scope of NPO activity according to the EU Commission, and types of such organisations under Polish law.

**Table 4.4 Total NPO<sup>61</sup> number distribution by type of main activities (2019)**

<b>NPO Type</b>	<b>Number</b>	<b>Percentage Distribution</b>
Culture & Art	11 600	12,9%
Education & Investigation	9 500	10,6%
Health	3 700	4,2%
Sport, tourism, recreation	25 500	28,5%

<sup>60</sup> In 2018, the GIFI organised four meetings dedicated inter alia to sanctions; in 2019, there were four seminars covering the issue of sanctions (for cooperative banks, accountants, auditors, notaries, legal advisers, real estate agents, tax advisers, attorneys, and insurance companies). In February 2020, the GIFI organised a training entitled "Application of specific restrictive measures and the National Assessment of Money Laundering and Terrorist Financing Risk - Threats and Vulnerabilities", attended by representatives of cooperative banks. In December 2020, the GIFI started a series of trainings (continued at the beginning of 2021) on the obligations of the obligated institutions in the field of counteracting the financing of terrorism, including the application of specific restrictive measures. The training was attended by representatives of customs and tax control offices, courts of appeal and the National Association of Cooperative Savings and Credit Unions.

<sup>61</sup> All NPOs not only associations and foundations

Rescue services	14 100	15,7%
Social services	6 600	7,3%
Business and professional affairs	2 900	3,3%
Environment	2 400	2,7%
Hunting	2 700	3%
Employment assistance	1 200	1,4%
Local social and economic development	3 500	3,9%
Law, advocacy, civil rights	1 500	1,7%
Support for institutions, NGO and citizens initiatives	1 300	1,5%
Other activities	3 000	3,3%
<b>Total</b>	<b>89 400</b>	<b>100%</b>

360. Two general TF possible scenarios identified by the EU Commission related to the collection and transfer of funds through the NPO for TF purposes are included in the body NRA (the establishment of an NPO in order to "raise funds" and the use of existing NPOs to finance local terrorist activities). In addition, Annex 3 of the NRA includes some TF risk scenarios associated with the charitable organisations, but it is not clear why this category of NPO was chosen, and it cannot be concluded that the guidance is thoroughly applicable to all NPOs.

361. The TF risk analysis related to NPOs stops there as the GIFI's assessment on NPOs activities<sup>62</sup> is exclusively focused on "money laundering threat without any links to terrorist organisations and financing of terrorism", followed by a description of possible fund-raising sources without any conclusions/assessment on where the threat may be. A statistical analysis on proceedings instituted by the GIFI in 2016-2018 where the words "association" or "foundation" were noted follows, but without any actual conclusion or explanation on what this would entail. In any case, such a conclusion would pertain to ML and not TF.

362. Overall, the NRA assessed the risk of NPOs exposure to FT as low-medium, without having a clear basis to substantiate this finding.

#### **Table 4.5 Overview of NPOs in Poland (2019)**

\*Number of entities that fit the NPO concept as defined by the FATF.

<b>Types of NPO</b>	<b>Number*</b>
Foundations	15 300
Associations	69 900
Private Legal Person of Public Utility	8 700
<b>Total</b>	<b>93 900</b>

363. There were 85.200 actively operating non-profit organisations registered in Poland (i.e. associations which constitute legal entities and other similar social organisations, foundations, social-religious organisations, as well as economic and professional self-government organisations) with a total of 8.9 million members. In 2019, 28.5% of organisations dealt with sports, tourism, recreation, 15.7% with rescue, 12.9% with culture and art, 10.6% with education and upbringing and scientific research, 7.3% with social and humanitarian aid. Social and

<sup>62</sup> Para 604 of the NRA

humanitarian aid activities are more often a point of interest of entities with the status of public benefit organisation (PBO).

364. Poland established that associations and foundations correspond to the FATF definition of non-profit organisation. Activities of organisations of this type are regulated by three acts: Act of 24 April 2003 on public benefit activity and volunteering (PBAV), Act of 6 April 1984 on Foundations and Act of 7 April 1989 - Associations Law.

365. Associations constitute the most numerous group of active organisations in the non-profit sector (69 100 in 2019; 78.4%). Supervision of the activities of associations of local government units lies with the voivode competent for the registered office of the association.

366. Foundations represent the second group of organisations that contribute to the non-profit sector, with 15 300 active foundations being registered (16.5% of the total number of active non-profit organisations). Foundations are supervised by the competent minister depending on their activities (indicated in the articles of association). If a foundation has the status of a public benefit organisation, it is also supervised by the Chairman of the Public Benefit Committee.

367. NPOs (except associations that are not PBOs) 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, as they are subject to additional scrutiny owing to their tax-preferential status. All foundations must publish their annual financial reports where the sources and the manner of financing are indicated for all income over €15 000. There was no information about instances (apart from that such situations do exist) where the foundations did not observe this obligation and the measures taken as a result.

368. Associations that are not PBO have no obligation to prepare and send (*e.g.* to the supervisory authority) a report on their activity. The authorities maintained, however, that in practice, most associations prepare such reports to enhance their credibility in the eyes of citizens and donors or for applications for grants (to which it is usually required to attach a financial report).

369. Associations and foundations become obligated institutions under the AML/CFT Law if they meet three cumulative conditions: they have legal personality; they have been established accordingly on the basis of the Act of 7 April 1989 –

Associations Law or on the basis of the Act of 6 April 1984 on Foundations; they accept or make payments in the amount equal to or exceeding the equivalent of €10 000 in cash, regardless of whether the payment is made as a single operation or several operations that seem to be related.

370. The general supervision of associations is performed by customs and tax control offices, competent governors of provinces (voivodes) or governors of districts. Foundations are monitored by customs and tax control offices, competent ministers (depending on the Foundations' profile and/or activities), or governors of districts. The voivodes conducted 79 inspections in 2018 and 80 in 2019 as ordered by the Chairman of the Public Benefit Committee (inspections conducted in PBOs). The remaining figures are found in the table below.

**Table 4.6: Supervisory actions on NPOs**

Year	Authority				
	Governors of district	Tax inspection office	GIFI	Ministry	The presidents of the cities
-					
2016	16	15	-	-	-
2017	14	2	3	-	-
2018	82	1	-	-	-
2019	7	-	-	2	5

371. The supervision performed on NPOs by various state authorities (i.a., Ministry of Labour, Ministry of Finance) is focused on other matters than CFT, is not performed as risk-based and is rather oriented to technically identify NPOs which could become obliged entities and report respective cases to GIFI. The supervisors lack human resources and AML/CFT trainings.

372. The control of compliance with the AML/CFT requirements by foundations and associations which are obligated institutions is performed by the GIFI, who is at the same time the coordinator of all AML/CFT control activities carried out by other institutions related to NPOs. The number of inspections carried out between 2016 and 2019 is reflected in Table 4.6, but the volume of supervisory actions is not commensurate with the sector's dimension.

373. According to the AML/CFT Law, in the framework of the NPO coordination, by 15 November of each year, the GIFI shall elaborate and make available information concerning areas and sectors particularly exposed to the risk of money laundering or financing of terrorism. The authorities maintained that such information was provided to the NPO sector in 2018, 2019 and 2020, but the assessors were not presented with a sample; therefore, a conclusion on the value of its content cannot be drawn. In the course of the GIFI's inspections, several AML/CFT aspects are checked, such as the internal procedures, the CDD measures applied (including the BO), and the manner of analysing transactions with a view to suspicious transactions reporting. One SAR was filed in 2019 by a foundation.

374. There is a nascent form of communication between the GIFI and the NPO supervisors on possible risk scenarios that should be taken into account when carrying out outreach and targeted risk-based supervision and monitoring of NPOs, but only two onsite inspections were carried out following such, by the Ministry of Economic Development, Labor and Technology.

375. Poland has not reviewed the frequency and monitoring of NPOs at risk. 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. During the respective training, the GIFI presented the manner in which foundations should fulfil their obligations in the AML/CFT area and discussed the control guidelines applicable to foundations. The document developed by the GIFI, containing guidelines on the manner of conducting controls and their and scope, was made available to the authorities supervising foundations. Information letters were sent to the

supervisory authorities carrying out controls in foundations and associations, and the content was published on the GIFI's website.

376. As a result of one of the controls executed by controllers of the Minister of Family and Social Policy on a foundation, several irregularities related to the AML/CFT obligations were identified, and administrative proceedings in the form of a fine were instituted. The AT is not aware of the level of fine nor of the findings on the specific irregularities detected.

377. The NPO sector itself is aware to a certain extent of the TF risks. They are able to articulate potential risks and the mitigation measures applied, such as the fact that the support may be delivered in the form of equipment or services (building wells, water dams, purchase materials, psychological or medical support or counselling), rather than actual monetary aid given to beneficiaries. The sector benefitted from training on TF risks organised by international organisations through the MoF. They are aware of the NRA and consider the financial reports sent to the Ministry of Economic Development, Labor and Technology a form of communication with the authorities, which contributes to the preventive measures. Nevertheless, their awareness of the CFT legislation and typologies and patterns of NPO misuse for TF purposes are areas for improvement.

#### *4.3.3. Deprivation of TF assets and instrumentalities*

378. No freezing under UNSCRs 1267 and 1373 have been reported. The obligated institutions met onsite, confirmed that upon a freezing action taken under the FT-related TFS regime, they would report the amount frozen to the GIFI. Following analysis by the GIFI, reports are disseminated to the ISA for further intelligence actions and investigations.

**Table 4.7: Property seized and confiscated in TF cases**

	<b>Property seized (€)</b>	<b>Property confiscated (€)</b>
2020	124 445	1 700
2019	0	0
2018	0	0
2017	0	1 900
2016	1 900	0
2015	0	0
2014	0	0

379. In relation to TF convictions achieved so far (two cases, see IO.9), confiscation measures aimed at depriving the terrorists of the allocated or used instrumentalities were applied. In one case, out of the total amount of the collected and moved funds (€8 500) and other assets (paramilitary equipment), only €1 900 were seized and subsequently confiscated. The authorities are currently conducting two TF investigations in relation to the collection and movement of funds via money transfer providers (and hawala). While one investigation included identification and seizure of assets (€124 445 and jewellery), no such measures were carried out in connection to the other case (despite the lengthy investigation initiated in 2018).

#### *4.3.4. Consistency of measures with overall TF risk profile*

380. As described above, confiscations for TF have been achieved, and a series of preventive measures have been imposed in the ongoing cases. This is a commendable outcome that proves the ability of the competent authorities to apply confiscation measures in TF cases. Nevertheless, the measures taken at the national level to deprive terrorists, terrorist organisations and terrorist financiers of assets and instrumentalities are not fully consistent with the Polish risk profile for several reasons.

381. First of all, the risk of terrorism financing itself is not fully assessed through the NRA or otherwise and is perceived primarily as a derivative of the risk of terrorism. The understanding of TF risk is not supplemented by good awareness among intelligence and investigative agencies about purely financial activities that could potentially infiltrate the financial or non-financial systems. In particular, due to the low level of terrorist threat and the associated link with terrorist financing in Poland, ISA acknowledged only individual cases of persons whose activities could indicate an intention to collect or transfer funds to entities related to particular terrorist activities. There is an acknowledged absence of instruments for deprivation of TF assets in case of using informal cash transfer services, as Hawala system.

382. Secondly, the ISA identified certain methods of raising funds in Poland for supporting terrorist organisations, such as income from work (legal and illegal), financial support from family members, collections under the guise of charity support (including online), collections conducted on behalf of a terrorist organisation (voluntary and forced), and proceeds from criminal activities (smuggling, fraud, extortion etc.). The identification of such typologies was not doubled by similar seizures and confiscations.

383. Turning to the general confiscation regime, the shortcomings identified there impact the authorities' ability to effectively seize and confiscate in TF cases as in any other crime (see R4).

#### ***Overall conclusions on IO.10***

384. Poland implements UNSCRs 1267 and 1373 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 based on UNSCRs 1267 and 1373 and did not restrain TF funds, which is largely corresponding to overall TF and terrorism 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 take 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.

385. Overall, the IO is achieved to some extent as the targeted financial sanctions regime is in place, assets have been confiscated in TF cases, and some measures were taken to ensure NPOs awareness and transparency.

386. **Poland is rated as having a Moderate level of effectiveness for IO.10.**

#### 4.4. Immediate Outcome 11 (PF financial sanctions)

##### *4.4.1. Implementation of targeted financial sanctions related to proliferation financing without delay*

387. The adoption of the JCPOA agreement in 2015 made it possible to rebuild relations between the European Union (including Poland) and Iran. In 2020, Iran was ranked 108th in terms of exports and 97th in imports. The largest positions in Polish exports to Iran in 2020 were “Other food products” (17.4% of the total); watt (8.4%); Fuel, oil or coolant pumps (5.5%) and engine parts USD (4.7%). The exports consisted in chemicals (21.3% of total); pistachios (12.5%); dried grapes (12.2%); fragrance blends (11.3%).

388. Poland and the DPRK do not have any bilateral agreements regulating the principles of economic co-operation. Mutual contacts of economic nature are very limited, in particular, due to the UN Security Council and EU sanctions imposed on the DPRK. The scale of bilateral trade is minimal. The vast majority of very insignificant imports and exports recorded in the statistics are the migrant property of employees of the Polish Embassy in Pyongyang or the DPRK Embassy in Warsaw.

389. The NBP does not record North Korean investments in Poland or Polish investments in DPRK.

390. Poland has in place national legislation requiring an export authorisation for the sale, supply, transfer or export of arms and related materials to third countries and an authorisation for the provision of brokering services and other services related to military activities, which, together with Council Decision (CFSP) 2016/849, provides the basis for enforcement of the arms embargo against the DPRK and the ban on related brokering services. Poland is a member of the main international export control regimes in this area, including the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies.

391. The trade in goods and technologies such as military equipment and dual-use goods, including technologies related to WMD, is subject to control by the state. The main role in this area is given to the Department for Trade in Strategic Goods and Technical Safety on behalf of the Ministry of Economic Development, Labor and Technology (minister competent for economy), which licenses international trade in strategic goods, including dual-use goods. The procedure is initiated by filing an application to the minister competent for the economy by the entity wishing to export products present on the control lists (dual-use goods list or military equipment list). Before a license is granted, an EU database (so-called COARM online system – in case of arms or DUES – in case of dual use goods) is checked for the presence of similar applications denied by the other EU MS within the last three years.

392. From the statistics provided, an increase in the number of licenses granted and certificates issued for dual-use goods is apparent (from 53 issued in 2014 to 195 provided in 2019). The authorities explained that this is due to a significant increase in foreign investments, especially in some regions of Poland. This resulted in new entities coming to the market, some specialised in development of advanced technologies which quite often use dual-use materials and products, hence needing licenses. This sector is more dynamic as compared to the conventional arms market, which is more stable and the players there are mainly seasoned Polish companies.

#### *4.4.2. Identification of assets and funds held by designated persons/entities and prohibitions*

393. Targeted financial sanctions concerning the UNSCRs relating to the combating of financing of proliferation are addressed in the Republic of Poland at the EU-level providing for sanction legislation referring explicitly to DPRK and Iran, such as Council Regulation (EC) No 1509/2017 (DPRK regulation) and Council Regulation (EC) No 267/2012 (Iran non-proliferation regulation), respectively. Both regulations are binding in their entirety and directly applicable in all Member States.

394. The EU mechanisms 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. There are additional mitigating measures applied by the EU requiring prior authorisation of transactions with designated Iranian entities. This allows the authorities to determine if the transfer of funds for which the authorisation is requested would be permissible according to the EU Regulations.

395. As for the TFS against DPRK, in the past, some designations by the UN were shortly transposed into the EU framework, but in some other cases, delays in implementation of the UNSCRs of DPRK can still occur.

396. Poland did not develop a domestic mechanism of publication of the UNSCRs on PF as the freezing obligations under European regulations are applicable to all natural persons and all legal persons within the EU and take effect immediately on publication of the regulations in the EU's Official Journal.

397. Pursuant to Article 47 of the Regulation 1509/2017 (DPRK regulation), the Council communicates its decision to the natural or legal person, entity, or body referred to in paragraphs 1 and 2, including the grounds for listing, either directly, if the address is known, or through the publication of a notice, providing that natural or legal person, entity or body with an opportunity to present observations. Identification of assets and funds held by designated persons/entities and prohibitions

398. The financial institutions have protocols in place to identify and freeze assets without delay and display a good understanding of their obligations in the implementation of PF TFS. The DNFBP sector has substantial deficiencies in observing the PF-related obligations, mostly due to the lack of awareness. This is partially explained by the lack of designated authority in controlling the implementation of the PF-related regulations.

399. No assets of persons linked to relevant DPRK or Iran UNSCRs have been identified in the country, and as a result, no assets or funds associated with PF have been frozen. In the period under review, no UTRs have been filed in relation to proliferation or PF. This corresponds to the country profile, as Poland is geographically located a significant distance from, and has no tight commercial or other links with the countries concerned. While no hits have been reported, there is no reason to doubt that financial institutions can take such steps effectively, at least as regards specifically named jurisdictions and persons.

400. As DPRK and Iran - related transactions are to be considered a high risk, it is therefore mandatory to perform enhanced due diligence, and what follows, there are neither exemptions nor thresholds applicable.

401. During the interviews, GIFI explained that in case of the identification of a transaction or a financial flow that might be related to proliferation activities (i.e., transfers into the accounts of regimes on which international sanctions were imposed), the information would be forwarded to ISA to perform statutory operational and analytical work.

402. In 2016, the Government of Poland adopted the National Interdiction Mechanism (NIM), describing the procedures for interagency co-operation and decision-making when interdicting a dual-use item suspected of being destined for production of WMD or their delivery means. It also presents international commitments in the non-proliferation domain and national legal basis for actions of governmental authorities. Although no direct reference to PF is made, NIM serves as a guidebook meant to help to expedite actions by relevant services.

403. The FSC and GIFI are not involved in the process of granting the licenses and issuing certificates for dual-use goods or any other activity related to PF at the national level; thus, it seems that the financing of proliferation is insufficiently prioritised when it comes to identifying persons and entities involved in proliferation of WMD.

#### *4.4.3. FIs, DNFBPs and VASPs' understanding of and compliance with obligations*

404. The financial sector demonstrated a sound understanding of their obligations under the PF UNSCRs, as well as the ability to take the necessary steps to apply the relevant mechanisms. Banks perform automatic checks on their customers, beneficial owners, other participants of the business relationships and transactions against the international sanctions lists (including PF UNSCRs and dual-use goods). The checks are done at the onboarding when a transaction is being conducted and periodically (mostly daily, with lists being updated on the same frequency). Most of these IT solutions are provided at the group level. In case of positive matches, the transaction is suspended or the account is blocked and is notified to either the GIFI or the PPO, who would then proceed to give further instructions.

405. Other FIs (PSPs, investment firms, insurance companies, credit unions and leasing companies) implement similar procedures adapted to their own business, size and complexity, although "positive" cases were not reported. Certain FIs (credit unions) confuse the notion of high-risk jurisdictions with that of sanctions lists and do not differentiate between measures for TF and PF. In the case of foreign exchange, checks are performed on the spot for transactions over a certain threshold against a self-generated list based on GIFI and EU listings. In case of a hit, the amount would not be exchanged.

406. Overall, the DNFBPs lack full understanding of PF rules and their obligations on the implementation, relying mostly on manual checks on the "sanctions lists", which in their understanding would comprise both TF and PF. No particular measures are taken to detect funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities.

407. Sectors with greater PF knowledge (real estate and casinos) are more aware of the restrictive measures but understand the concept of "lists" in a broad sense and would equally treat matches in any list (PEPs, TF or PF sanctions, high-risk jurisdictions, etc.). Notaries were not aware of the PF UNSCRs or of their obligations thereof. Most of the sectors (lawyers, notaries) deplored the lack of communication from the authorities in this respect.

408. VASPs run real-time and ex-post screenings (including on PF TFS), on their customers and transactions, based on risk criteria (which can include nationality, potential suspicions raised

during the remote identification process or the transaction history, amount of the transaction, etc.).

409. Most of the reporting entities that met onsite mentioned that they would inform the GIFI and ISA before proceeding with a transaction when a link to a PF UNSCR would be established. Only FIs, especially banks, acknowledged the potential for sanctions evasion, including through the use of persons or entities owned or controlled by those designated, otherwise it is not widely understood by other obliged entities.

410. The obliged entities have the possibility, on their own initiative, to acknowledge the potential risk of being abused for PF, based on the e-learning course provided on the GIFI website, which informs about the obligation to verify the sanction lists (including sanctions against Iran and DPRK) in the context of the risk related to business relationship or transaction associated with those countries. It directly states that in the case of association of business relationships or an occasional transaction with a high-risk third country (including Iran and KRLD) or a state in relation to which the UN or the EU made the decision on imposing sanctions or specific restrictive measures, the obligated entities should apply enhanced due diligence measures.

411. The MFA is responsible for sanctions-related guidelines both for public and private stakeholders issues some guidelines on financial sanctions imposed on DPRK and Iran. A training devoted to the issues of CTF/CPF (Iran & DPRK) was organised for the obliged entities in 2017 at the invitation of the Polish Bank Association. The MFA sent letters to entrepreneurs regarding the activities related to the DPRK and issued legal opinions in response to specific questions posed by the private sector. The MFA informs about materials of the European Commission, and the website includes a link to EU websites, where all information on sanctions, including guidelines and opinions, can be found.

412. However, those initiatives were left to the initiative of the private sector, and the obliged entities deplored limited awareness-raising action taken by other supervisory authorities in relation to PF issues. No systematic outreach to support the private sector in fully understanding their obligations was provided.

#### ***4.4.4. Competent authorities ensuring and monitoring compliance***

413. The supervisory authorities do not have legal responsibilities in ensuring and monitoring compliance with the PF TFS. However, during the interviews, UKNF stated that they would consider the verification of PF-related TFS obligation in their respective inspection procedures in an attempt to have an overall view on the entire system where preventing PF is seen as part of. This statement was confirmed, i.e., through the inclusion in the UKNF “co-operation” questionnaire for payment institutions of a question on the existence of clients who deal in arms or have transactions with entities and individuals in countries subject to EU and US sanctions. Similarly, the UKNF off-site supervision questionnaires for payment institutions include the provision of the sanctions lists used and a description of the methods and frequencies of the screening of customers against sanctions lists, together with printouts of system logs confirming the screening of the customer database against those lists, and information on the percentage score (or related algorithm applied) of customers’ identification details with the sanctions lists.

414. UKNF and NBP do not draw a distinction between TFS related to PF and TF when conducting onsite inspections in the exercise of their general functions, and examined the systems put in place by FIs to implement the sanctions regimes for both TF and PF.

415. However, during the interviews, other supervisors (notaries, gambling sector) stated that they do not consider any issues related to PF during the inspections. While the staff of the supervisory authorities receive trainings in TFS matters, the lack of specialised training on PF may have an impact on the effectiveness of monitoring the PF-related obligations, as all supervisory authorities stated that no specific training on PF was provided.

416. The assessment team was not provided with data that would suggest that there are methodologies in place to specifically check compliance with TFS related to PF. No sanctions or penalties have been imposed.

417. While from the technical perspective, the EU freezing mechanism is functional and mandatory, a coordination domestic mechanism on PF matters would enhance the country's capacities to prevent sanctions from being evaded and to develop and implement policies and activities to combat the financing of proliferation of WMD.

### ***Overall conclusions on IO.11***

418. 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, which is largely in line with its risk profile. Most of the financial institutions (by far the most material) 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. Supervisory authorities do not have responsibilities in ensuring and monitoring compliance with the PF TFS while there is proof of some supervisory actions on PF in practice. The Immediate Outcome is achieved to some extent as the legal framework is largely in place and the most material sectors apply sound preventive measures. Major improvements are needed, especially by introducing a supervisory mechanism and more targeted guidance to DNFBPs.

419. **Poland is rated as having a Moderate level of effectiveness for IO.11.**

## 5. PREVENTIVE MEASURES

### 5.1. Key Findings and Recommended Actions

#### **Key Findings**

- a) All FI and DNFBPs met onsite to perform regularly updated risk assessments. Certain entities, particularly in the banking sector, demonstrate a remarkable degree of risk understanding. Entities having a lower degree of risk understanding (mostly DNFBPs) perform risk assessments more as formalistic exercises aimed to comply with the legal obligations, not allowing them to fully identify specific risks applicable to the entity or to implement more comprehensive mitigation measures besides the general AML framework.
- b) Most FIs belonging to international financial groups implement robust group-wide procedures. This circumstance does not prevent the implementation of the local AML requirements. On the contrary, often, the group procedures demand the implementation of higher (than Polish) standards, thus enhancing the overall degree of AML compliance of the obligated entities.
- c) FIs establish comprehensive transaction monitoring systems based on IT tools that generate alerts. However, some cases in which a heavy reliance on alert systems is placed without fully considering whether the determined risk scenarios are commensurate to the business profile and risks have been detected. Regardless of the approach adopted to transaction monitoring, banks amount for most of the SARs reported, with other FIs and DNFBPs reporting lower numbers, although this is mostly in line with their respective risk profiles. Notwithstanding this fact, some cases of inability to detect suspicions by DNFBPs have been noticed.
- d) FIs, have a good understanding of their CDD, ongoing monitoring and record-keeping requirements and apply them appropriately. DNFBPs comply with the basic CDD/KYC and record-keeping obligations, although employing less sophisticated control mechanisms when compared to FIs, which is in line with the lower degree of complexity of their businesses and their risk profile.
- e) The application of enhanced due diligence (EDD) is mostly made according to the risk scenarios determined by the law (*i.a.*, politically exposed persons (PEPs), high-risk jurisdictions or private banking) and mainly consist of a more frequent review of the customer, which is in line with the local legislation and international standards. Better performing entities within FIs (mostly among the banking sector) also adopt additional control measures that are commensurate to the risks identified for their own businesses. Similarly, obtention of support documents or review of external sources to ascertain customer declarations, including the source of funds, are, at least, undertaken as EDD measures, except in the cases of better performing FIs, who adopt this approach on a more regular basis.

- f) There is a widespread policy not to engage with a business relationship if the entity is not satisfied with the information held on the beneficial owner. The identification and verification of the identity of the beneficial owner are satisfactorily done via the use of several external sources, not solely based on the register of beneficial owners.
- g) Virtual assets service providers (VASPs) have no specific registration obligations and are instead registered as payment service providers (PSPs). Notwithstanding this fact, VASPs are REs and are supervised for AML/CFT purposes. Even in a context in which guidance for a harmonised approach is not provided by the authorities, VASPs demonstrated a degree of initiative and commitment in the implementation of preventive measures commensurate to the characteristics of their activities. In terms of relationships with other obligated institutions, no banks reported to deal with VASPs as customers, nor to undertake VASP activities themselves.
- h) Some banks and insurance companies, as well as most PSPs and VASPs met onsite to allow for online customer onboarding and identification processes. In such cases, entities have implemented effective control measures and verification steps to ascertain the identity of the customer and to avoid any potential risks associated with anonymity and non-face-to-face relationships.

***Recommended Actions***

Poland should take appropriate steps to ensure that:

- a) DNFBPs and some smaller FIs should conduct more specific risk assessments with the view of identifying specific ML/TF risks applicable to their own business, allowing them to establish more targeted preventive measures (including EDD measures) that are commensurate to such risks.
- b) Good practices on effective monitoring and SAR reporting are provided by the authorities, which should lead to an increase in the number of SARs from all reporting entities, especially in relation to DNFBPs and smaller non-banking FIs.
- c) There is less reliance on customer declarations, especially among DNFBPs, to comply with CDD/KYC obligations, shifting the focus towards verification of statements through external and reliable sources. Verification of the source of funds should be considered a regular CDD measure, and the degree of verifications should be enhanced for EDD.
- d) VASPs apply AML/CFT obligations in a consistent and harmonised manner, operating under a robust legal framework that includes specific licensing and registration requirements.
- e) DNFBPs are able to understand the differences between AML/CFT compliance and TFS implementation.

420. The relevant IO considered and assessed in this chapter is IO.4<sup>63</sup>. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23 and elements of R.1, 6, 15 and 29.

## 5.2. Immediate Outcome 4 (Preventive Measures)<sup>64</sup>

421. The banking sector, amounting to 92,3% of GDP in terms of assets, is by far the most material in Poland. Banks are also highly relevant in terms of risk; therefore, their level of compliance has a substantial place when weighting and concluding on the overall compliance of the private sector. Major players of the sector include entities that are part of bigger international financial groups (mainly EU-based) as well as Polish-owned banks with branches and subsidiaries of their own, both locally and abroad (mostly in neighbouring or close-ranged countries).

422. While the sector mainly targets polish natural and legal persons, foreign customers and complex structures (several layers of ownership, multijurisdictional) are equally onboarded (or present in the ownership chain of onboarded customers), albeit in a lesser capacity. The range of products and services includes, among others, traditional banking services, private banking or payment services, as well as insurance and investment solutions. Some firms have also put their focus on more innovative, technology-driven business lines.

423. Other sectors among FIs that draw attention are PSPs (rated by supervisors as the highest risk sector) and the currency exchangers. Although the PSPs sector is broadly characterised by its fully online presence, different profiles of entities can be spotted amongst the sector. While some entities belong to wider foreign groups or offer limited services (for instance, provision of e-commerce solutions to polish merchants), the risk seems to reside in smaller, less regulated and harder to identify PSPs, who offer more complex and sophisticated services, which hinder the traceability of transactions. Authorities have also detected cases involving such entities and organised crime. Nevertheless, in terms of materiality, those entities are marginal in the context of the Polish economy. Foreign currency exchanges are mostly polish-owned and have a limited number of offices across the country per firm since they are mainly familiar businesses managed by individual entrepreneurs. However, some entrepreneurs running foreign exchange offices also carry out VASP functions (as separate entities/businesses and not under the same FEO license), which is the sole reason for considering them with particular care in the context of the present report.

424. Other FIs fare lower in terms of relevance and risk. While insurance companies, investment firms and financial leasing companies can also be part of international groups, their

---

<sup>63</sup> When assessing effectiveness under Immediate Outcome 4, assessors should take into consideration the risk, context and materiality of the country being assessed. Assessors should clearly explain these factors in Chapter One of the mutual evaluation report under the heading of Financial Institutions, DNFBPs and VASPs, as required in the instructions under that heading in the Methodology.

<sup>64</sup> The first paragraph should give a short summary of what relative importance assessors have given to the different types of financial institutions, designated non-financial businesses and professions and VASPs, taking into account the risk, context and materiality of the country being assessed. This should be supplemented by a cross-reference to the more detailed information in Chapter One on how each sector has been weighted (based on risk, context and materiality) (as required in the instructions under that heading in the Methodology).

offer of services is limited (open-ended, closed, and pension funds for capital market firms and retirement and saving plans, as well as unit-linked products for insurance companies), aimed mostly at polish natural and legal persons. Collective savings and credit unions offer services exclusively to its members (polish residents), which are heavily standardised across the industry (mostly loans and short-term loans and, in a much less significant way, incoming foreign money transfers corresponding to recurrent payments and providing access to money remittance services).

425. DNFBPs as a whole are less material than FIs and are focused on the Polish market. Notaries and lawyers do not participate in activities such as opening or managing accounts or executing payments on behalf of customers, managing customer assets or management of incorporated companies. Lawyers, tax advisors, auditors and accountants tend not to be majorly involved in company or legal arrangements of incorporation activities, as such activities are concentrated among TCSPs, which were not bound to market-entry requirements at the time of the onsite and were less supervised as a result. Casinos are mostly land-based (only one authorised online operator) and with a similar profile: cash-intensive, offering a limited range of services and with a vast majority of local customers.

426. The VASP sector is composed of Polish-established companies, including: (i) 20 onsite exchange offices that require physical presence of the customer, which focus on converting FIAT to crypto and vice-versa; (ii) 3 online exchange offices that allow the purchase of cryptocurrencies and; (iii) institutions offering the instant exchange of cryptocurrencies via the so-called BitMats (3 operators). Poland adopted a restrictive approach in relation to this sector by flagging the cryptocurrencies operators as high-risk customers for FIs and requiring the application of EDD measures, which explains the low number of players and overall low materiality.

427. VASPs have been legally obliged to implement AML/CFT preventive measures since their categorisation as reporting entities in 2018. Entities are mostly being registered as PSPs as a temporary measure until the entry into force of the specific licensing and registration requirements that were being worked on at the time of the onsite. This measure allows the authorities to identify the number of actors and avoid the provision of unregistered activities, but in the same time could lead to an overestimation of the risks of the PSP sector and make determining the real scope and range of activities of each of the sectors more difficult.

#### ***5.2.1. Understanding of ML/TF risks and AML/CFT obligations and application of risk-mitigating measures***

428. All reporting entities are obliged to perform comprehensive ML/TF risk assessments associated with their activities (covering customer, geographical, products and services, transactions and distribution channel risks) pursuant to article 27 of the AML/CFT Act and to update them periodically or whenever changes in the business activity occur.

429. In practice, all entities met onsite have performed such assessments and formalised them into a written document, which is periodically updated. In the case of FIs, the assessment of risks is updated, on an annual basis, if not more frequently, whenever major events occur, such as adoption of new products or technologies or opening of new branches and subsidiaries. Similarly, all entities were aware of their AML/CFT obligations and implemented internal controls and procedures.

430. In terms of risk mitigation, obligated institutions generally use risk scoring models, which are effective tools to ensure that the preventive measures applied are commensurate to the risks

that each customer and transaction poses. These models rate business relationships into different risks categories (mainly low, medium, high and non-acceptable) based on different factors regarding the customer, such as country of residence, nationality, legal form, professional activity, source of funds or the bank products and services used. In this regard, banks and larger FIs perform the risk classification through IT systems that calculate and update the scoring automatically. The risk scores given to the customers are updated when significant changes in the business relationship (i.a., changes in customer data or alerts triggered by the transaction monitoring systems) materialise. The risk scoring model itself, the factors it takes into account, and their weights are mostly reviewed on an annual basis, pursuant to UKNF recommendations.

### ***Financial institutions***

431. Common practice within FIs, particularly the banking sector, was to conduct risk assessments even before the legal obligation entered into force in 2018. Assessments provided by some financial institutions were collected by the authorities to serve as a source for the elaboration of the NRA, although no feedback from the authorities was received by the OEs.

432. UKNF requests risk assessments from FIs as part of their onsite supervisory actions, although the provision of specific feedback or recommendations for improvement besides minor formal issues is rare. Feedback in relation to risk assessment shortcomings is most commonly provided in an aggregated form via the publication of general guidance related to the scope of the assessment, identification of risks, mitigating measures and their implementation or customer risk classification, among others.

433. The banking sector is knowledgeable about ML/TF risks which is, attributable, in part, to their belonging to international groups and conglomerates. Although the ability to identify specific ML/TF risks applicable to each of their entities and to adopt preventive measures commensurate with those varies in-between banks, it can be concluded that the degree of risk understanding across the sector is, overall, solid. Depending on their own business model, some entities mainly allude to more general risks, such as corresponding relationships, private banking, certain types of customers (PSPs, PEPs, etc.), high-risk jurisdictions or wire transfers, to name a few, while others, more focused on innovative business lines, are able to articulate specific risks better, such as those associated with non-face-to-face customer onboarding and provision of services, opening of branches and subsidiaries abroad, cross-border risks with jurisdictions they are particularly exposed to (mainly within the EU), trade finance or collective accounts.

434. Similarly, the adoption of mitigating measures for the banking sector relies on the risk profile of each entity, but, in general terms, the measures adopted are commensurate to such profiles. In this regard, those entities that mainly allude to high-risk scenarios covered by the AML legislation also refer to legislative AML obligations, such as availability of internal audit function, internal controls and procedures, training programmes, transaction monitoring, CDD/KYC procedures or application of EDD to pre-defined scenarios (private banking, PEPs, etc.), or augmenting the frequency of their implementation.

435. On the other side of the spectrum, those entities involved in providing more innovative products and services with better risk identification procedures have also implemented more tailored risk-mitigating measures. For example, entities that have identified risks related to non-face-to-face business relationships have implemented mitigating measures such as the use of digital identification tools (biometrics, ID scanning mechanisms, gathering information directly from the Polish electronic ID card, use of video tools and algorithms to verify the identity of the person appearing in it, etc.), imposing limitations to the accounts (thresholds, access to certain

products and services, etc.) and enhanced ongoing monitoring until physical identification can be accomplished or non-allowance of certain high-risk customers (PEPs, foreign customers, etc.) to be onboarded via such means.

436. Among measures to deal with risks, a fairly widespread practice is termination of business relationships that could be related to the risks identified, for example, reducing the number of accounts associated with PSPs, especially those with foreign ownership or that have been detected not to be licensed. These measures are to be understood within the framework of a growing tendency within the banks to be more risk averse and risk cautious, hinting at some instances of de-risking instead of risk mitigation.

437. Some of the risks that best exemplify the previous statement are those related to VA and VASPs. While those are frequently brought up as risks, there is a widespread consensus within the banking sector not to expose themselves to these technologies or to customers engaging with such activities.

438. Other FIs besides banks tend to have a less sophisticated risk understanding, which somehow mirrors their risk profile and complexity of their business. For example, while PSPs and foreign exchange offices are mostly able to identify specific risks and apply commensurate mitigating measures, other FIs (insurance, investments firms, financial leasing and credit unions) consider their sectors to be inherently low-risk, and the application of the AML/CFT regulation to be a sufficient mitigation measure. These general low-risk claims, while generally accurate, lead to less specific ML/TF risks identified and do not fully substantiate the translation of sectorial conclusions at each entity level.

439. In the insurance sector, most companies are part of wider international financial groups, and the risk assessments tend to be performed at the group level or with significant input and directions from parent companies. For the entities, such assessments allow them to adapt and graduate their internal AML/CFT preventive measures and enhance the monitoring in areas of higher risk. Most risks identified are product-related, although the general belief among entities is that their life insurance products are low-risk, which is in line with their risk profile. Authorities report some trends associated with the insurance sector, such as an increase in foreign customers, which pose greater difficulties to the CDD process, areas of decreasing risk, such as a low degree of cross-border activities or a shift from investment products to endowment products. However, these conclusions were not replicated by entities met onsite.

440. The capital markets and pension funds firms share a similar low-risk perception in relation to their products and customers, who are mainly Polish-based and, to a lesser extent, within the range of the EU. The fact that the funds corresponding to contributions and withdrawals from investment products have to circulate through the banking sector is also considered a risk-mitigating factor. On a less positive note, these considerations do not allow the sector to determine all ML/TF scenarios that could be applicable to their firms.

441. Payment service providers focus on the business activities of their customers, considering sectors such as casinos, DPMS or other cash-intensive businesses as riskier in terms of ML/TF or, in some instances, non-acceptable. Given the prevalence of online activities, PSPs identify the risks of non-face-to-face business relationships as their major focus in terms of risk and do adopt specific mitigating measures (digital identification tools like those mentioned for the banking sector).

442. Exchange offices are rightfully concerned about risks associated with acquisition and physical transportation of cash, high denomination banknotes and linked transactions. In terms

of mitigation of those risks, entities implement different measures, such as CCTV tools or controls over transactions below the legislative threshold over which CDD must be conducted.

443. Financial leasing institutions, by the very nature of their activities, do not consider themselves to be much exposed to ML/TF risks, as these firms do not hold accounts on behalf of customers, nor do they accept cash as means of payment, but only wire transfers. The AT agrees with this conclusion. The sector is mostly concerned with the exposure to monetary damages (not ML/TF-related) due to fraud risks such as use of fraudulent documentation or non-provision of the assets subject to leasing.

444. Collective savings and credit unions are in a similar position regarding their perception of exposure to ML/TF, which has not led to identification of any particular sectorial risk or at the level of each entity. The reasonable arguments to support such assessment is the provision of products and services solely to natural persons, members of the union and residing in Poland, and their limited range and amounts, mainly including loans, accounts and fixed-term deposits and, in a much lesser capacity, insurance brokerage, electronic banking, outgoing money remittances and incoming wire transfers.

### ***DNFBPs***

445. In general, risk understanding amongst DNFBPs is lower than that of financial institutions, in particular when compared with the banking sector. However, there are differences between DNFBPs. While casinos are able to articulate specific risks and mitigation measures, risk understanding from other DNFBPs mainly alludes to general risks, academic typologies or knowledge about the AML/CFT legislation and its implementation. Similarly, belonging to sectors perceived as low-risk or the participation of other obligated institutions (like banks) in their services are considered sufficient mitigating measures. In these cases, risk understanding is lower and, although risk assessments are conducted, these tend to be formalistic exercises aimed at complying with the legal obligation but do not lead to the identification of specific ML/TF risks or mitigating measures applicable to the entity.

446. The real estate sector is considered to be exposed to an average or medium level of risk (therefore not sharing the NRA conclusions for the sector) and does not identify any particular ML/TF risks. The reasoning behind this is that cash is not accepted in real estate transactions; hence all transactions are settled through the banking system, which exercises its own controls. There is a view that potential launderers tend to target smaller-scale real estate agencies, not part of bigger national or international groups, which seems to be correct. The sector tends to confuse the individual risk assessment at the entity level with the assessment of risks on a customer/transaction basis and the adoption of CDD/KYC measures.

447. In relation to tax advisors, auditors and accountants, they periodically conduct risk assessments, although these are limited to broad, academic risks associated with cross-border tax services. The general understanding alludes to ML/TF risks being mitigated by refusing to perform transactions on behalf of customers. Furthermore, the sectors do not share the views of the NRA in relation to the high risks associated with accounting services, nor do they consider it to be particularly helpful due to its main focus being towards FIs.

448. It should also be noted that representatives of accounting-related sectors referred to the risks associated with shell and shelf companies and the misuse of legal persons in general, despite not being directly applicable to them due to their lack of engagement with company incorporation activities. Such risks were said to be related to underregulated TCSPs, whose registration obligations would not come into force until after the onsite, and the potential abuse of the online

company incorporation procedure (S24 electronic system), which allows to set up limited liability companies without requiring physical presence in Poland nor a notarial deed but requires electronic signature and submission of the articles of association online.

449. Lawyers and, even more so, notaries do not share those views in relation to shell companies risks, considering that those are mostly mitigated by the controls exercised before the granting of a notarial deed (non-registration of companies without physical presence and effective address in Poland, identification of proxies, no possibility of anonymous parties, etc.), although they recognise the difficulties associated with the identification of shell companies at the time of their incorporation. Besides those remarks, the understanding of legal professions in relation to ML/TF risks mostly resides in knowledge about AML/CFT obligations, their implementation and knowledge of the Polish legal framework in general.

450. Lastly, casinos consider that the findings of the NRA are more applicable to a different profile, namely bigger casinos. They have identified several ML/TF risks of their own, which mainly include exchanges from chips to currency unlawfully claimed as winnings, payment of prizes via wire transfers, associated persons to assure winnings by placing opposite bets and exchange of small banknotes into higher denomination ones.

451. Several mitigation measures to address those risks are in place, such as the issuance of certificates of winning after ascertaining, via CCTV controls, that the player has indeed been playing and won, checking that the bank account where the winnings are sent is linked to the customer (for example, by checking that the account is related to the credit card used to acquire the chips) and determining the source of funds before exchanging large sums of low-denomination cash.

452. The sector also acknowledges the potential threats of illegal online gambling but considers the probability very low, and in any event, those would be banned from issuing winning certificates.

### **VASPs**

453. VASPs have identified ML/TF risks related to anonymity and the overall acknowledgement of their activities being high risk. The need for a blacklist of crypto wallet addresses at an EU level as a means to mitigate the risks associated with VA transactions was mentioned during the onsite. Regarding the AML/CFT obligations, the entities considered that becoming reporting institutions has not had any major impact in terms of their internal controls and procedures, as they were already in place, which shows a good degree of awareness and understanding of their obligations and their commitment to implement preventive measures.

#### ***5.2.2. Application of CDD and record-keeping requirements***

454. In general terms, obligated institutions, in particular FIs, have a good understanding of their CDD, ongoing monitoring and record-keeping requirements and apply them appropriately. If all necessary CDD data cannot be obtained, business relationships are generally not initiated or terminated. Similarly, a “no beneficial owner, no business” approach seems to be governing all business relationships across all RE. The mechanisms and tools for the implementation of these CDD measures depend on the type of business, scope of activity or resources available. For instance, more complex institutions (such as banks and larger FIs) have more sophisticated resources at their disposal (software and analytical tools, access to databases, dedicated human resources, periodic reporting to the Management Board, internal control and audit functions, etc.)

whereas smaller entities rely less on sophisticated IT tools and more on simpler IT tools and manual checks, in line with their size and complexity.

455. Supervisors (mainly UKNF) assess compliance of FIs against CDD obligations. Through their supervisory actions, some isolated, non-systematic shortcomings in the implementation of some CDD measures (customer screening, identification of the beneficial owner, no application of CDD in certain occasional transactions or overreliance in customer declarations) and record-keeping requirements (failure to document and keep analyses) were detected for certain entities.

### ***Financial institutions***

456. The banking sector is particularly aware and correctly applies CDD obligations. In this regard, customers are duly identified during the onboarding process via ID documents, external databases or company incorporation documents for legal persons. Other CDD measures beyond identification and verification of the identity include gathering information relative to customer knowledge (KYC), such as the source of funds, the ongoing monitoring of the business relationship through dedicated alert systems or the establishment of mechanisms for customer acceptance (i.a. several stages of approval depending on the level of risk).

457. The application of CDD and updating of CDD data are equally graduated depending on the risk rating assigned by the scoring systems. The degree of reliance in customer declarations depends on the entity: while some mainly use them to pursue CDD and limit the use of external, independent sources to high-risk business relationships (that is, as an EDD measure), others perform external sources checks regularly. Ascertaining source of wealth is almost exclusively relegated to an EDD measure for business relationships with PEPs, as is required by the standards and the national legislation.

458. Regarding beneficial ownership, the sector adopts measures to understand the structure of ownership and control of their customers and to be satisfied with who the beneficial owner is. These measures include both customer statements and checking independent and reliable external sources, such as external databases or public registers (national and international), including the National Court Register and the Central Register of Beneficial Owners.

459. The banking entities are fully aware of the fact that the latter cannot be the only source they can rely on to determine who the BO is. For example, one of the entities met onsite maintained that, whenever encountering differences between BO information held by the Register and their own analyses, these are further analysed and documented, in views of the upcoming legal amendments that will require reporting these discrepancies to the authorities. BO information of the whole customer portfolio is periodically reviewed and updated, whenever deemed necessary, by the internal audit function or other dedicated teams or departments to detect any changes in ownership and to ensure the validity and relevance of the data on an ongoing basis.

460. Termination of business relationships when unable to pursue CDD (including determining the BO) is a widespread practice among banks, as expressly regulated by the legislation, although numbers of instances can differ greatly between entities, depending on their more or less conservative approaches. Other risk-appetite reasons to not onboard customers or to discontinue business relationships include certain higher-risk industries and businesses, shell companies or unlicensed professionals.

461. In terms of record-keeping requirements, banks keep, mostly in electronic form, all the relevant data and information for AML/CFT purposes (not just ID documents, but also evidence

of analyses and controls performed) for five years from the date of the end of the last business relationship that the customer had with the entity (that is, taking into account all products contracted by the customer). UKNF has detected some failures to comply with these obligations but qualified them as “minor”. The AT has no reason to challenge this conclusion.

462. The application of CDD mainly rests on the banking entity, notwithstanding the outsourcing of some support tasks (provision of IT tools, centralisation of information and data, etc.) to external consultancy firms. However, a certain trend of using courier companies/postal offices as delivery channels has been detected by the UKNF and was confirmed by some of the banks interviewed onsite. The supervisor does not consider this practice risky since the scope seems to be limited to customers holding a Polish ID card. However, the full extent of such relationships, the degree of involvement of these parties in performing CDD obligations (which, at least, include customer identification and gathering of KYC information duties) and their accountability in cases of failure is not fully clear or formalised.

463. Most of the statements made for the banking sector in relation to the implementation of CDD (including BO identification) and record-keeping requirements can also be applicable to other FIs. However, certain sectorial particularities can also be found.

464. The insurance sector adapts CDD measures in relation to the delivery channel used, which include vast networks of agents and brokers (who act as the first line of defence, identify the customer and gather KYC information), and remote onboarding (when specific IT tools for customer identification are used). The sector also notes how complex structures tend to be more present in investment policies, thus making the BO identification harder, although external databases and the Central Register of Beneficial Owners are used as sources in all cases. In terms of transaction monitoring, the sector is remarkable in establishing logic algorithms and alert systems to track sectorial-specific typologies, not just taking into account the transactions themselves but also all participants in the insurance contract.

465. Some exchange offices pay particular attention to potentially linked transactions (mainly related to tax avoidance) and customers acting on behalf of companies when determining their CDD measures. Specific questions aimed at detecting such circumstances are put in KYC documents, or lower thresholds than those of the AML Act (€15 000) are applied to start recording transactions and pursuing CDD. Other measures include setting communication, information sharing and real-time control mechanisms between different offices belonging to the same exchanger. It must be noted that the implementation of such controls goes beyond the legal obligations, depending on the initiative of each entrepreneur, and is not due to dissemination of best practices or other types of encouragement by the supervisors.

466. Investment firms’ main distribution channels are tied agents, who are authorised and supervised by the UKNF and can be investment firms themselves (e.g. brokers), which are subject to licensing and AML/CFT requirements. Regarding the termination of business relationships when unable to pursue CDD, some capital market companies sell open-ended investment funds that do not allow customer rejection due to the nature of public products. On a positive note, the sector claims to have never encountered any suspicions related to these types of business relationships. In terms of beneficial ownership, companies periodically check external sources (mostly national registers), basing the frequency on the risk assigned to the business relationship. In this regard, the sector detected differences between their own BO analyses and the information held by the national register and expressed some concerns about the accuracy, validity and completeness (lack of associations and foundations) of its information.

467. PSPs often check external sources (open sources, external databases, contracts, invoices, etc.) when pursuing CDD to ascertain the payment, as well as the customer profile and its business activity. In terms of source of funds, however, PSPs that mostly serve Polish merchants (payees) consider that the verification of this point should more reasonably be carried out by the banking entity from which the payment comes. Regarding ongoing monitoring requirements, the ex-post controls take into account all elements of a transaction (that is, the payer, the payee, the beneficial owners and/or representatives of legal persons and the rationale behind the transaction received by the customer), as well as transactional history (including cases of reimbursements or refunds). In case alerts are triggered, further documentation is requested, and if the entity is not satisfied, several measures can be undertaken (blocking of the account, suspending the transaction, reporting to GIFI, etc.). Other CDD measures implemented by some PSPs include requesting internal policies, risk assessments or the results of the internal audit to customers who are FIs. In relation to the beneficial owner, some entities mentioned having detected legal arrangements, such as trusts, in the chain of ownership of some of their customers, evidencing the presence of more complex structures, whose beneficial owner is determined by regularly checking the sources already covered for other FIs. Evidence of all controls described is subject to record-keeping requirements and not just customer identification documents.

468. Leasing companies not only implement KYC procedures but also KYS (Know Your Supplier), as their CDD systems take into account three factors: customer, supplier and asset. KYS measures include verifications such as onsite visits to the suppliers, checking external databases to ascertain beneficial ownership or consulting open sources of information to check the business activity and the existence of negative news. The purpose of the business relationship is also a point of focus, as companies determine whether the need to lease a particular asset is consistent with the business activity of the counterparty. The leasing sector also employs a significant sales force as delivery channels (first line of defence), although the customer identification process is centralised. The role of the sales agents is limited to gathering customer information, but not their acceptance. Termination of relationships is only related to suspicions and cases in which the beneficial owner cannot be determined. In terms of ongoing monitoring, and due to the nature of the business, the focus is placed on performing periodical reviews of samples of KYC and BO information, detecting changes in behaviour from what was established at the initial contract and tracking typologies such as payments after the date of the instalment or after 30 days from the due date of the contract.

469. Credit unions usually work with natural persons acting on their own behalf; therefore, BO identification is a much less significant issue for the sector. CDD measures are mostly related to determining the range of products of interest and the expected account balance, factors that will be taken into account during the ongoing monitoring to detect behavioural deviations, like cases in which natural persons act as business owners or cards exceeding certain amounts, thus raising suspicions about not being used for the expected purposes. Detection of such typologies can lead to risk rating increases or reporting to the GIFI. Unions have integrated into their systems the record-keeping obligations in order to ensure that customer identification documents, as well as support documentation (source of funds, notarial deeds, forms, declarations, etc.), are kept for a period of 5-years after the end of the business relationship.

### ***DNFBPs***

470. DNFBPs comply, in general terms, with the basic CDD/KYC and record-keeping obligations. For transaction monitoring, less sophisticated tools are employed when compared with FIs, although it should be noted that most non-financial professions, by their very nature, do

not engage with long-term business relationships involving transactions. Regarding the effectiveness of the measures implemented by the sectors, some results of inspections carried out by the GIFI show certain failures in the identification of the beneficial owner, determination the customers' ownership structure (and documentation and retention of such analyses) or examination of the source of funds, but this is rather rare and not systematic.

471. The real estate sector complies with customer identification and KYC obligations, although these are limited to just the part of the transaction that they are representing (either the buyer or the seller). Identification of BO is mostly limited to customer statements, although in certain situations deemed to be of higher risk, external sources (mostly national registers, including the Central Register of Beneficial Owners) are checked too. All verifications are once again performed for recurring customers. In terms of source of funds, the sector claims that two situations prevail: i) transactions previously carried out by them, where this previous selling is considered as the source of funds, or ii) transactions associated with bank financing (mortgages), where the responsibility to perform the verifications falls on the banks. In general, although the sector implements CDD measures, it does not always understand the need for their implementation besides for legal compliance purposes, as the involvement of notaries and the banking sector in real estate transactions can be considered as a sufficient preventive measure. Regarding record-keeping, all relevant documents (ID, VAT number, powers of attorney, BO information, etc.) are kept for a period of five years from the date of the transaction.

472. Notaries and lawyers perform CDD/KYC procedures on their customers, including conducting background checks in external sources. When company incorporation is involved, the measures are stricter, and BO identification and justification of the source of funds is pursued. In the case of notarial deeds, physical presence is always required; hence, there is no possibility for anonymous parties. The statements made in the deed are ascertained based on information held in public registers and/or documents.

473. Accountants, auditors and tax advisors all have CDD processes in place, collect customer information using credible external sources (mostly open sources of information and external databases), analyse the ownership structure of their customers and determine the BO via the use of external sources (mainly the National Court Register and the Central Register of Beneficial Owners, acknowledging that the latter cannot be the only source).

474. Casinos identify every person entering their premises using CCTV systems and requesting ID documents. Certificates of winning are issued and payouts above a certain threshold (around €500) are recorded. The systems implemented ensure that there is no potential anonymity at any stage. KYC forms are only applied to high turnover customers (which also grants them the rating of high risk). Source of funds is not pursued systematically, but only in instances where certain suspicions are raised (for example, customers attempting to exchange large sums of small-denomination coins) via the means of documentation or explanations provided by the customer, checking external databases or performing internet searches. The sector claims that considering their business profile (do not engage with long-term relationships or cross-border transactions), the AML obligations are not reasonably tailored to their business.

#### **VASPs**

475. VASPs have implemented formal AML/CFT procedures, covering CDD and record-keeping obligations, although, in practice, controls are implemented on a transaction per transaction basis due to the quickly evolving nature of their businesses and the ML/TF schemes associated with their activities. This leads to controls being implemented above certain thresholds and conditions

defined by each entity, which are periodically reviewed and updated. This fact, however, demonstrates the initiative and commitment of the sector to implement preventive measures that are commensurate to their businesses and risks in a context in which a lack of legal framework and guidance from the authorities hampers the adoption of a more unified approach.

476. Due to their fully online nature, customer identification is performed remotely (ID scanning or multiple pictures of the customer showing an ID document), alongside several security mechanisms (geolocation to ensure the customer is located in Poland, ascertaining the address via invoices or phone calls, detection of anonymous IPs, monitoring of red flags and certain keywords, etc.). Verification of the source of funds is also threshold and suspicion-based according to the criteria defined by each entity (for example, an amount that does not correspond with the claimed business activity). While the sector relies on the fact that funds can only come from and be transferred to Polish bank accounts, it also ensures that the accounts involved are linked to the customer without any third parties involved. Additionally, representatives who met onsite acknowledged the risks associated with their line of business, such as anonymity or the difficulties in tracking the funds once leaving the scope of their exchanges.

### ***5.2.3. Application of EDD measures***

477. The circumstances in which EDD must be applied, regardless of any other characteristics, are covered by the AML/CFT legislation and can mostly be summarised in private banking customers, PEPs and high-risk jurisdictions, as well as the implementation of restrictive measures whenever positive matches pursuant to UNSCRs, are detected. GIFI assesses compliance with these EDD requirements through supervisory activities, which have allowed it to detect certain shortcomings in relation to PEP obligations in some entities.

478. Banks and larger FIs are exposed to a greater number of high-risk scenarios: corresponding banking, use of new technologies, private banking, PEPs or high-risk customers (PSPs, certain industries, complex structures (trusts, multijurisdictional ownership chains, etc.)) and as a result, use more sophisticated systems (commercial databases, automated systems, additional research from open sources, customer and transaction screenings, etc.) to implement the necessary EDD measures.

479. EDD measures mostly consist in incrementing the frequency and intensity of regular CDD measures. In the case of FIs, it includes ascertaining the source of funds and wealth via external support documentation, enhanced transaction monitoring and analysis by reviewing documents allowing for a better understanding of the transactions (agreements, contracts, invoices, etc.), a more frequent reassessment of customers and update of their data, establishing several layers of approval for the business relationship, customer screenings against external databases and adverse media or onsite visits to customers (in the case of leasing companies) etc. If customers do not provide the information required for the implementation of EDD, entities tend to submit a SAR or even end the business relationship. DNFbps tend to avoid high-risk business relationships, and, as a result, the implementation of EDD is limited in practice.

### ***PEPs***

480. In general terms, obligated institutions identify the condition of PEP of their customers and beneficial owners, require authorisation from senior management to establish or continue business relationships with them and determine their source of funds and wealth, as the legislation requires. In the case of FIs, especially larger ones, PEP condition is identified through screenings against external databases, both at the onboarding and periodically during the course

of the business relationship (mostly overnight), in order to detect any changes from the initial status.

481. Some representatives of the PSP and insurance sectors rely on customer declarations during the onboarding phase, but subsequent checks are done via automatic screenings. In the particular case of insurance companies, checking PEP status is extended to other participants of the contract, like the assured person or the beneficiary of the policy before the payout. Similarly, PSPs consider both the originator and beneficiary in their screening to determine PEP status, including those performed at the time of processing the payment. Investment firms pointed out the fact that, prior to 2018, only foreign PEPs were classified as such and that they needed to adapt their systems to include national PEPs after the legislative change. Credit unions consider the presence of PEPs in their sector to be rare. Regarding verification of source of funds and wealth, public information bulletins, notary confirmations, contracts or payroll documents are used.

482. DNFBPs place a higher reliance on customer declarations to ascertain PEP status and the source of funds/wealth. Tax advisors, accountants, auditors and lawyers present low numbers of PEPs as customers. Representatives of the real estate sector interviewed, despite complying with the legal obligations of PEP identification, did not fully comprehend the reasoning behind those obligations nor the risks associated with business relationships with PEPs. In the particular case of casinos, screening against lists from external providers (including PEPs) is mandatory when accessing their premises. Although the sector claimed never to have encountered any positive matches, it also expressed some concerns about the accuracy of the lists, which led them to implement customer declarations subject to criminal liability in case of false declaration. Furthermore, casinos also expressed difficulties in implementing EDD measures, like verifying the source of funds, due to the nature of their business and consider that there should be greater involvement from the authorities in providing tailored guidance about their expectations on how compliance with such obligations should be achieved.

483. VASPs implement real-time and ex-post screenings against PEP lists, updated on a 24-hour basis. As is the case for identification and CDD, not all transactions and customers are scanned, depending on the criteria and thresholds established by each VASP. Representatives who met onsite stated that they never identified a PEP among their customers. One of them received an onsite inspection by the UKNF, which concluded that the frequency of PEP screening was insufficient. The shortcoming was subsequently remediated by the VASP.

### ***Correspondent banking***

484. Polish banks engage, in large numbers, in corresponding relationships with banks abroad and provide such services to foreign banks who wish to operate in Poland. Such relationships are considered as high risk, which warrants the implementation of EDD measures like assessing the respondent entity in terms of customer, geographic and product risk, demanding their AML/CFT policies and procedures, requesting information via standardised and periodically updated questionnaires (Wolfsberg group), ensuring that the entity is duly licensed or conducting background checks and checks against sanctions lists, among others. Unless these criteria are fully met, the correspondent relationship is not established. In some instances, corresponding banking relationships are provided intra-group, in which case the customers accessing those services are already onboarded and subject to CDD by the group matrix or branch, and the Polish banking entity can have access to such information. One entity brought up the fact that having PSPs as customers raises concerns among correspondent banks abroad and that the

implementation of EDD measures towards these types of customers (implementation of periodic requests of information regarding their degree of compliance with AML/CFT and sanctions lists screening obligations) was well received by the foreign entity and allowed establishing the corresponding relationship.

485. Regarding VASPs, no evidence could be gathered onsite in relation to implementation of due diligence measures to counterpart VASPs (akin to corresponding banking relationships) when facilitating transfer services.

### ***New technologies***

486. As already stated, adoption of new technologies is significantly present in certain banking entities and insurance companies, as well as the VASP and PSP sectors. New technologies are mostly associated with remote identification and provision of products and services, including contactless payment services. Although most entities, as described in section 5.1.1, implement commensurate risk-mitigating measures (which fall within the scope of EDD), these are applied in a non-harmonised manner (that is, at each entity's own initiative), as a result of a lack of standardised risk assessments prior to launch or adoption of new technologies. In terms of exposure to new technologies via customers, obligated institutions have very little appetite for VASPs, VA-related customers and PSPs.

### ***Wire transfers***

487. Wire transfers rules are applied by banks and other FIs in accordance with EU Regulation 2015/847. Compliance with wire transfer requirements is checked via UKNF controls and supervision activities (specific checks regarding payer and payee information on a sample of selected messages), which detected some failures mostly related to small and medium-sized enterprises with less significant risk profiles.

488. The banking sector monitors cross-border incoming and outgoing wire transfers in real-time and via ex-post analyses, including those of the branches. Controls aimed at ensuring that wire transfers are accompanied by the necessary originator and beneficiary information are applied to all transfers, irrespective of the amount, and include suspension of transactions lacking completeness in this regard and the periodical review of samples of already processed transfers to ascertain the proper functioning of ex-ante controls. Additionally, banks implement threshold-based controls that pursue the goal of detecting suspicions, also both in real-time (checking keywords and phrases, the existence of numbered accounts or unrelated parties, etc.) and ex-post (coherence with the customer transactional behaviour). The alerts trigger the analysis of the corresponding AML department, and if the suspicion is confirmed, a SAR is filed. Alerts generated ex-post can also be carried over to real-time controls, suspending subsequent transfers associated with the account until expressly authorised. White-lists (exclusions from controls) are very rarely used and are often limited to temporary uses in relation to previously generated alerts by an account that has already been positively analysed.

489. Credit unions also provide wire transfer-related services, although in a much less significant capacity. In this regard, the limited amounts of incoming wire transfers are always monitored by IT systems shared across all unions and are subject to intermediary supervision (the National Union). The sector also provides access to money remittances services by a worldwide financial services company, the only service offered to the general public and not just union members, although these types of customers are subject to the same CDD/KYC requirements as any member of the union would be.

490. PSPs implement similar real-time and ex-post controls to those of banks for wire transfers when processing payments. Real-time checks include determining the coherence of the payment in relation to transaction history, scanning of keywords and red flag scenarios, non-allowance of certain words or characters in mandatory fields for issuing the payment, IP tracking, etc. These criteria are periodically reviewed and updated. Payments can be put on hold until they are duly analysed and the PSP is satisfied with the explanations and/or additional documentation before authorising them.

### ***Targeted financial sanctions relating to TF***

491. In terms of TFS, banks automatically check customers, beneficial owners, other participants of the business relationships and transactions against international sanctions lists (including those of external providers of databases, UNSCRs, EU, local ones provided by the GIFI, dual-use goods, etc.), during the onboarding, in real-time when a transaction is conducted and periodically (mostly daily, with lists being updated on the same frequency). Most of these IT solutions are provided at group level. In case of positive matches, the transaction is suspended, or the account is blocked, and a notification is sent either to the GIFI or to the PPO, who then proceeds to give further instructions (including unfreezing in cases of false positives).

492. Other FIs (PSPs, investment firms, insurance companies, credit unions and leasing companies) implement similar procedures adapted to their own business, size and complexity, although cases where transactions or accounts needed to be blocked and notified are much rarer, non-existent or the result of false positives. Investment firms expressed some concerns regarding delays in lists updates by external providers. Credit unions confuse the notion of high-risk jurisdictions with that of sanctions lists and do not differentiate between measures for AML, CFT and TFS. In the case of foreign exchange, checks are performed on the spot based on the self-generated list provided by the GIFI for those attempted transactions over a certain threshold (€15 000 according to the legislation, or lower if the entrepreneur has so decided). In case of hits, the amount would not be exchanged. Verification of further scenarios, besides sanctions screening, that could be potentially linked to TF is not common among smaller, less material FIs.

493. DNFBPs mostly conduct manual checks on sanctions lists provided by the GIFI through its website. Sectors with greater legal knowledge (notaries and lawyers) are more aware of restrictive measures that would have to be implemented in case of a positive match, which would include notification to the GIFI and the PPO, blocking of the provided funds and the non-provision of services. Other sectors (real estate) understand the concept of “lists” in a broad sense and would equally treat matches in any list (PEPs, sanctions, high-risk jurisdictions, etc.). As stated, screening against lists, including sanctions, is systematically performed for all customers visiting a casino. However, situations that would lead to TFS implementation are very rare for DNFBPs.

494. As explained for PEPs, VASPs run real-time and ex-post screenings, including international sanctions lists, of their customers and transactions, when the criteria determined by the VASP is met (which can include nationality, potential suspicions raised during the remote identification process or the transaction history, amount of the transaction, etc.). There have been no notifications of implementation of TFS by VASPs.

### ***Higher-risk countries***

495. Obligated institutions have internally implemented lists of high-risk countries, based mainly on FATF and EU lists, guidelines from the GIFI and, in the case of bigger FIs, also following indications from the international financial group, among other sources. These lists are regularly updated. In some instances, entities have also developed lists of prohibited entities in relation to

their own risk appetite. Links with high-risk jurisdictions are detected via screenings against the lists (or manual checks for small FIs and DNFBPs) at the onboarding or during the ongoing monitoring of the business relationship.

496. EDD measures implemented in relation to customers, beneficial owners (or any other participants in the business relationship) or transactions linked to high-risk jurisdictions are mainly those implemented in any other high-risk scenario determined by the AML/CFT legislation (higher intensity and frequency of CDD), including rating that particular customer as high-risk. On top of that, certain sectors, like banks, have additional dedicated tools to monitor transactions linked to high-risk countries and suspend them in real-time until further analysis is conducted. Some banks adopt a stricter approach by not accepting any business relationship where high-risk jurisdictions are involved. This approach is also shared by other FIs (insurance companies, credit unions, etc.) and most DNFBPs and VASPs as well. Regardless of the approach, it should be noted that all obligated institutions met onsite claimed scenarios in which high-risk jurisdictions are involved are either rare or non-existent.

#### *5.2.4. Reporting obligations and tipping off*

497. Obligated institutions are, overall, aware of reporting obligations, either those falling under the scope of article 74 of the AML/CFT Act (circumstances pointing to potential ML/TF) or article 86 (blockage of accounts or suspension of transactions due to justified suspicions of ML/TF). Reporting from banking entities accounts for the vast majority of SARs, with numbers oscillating between 100 to 500 reports per entity per year. The same can be observed regarding the number of blocked accounts.

498. For transaction monitoring and detection of suspicions to consider for reporting, bigger FIs, in particular the banking sector, rely on automated alert-generating systems. Their degree of development depends on the degree of sophistication of compliance function, its size and the complexity of activities. UKNF reviews the effectiveness of such systems, the management, analysis and closure of alerts and their timeliness, as well as compliance with reporting obligations to the GIFI and its promptness. Although the feedback is mostly positive, the monitored scenarios do not always fully align with the risks identified by the entity.

499. Regarding the typologies reported by the sector, there is not one single pattern. Some entities refer to risks detected in the NRA, such as tax crimes or VAT frauds, and claim to have detected and reported cases associated with those risks (for example, companies suspected to be involved in carousel schemes). Other entities consider the NRA conclusions not applicable nor useful for them and focus their detection systems on other typologies such as the trade of illegal pharmaceuticals, investment frauds, transfers of funds outside Poland via cash withdrawals or Polish companies with foreign ownership.

500. There is a widespread consensus among banks to adopt a qualitative approach rather than a quantitative one in terms of SARs. In this regard, the aim is for SARs not to be limited to a particular customer or transaction, but to rather to typologies or cases involving multiple customers and accounts, taking into consideration the entire transaction history and even resorting to information and documents held by branches, subsidiaries or the matrix of the group to be able to provide the overarching picture of the case. Contacting the GIFI before submitting the SAR to comment on the case is also common practice, as is terminating business relationships (which can range from 0 to more than 800 depending on the institution) rather than onboard customers that could potentially be reported later on, thus decreasing the overall count of SARs.

501. Notwithstanding the above, supervisors (GIFI and UKNF) have detected some shortcomings concerning transaction monitoring, analysis, and reporting by some obligated institutions in relation to insufficient substantiation of suspicions. However, none of the entities that met onsite reported to have received any feedback after a SAR is submitted, unless the case is forwarded to the PPO or whenever the blockage of an account or the suspension of transaction is triggered at the request of the GIFI or the PPO. Some banks met onsite acknowledge the lack of feedback as a serious issue and claim that it impacts their capacity to determine whether they are complying adequately with their reporting obligations or not.

502. Other FIs besides banks submit far fewer SARs, which is in line with the materiality and the risk of the sectors. The numbers oscillate from 18-22 SARs per year for the capital market sector to 18 to 72 SARs for the PSPs (statistics are presented under IO6). Although the typologies monitored mainly allude to customer behavioural changes and other sectorial-specific scenarios triggered ex-post by the alert systems, the actual suspicions reported are managed on a case-by-case basis, and not many clear patterns can be established. Generally, the volume of the SARs reported follows the materiality and risk patterns, although, in the case of certain sectors (mostly currency exchangers), the reporting system is an area for improvement.

503. In terms of blockage of accounts, suspension of transactions and seizure of assets, these other FIs also receive requests from the GIFI and/or the PPO, either at their own initiative or as a result of the reporting of the FI, albeit much more occasionally.

504. Some sectorial particularities can be spotted, such as: (i) difficulties expressed by PSPs to report the whole case when providing services to only one of the parts of the transaction (the payer or the payee); (ii) the splitting of big amounts into different accounts at different entities for credit unions; (iii) the preference of exchange offices to deny the exchange when there are suspicions rather than reporting them later; (iv) the focus of financial leasing companies on fraud risks, which leads them to report hundreds of cases per year to the PPO but no ML/TF SARs or; (v) the fact that the monitoring of sectorial-specific scenarios by the insurance companies, such as contribution and surrenders from parties unrelated to the policyholder, or their focus on new trends, such as the abuse of certain investment products for tax evasion purposes, does not lead into higher SAR numbers.

505. DNFBPs report less than most FIs. Entities filing low numbers of SARs tend to consider potentially reportable cases to be theoretical and not applicable to them or perceive their activities to entail a low risk of ML/TF. There were instances where customers declined starting the business relationship if CDD/KYC measures were pursued, but in such cases, not enough information has been gathered to issue a SAR. Similar to the views expressed by some banks, some DNFBPs deplored a lack of approachability of the GIFI during the reporting procedure and the subsequent feedback.

506. VASPs started to report in 2018 when they became REs according to the law, although the vast majority of SARs can be attributed to the year 2020 (up to 50 SARs). Considering their relatively recent inclusion as REs, this can be considered as a positive start.

507. Regardless of the number of SARs, a general pattern across all sectors, both financial and non-financial, is the lack of SARs involving TF. In terms of FIs that have automated transaction monitoring systems, the availability of specific TF-related scenarios within those systems is not common, and the screenings are mostly limited to sanctions lists screening and adoption of freezing measures in cases of positive matches.

508. Most entities are aware of the prohibition to inform customers about filed SARs, accounts blocked, and transactions suspended, which has been duly transposed into their internal controls and procedures, determining what is allowed to be shared with customers under such circumstances. This is reinforced via additional measures, such as specific employee trainings in this regard. Despite this fact, entities do not consider further questions from customers whose business relationship has been terminated to be frequent.

#### *5.2.5. Internal controls and legal/regulatory requirements impending implementation*

509. FIs, DNFBPs and VASPs implement internal controls and procedures that regulate the application of preventive ML/TF measures within the entity, including issues such as recurring customer checks, regular reporting or analysis and identification of suspicious transactions, among others, with the aim to comply with the AML/CFT obligations set in the legal framework.

510. The implementation of internal controls and procedures, internal and external audit functions by FIs takes into account recommendations and principles from the UKNF, which also reviews their implementation and effectiveness via inspections, allowing detection of shortcomings in relation to the effectiveness of the procedures.

511. Most banks and larger FIs belong to international financial groups and implement robust policies and procedures at that level. This fact does not prevent the implementation of the local AML requirements, as international groups to which Polish FIs are part of are mainly EU-based, therefore implementing similar international AML standards. Although FIs are working towards greater harmonisation of processes across the group, discrepancies between the local requirements and the international standard can still appear. If the latter is stricter (for example, implementation of BO identification procedures for cases of 10% of share capital or above), which tends to be the most frequent case, addendums or waivers can be applied to local procedures in order to implement the group policy; in any other instance application of Polish requirements prevails.

512. Implementation of group-wide procedures has improved the overall degree of AML compliance due to additional inspections, controls and reporting from and to the parent company. It has also favoured an environment in which there is fluid and frequent communication across the group, which allows, for example, the exchange of information to form a complete picture of a customer for the purpose of suspicions reporting, or the implementation of periodic committees to exchange views, share approaches or propose modification to ML/TF monitoring scenarios.

513. Larger FIs and, more prominently, the banking sector have developed their internal compliance and internal audit functions to a significant degree. In this regard, most of them operate under a three lines of defence model in which the compliance department or the specific unit dealing with AML/CFT issues acts as the second line, exercising functions in relation to customer acceptance and risk appetite policies, authorisation of high-risk customers and overall assurance of the correct implementation of the AML/CFT procedures. Regarding internal audit, this instance of control allows entities to detect shortcomings regarding the implementation of AML/CFT policies and procedures in areas such as BO and PEP identification and monitoring, which have led to improvements in these processes.

514. Smaller FIs and DNFBPs, mainly targeting the Polish market, have internal procedures focused on the local AML obligations. Their degree of effectiveness differs amongst sectors and entities; that is, while some internal procedures are tailored to the risks faced by the entity and

accurately represent the specific preventive measures implemented by it (like certain foreign exchange offices), others (most DNFBPs) tend to be formalistic documents that do not provide many details on the specific measures and procedures implemented by the entity, commensurate to their risk profile, beyond the general AML obligations already prescribed by the legislation.

515. Regarding VASPs, the effectiveness of their internal procedures could not be assessed as in-depth due to their recent categorisation as reporting entities. However, despite having formal AML/CFT procedures in place, the onsite meetings with sector representatives pointed out management of AML obligations on a case-by-case basis rather than a strict following of formalistic procedures due to the dynamic and rapidly changing nature of the sector.

#### ***Overall conclusions on IO.4***

516. 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 risk understanding by REs (both national and business-related) is sound, especially when considering the most material entities. FIs and DNFBPs are aware of their 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 in incrementing the frequency and intensity of regular CDD measures and, in the case of FIs, also include 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. The riskiest and most material sectors apply sound ML/TF preventive measures. Moderate improvements are needed in less material FI, some of the DNFBPs and VASPs. The latter have low materiality, explained by the reduced number of players and the restrictive approach adopted by the Polish authorities, which are taken into account in weighing them.

517. **Poland is rated as having a Substantial level of effectiveness for IO.4.**

## 6. SUPERVISION

### 6.1. Key Findings and Recommended Actions

#### ***Key Findings***

##### ***Immediate Outcome 3***

- a) The UKNF pays particular attention to the licensing of the new participants of the financial market for which it has responsibility and has the most robust entry checks for all obligated institutions, especially concerning legal and beneficial ownership. Nevertheless, there are gaps in the controls, particularly in relation to some senior management. There is also a need to complement the existing staff resources in the licensing department for banks.
- b) 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. In addition, while there has been success in dealing with unauthorised payment institutions, it is probable that there are still a few unauthorised operators.
- c) 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.
- d) Casino operators are subject to some licensing controls in relation to shareholders. There are also gaps in controls relating to beneficial owners and some senior management positions.
- e) There are basic controls in place for legal practitioners and notaries. However, there is a need to complement the existing staff resources at the MoJ to take a more proactive approach. There are no developed operational market entry controls in place that are able to prevent criminals from establishing, operating or benefitting from holdings in real estate brokers, DPMS and any TCSPs when undertaking activities covered by the FATF. There are also no market entry controls in place with regard to VASPs.
- f) Overall, 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. Nevertheless, a more discrete and forceful approach to the individual components of threat and controls would lead to more sophisticated

understanding and approaches to supervision. Fundamental changes are not needed.

- g) The UKNF has the most comprehensive approach to supervision; its use of IT and data analytics are a key part of this. The UKNF's supervisory team would benefit from a relatively small number of additional staff to enable increased supervisory engagement. 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. Although there is scope for refinement, the NBP provides the best model in Poland for coordination for organisations with regional offices around the country engaged in AML/CFT.
- h) 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.
- i) 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. At a strategic level, the greater focus on notaries by the Appeal Courts is consistent with the risks presented by legal persons in relation to VAT fraud and laundering of the proceeds of this crime. Nevertheless, there are shortcomings in resources and coordination within the Appeal Court system, which militate against comprehensive risk-based supervision. GIFI has been able to undertake some supervision of DNFBPs on the basis of risk-based triggers.
- j) Until July 2018, GIFI was the only supervisory authority that could impose sanctions for AML/CFT breaches; since then, the UKNF and the NBP have also had powers of sanctions. GIFI has a long history of applying sanctions and, importantly, has made recommendations for prosecution. The UKNF has imposed a few penalties and has sought to develop a more robust approach since 2018. It is establishing an enforcement team within its AML/CFT supervisory department to further increase the robustness of the approach, including with regard to the application of sanctions to individuals (with one such sanction under investigation) and the promptness of enforcement. 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; this is not consistent with the risks represented by DNFBPs.
- k) All the supervisory authorities met by the assessment team have endeavoured to promote understanding by supervised entities of their obligations. GIFI, the UKNF and the NBP have been particularly active and have made strong efforts to promote understanding.
- l) Supervision and awareness-raising by supervisors have made a positive difference to the level of AML/CFT compliance by FIs and registered DNFBPs.

## ***Recommended Actions***

### ***Immediate Outcome 3***

The UKNF should:

- (a) reinforce controls in relation to preventing the possibility of criminal control of obligated institutions subject to its registration/licensing and supervision by:
  - i. ensuring the scope of checks covers all senior management of FIs and associates of criminals, and also appointing additional staff resources within the bank licensing department sufficient to achieve this in relation to banks;
  - ii. developing a more intensive approach to ensuring consistency across the departments dealing with licensing and market entry to prevent criminals from controlling FIs;
- (b) establish systems to more formally identify whether or not unauthorised MSBs are in operation (for potential investigation by LEAs) and to address the risks presented by domestic payment institutions not subject to market entry requirements;
- (c) refine the existing ORION risk rating methodology to include further detail on threats and controls;
- (d) appoint some additional staff resources to the supervisory department and develop the approach into comprehensive risk-based supervision;
- (e) the sanctions team (with additional staff resources) should ensure that the approach to enforcement is demonstrably proportionate and consistent with risks;

GIFI should be provided with substantial additional staff resources; with these additional resources, it should:

- (a) as the “lead” supervisory authority, coordinate the operational activities of the supervisory authorities, monitor their activities and ensure that, as a whole, the supervisory framework for all FIs and DNFBPs is comprehensive, risk-based and effective;
- (b) refine its risk rating methodology for FIs so that it is more detailed and refine the risk ratings of FIs, and extend the risk rating methodology or develop a new methodology and risk rate DNFBPs;
- (c) collect, check and analyse sufficient data on a period basis in order to ensure the risk rating methodologies for FIs and DNFBPs mentioned in sub-paragraph (b) above are effective;
- (d) develop its existing supervisory approach so that it is comprehensively risk-based;
- (e) develop its approach to the application of sanctions in light of increased staff resources and increased supervisory engagement.

The NBP should:

- (a) in relation to the prevention of criminal elements from controlling currency exchange offices, be provided with additional powers and develop its controls

pertaining to entrepreneurs, currency exchange office staff and beneficial owners;

- (b) be provided with increased statutory powers to prevent registration of currency exchange offices for persons with criminal record;
- (c) enhance its existing risk rating methodology and develop a risk-based approach to the intensity of supervision.

With regard to market entry for DNFBPs:

- (a) Real estate brokers, DPMS and any TCSPs should be subject to registration and supervisory requirements, including requirements to ensure criminals cannot beneficially own or control such DNFBPs. The controls in relation to preventing criminals from being appointed as notaries or lawyers or from controlling casinos, including coordination of controls, should be strengthened. Additional staff resources should be provided to the MoJ so as to maintain up to date lists of registered and practising notaries and to facilitate and ensure this combination of strengthened controls and coordination in relation to notaries and lawyers.
- (b) Additional resources should be appointed within the Appeal Court system (or appointed elsewhere, which can assist that system) to ensure comprehensive and risk-based supervision of notaries. In addition, formal reporting and measurement systems should be introduced so that the activities of the individual Courts can be easily understood and coordinated.
- (c) Within the context of overall coordination by GIFI, the KAS should develop a formally coordinated approach to risk assessment and supervision by its headquarters and regional offices so that there is greater understanding within the KAS of the activities of the offices and the extent to which they are risk-based.

518. The relevant IO considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26-28, 34, 35 and elements of R.1 and 40.

## 6.2. Immediate Outcome 3 (Supervision)

### *6.2.1. Licensing, registration and controls preventing criminals and associates from entering the market*

#### **UKNF**

519. Banks - The licensing team for banks has 31 staff, who also have other responsibilities. It is understaffed, albeit not significantly, and is recruiting further officers and looking to improve IT and other systems. The licensing of a bank is a two-step process, which can be regarded as the issue of a preliminary licence to the founders of a bank in order to establish the entity, followed by the issue of a follow-up licence which enables commencement of commercial activities. This second step allows assessment of a bank's operational readiness before it can accept customers. The business model for each bank is understood by the UKNF; the model does not affect the level or type of checks undertaken to prevent criminal control of banks.

520. The UKNF is content that its controls have not allowed criminals either to beneficially or legally own a bank or to be a controller of a bank at the executive level (even where it has relied on assessments of fitness and propriety of senior management carried out by the bank). It obtains information on ownership and control structures, and its checks on these and beneficial ownership include banks acquiring a licence and covers the management board of the acquiring bank. Any lack of clarity in the structure is investigated. Information sought on legal and beneficial owners includes the source of the funding for those funding the bank. As part of the checks, individuals in the ownership structure and on the management board of a parent or acquiring bank are required to provide the most recent tax return, CV and a certificate of absence of criminal conviction in Poland from the National Criminal Register (and also a certificate from other jurisdictions where the individual has been resident for more than five years). Sanctions lists, the internet and the European Banking Association's (EBA) database are checked, and input is sought from foreign supervisory authorities on entities in the ownership structure, subsidiaries, and the parent or acquiring bank. The UKNF gives the foreign authority one month to provide a response before proceeding with its decision. The vast majority of requests (estimated at more than 95%) to foreign authorities receive a response within a month. The number of requests made by the UKNF is dependent on the nature of the acquirer but can be numerous (one case leading to over 40 requests).

521. With reference to Polish sources of information, the licensing department checks its internal databases, liaises with other departments of the UKNF (one of which, the Compliance Department, obtains information from GIFI) and the ISA. The AT notes that a conviction is considered as "spent" after five years and removed from the central register of convictions after that time and that this would apply to any request for information to any person as to whether they had a conviction (i.e. a conviction of economic crime older than five years would not need to be declared). The UKNF has pointed out that the circumstances leading to a spent conviction might, nevertheless, still be relevant to it if it learns of those circumstances from another source. The UKNF requires each application to provide information on any penalties which have been applied and any ongoing proceedings and, where there is pertinent information, also asks relevant authorities (usually the court and the Public Prosecutor's Office) about the case.

522. Changes of legal or beneficial ownership must be advised to the UKNF before they take effect and can only take effect once the UKNF has given its consent.

523. The same approach for individuals on the management boards of parent and acquiring banks mentioned above also applies to the president (i.e. the chief executive officer) and the chief risk officer of the management board of the applicant or licensee in Poland prior to their appointment. Other members of the management board and members of the supervisory board are automatically assessed on the same basis but after, rather than before, appointment, with the UKNF relying on the bank's own assessment prior to appointment. All supervisory and management board members must inform the bank if they become subject to criminal proceedings, and the bank is in turn required to inform the UKNF. Management and supervisory board members must be dismissed by the bank on conviction. Key function holders (for which the UKNF uses the EBA definition) are not automatically assessed for fitness and propriety by the UKNF either before or after appointment; subject to the triggers referred to in the paragraph below, the UKNF relies on the bank's own assessment.

524. The UKNF's assessment of beneficial owners, legal owners, management and supervisory board members - as well as any assessment of key function holders - after the licensing of a bank is based on a set of weighted signals. The signals derive from various sources - off-site

supervision, onsite inspections, the SREP process, whistle-blowers, the fit and proper assessment carried out by supervised institutions and provided to the UKNF, information received from other authorities or media monitoring. Each signal is assigned a weight. Where the combined weight of signals reaches a certain threshold, an in-depth fit and proper assessment is triggered; this is similar to the initial assessment (although, depending on the case, it might be limited only to the factors which have led to the signals). A review of a few key function holders has been undertaken via this risk-based approach.

525. The UKNF intends to use its proposed increased staff resources for the licensing department to focus more on members of the management board beyond the president and chief risk officer, members of the supervisory board and key function holders. The UKNF has published prospective requirements for the fit and proper test for the management board and the supervisory board (although these requirements seem to gather existing regulations and practices in one place rather than establish new requirements) but has been unable to publish material, as has been planned for some time, on key function holders as a result of the pandemic.

526. The UKNF was of the view that consideration of tax returns and audited financial statements from legal persons is helpful in identifying associates of criminals. In the case of the persons funding a new licensee and acquirers of significant holdings, information in relation to bank accounts for the previous year is also required. The AT notes that the totality of checks carried out would usually uncover any apparent links with criminality.

527. **Payment institutions** – The licensing team for payment institutions comprises five staff (one of the positions is vacant). This seems to be sufficient. The UKNF also has specialised departments (i.e. cybersecurity and FinTech), which are routinely consulted when dealing with payment institution applications; the FinTech department includes an intelligence unit, which is consulted on a risk basis, i.e. when there is uncertainty or suspicion about the applicant, including in relation to links to third parties – this is relevant to whether persons might be associates of criminals. Larger domestic payment institutions are considered in the same way as a bank, with a few differences as follows. Financial statements and tax returns are not requested at the licensing stage, although they are required of potential new beneficial and legal owners after licensing. Input is sought from foreign supervisors in every case where the applicant has undertaken supervised activity in other jurisdictions - a response has always been received.

528. At the operational level, all members of the management board (not only the president and chief risk officer) are assessed by the UKNF prior to authorisation of the institution. After authorisation the same assessment is undertaken for new appointments to the board, albeit after the person has been appointed. Requests have been made to the UKNF for information on the probity of individuals by the Police and the Public Prosecutor's Office. One of these has been in relation to an authorised payment institution, with most of the others being in relation to unauthorised business and in a few cases relating to small payment institutions (such an institution does not need an authorisation provided it has registered with the UKNF). Grounds for refusal of authorisation do not appear to include criminality, although it might be possible to use the criterion on the inability of the applicant to ensure sound and prudent management of its activities.

529. Smaller payment institutions are registered without checks in light of the EU Payment Services Directive framework, their size (and consequential risk profile), the importance of ensuring competition and as they are permitted to provide only a limited range of services. A significant increase in the number of small players (now more than 100) began in 2020. It is an

offence for a person with a conviction to establish a small payment institution, and any conviction handed down after registration must be advised to the UKNF. Small payment institutions are subject to ongoing AML/CFT supervision, and the payment service department (which concerns both licensing and offsite supervision) provides overarching information on risks to the supervisory department.

530. Non-domestic payment institutions based in the EU can undertake activity in Poland on the basis of EU passporting provisions.

531. Although it does not actively search for unauthorised activity, since the beginning of 2017, the payment service department has promoted, and the department responsible for co-operation on criminal justice matters has made 25 referrals to the Public Prosecutor's Office on the basis of suspicion that institutions have been engaging in unauthorised business. These referrals originated from the UKNF's offsite analysis and signals from the market and customers. Feedback on the outcome of these referrals has not been provided. The UKNF has also issued 37 warnings in relation to unauthorised operators. The UKNF has considered there are a small number of operators providing unauthorised or unregistered business but to a low level, with small scale transactions and by persons who are not aware of the legal and regulatory framework. The UKNF has noted that it does not have the legal competence to detect crimes and that such detection is inconsistent with a supervisory body but, whether or not changes to the legal framework are needed, the AT considers that the UKNF should be proactive in identifying unauthorised business (for potential investigation and prosecution by other authorities).

532. **Insurance** – the department for licensing and non-AML/CFT supervision for insurers comprises 37 people; 13 staff are dedicated to licensing and related functions after licensing (e.g. dealing with changes of beneficial owner or new members of the management board). Licensing of brokers is the responsibility of a separate department of five people. While there is a need for an increased number of staff, more generally in relation to supervision of the insurance sector, the UKNF considers that the functions with regard to licensing and related functions have not been adversely affected.

533. The approach to dealing with applications for insurers is similar to that for banks with a few differences. Financial statements are required for the last three years and bank statements in relation to the last year for corporate entities; where the legal or beneficial owner is an individual (there has been one case in the period since 2017), the last three tax declarations are required. Where the legal or beneficial owner is a foreign entity, input is sought from the relevant supervisory authority – in every case, a decision has been made only after input has been received.

534. The approach to management boards in relation to insurers is similar to that for banks with assessment of the president and chief risk officer prior to appointment and other members of the board after appointment. Input is sought from foreign supervisory authorities; consent is not provided until input has been received. Other members of the management board, members of the supervisory board and key function holders (the heads of the compliance, actuarial, internal audit and risk management departments) are assessed after they have been appointed. Other members of senior management are not subject to assessment by the UKNF.

535. **Investment/securities** – the department for licensing and non-AML/CFT supervision for investment firms has over 40 people, of which eight are in the licensing team and ten on the financial supervision team (which provides support to the licensing team). This seems to be sufficient. The department for licensing and supervision (other than for AML/CFT) for UCITS

managers and alternative investment fund (AIF) managers has 62 people, of which 23 are in the licensing team. This also seems to be sufficient. The approach for investment firms and UCITS and AIF managers is similar to that for the banking sector.

536. With regard to investment firms and UCITS and AIF managers, members of the supervisory board must be notified to the UKNF at the application stage and immediately after appointment, together with supporting information on the impeccability of reputation, including certificates of non-criminality in relation to Poland and other jurisdictions. Consent from the UKNF is required prior to the appointment of the chief risk officer and chief investment officer of the management board (based on consideration of supporting information, including certificates of non-criminality in relation to Poland but not outside Poland). Consent is not required for other members of the management board or for other members of senior management, and the UKNF does not review whether or not they might have criminal records.

537. **Non-bank lenders** – non-bank lenders have been required to register with the UKNF since 2017. The registration process is automatic, and the framework of registration does not provide for controls to prevent criminals or their associates from entering the non-bank lending sector. The UKNF's website makes it clear that non-bank lenders are not licensed or supervised by the authority.

538. Each sector for which the UKNF has a licensing, market entry or registration role has a different department responsible for the role (also see the UKNF's role below in relation to credit unions). There would be merit in refining the high-level approach within the UKNF so that there is a deeper shared understanding in a single place as to the similarities and differences between the operationalisation of the roles (and use of the assessment methodology, which is proposed to be further developed) and to what extent this should lead to any refinement of approach by individual departments.

539. **NBP – Currency Exchange Offices** - The headquarters and other regional offices of the NBP include AML/CFT amongst the range of their duties. Each regional office is responsible for licensing of currency exchange operations within its geographical area and enters data into a central register available to all NBP offices; headquarters approve all entries (notwithstanding that registration has already taken place). 85% of currency exchange offices are sole traders, with 15% structured as commercial companies such as limited liability companies and joint-stock companies.

540. As a matter of law, entrepreneurs who own and run currency exchange offices (sole traders and shareholders of commercial companies, with the shareholders generally being the beneficial owners as well) and any person providing exchange services cannot have a criminal conviction. As part of their application, entrepreneurs must confirm that they (i.e. not any staff or the beneficial owners of the limited number of exchange offices where the beneficial owners of a commercial company might be different to the entrepreneur) have a valid certificate from the National Criminal Register confirming absence of criminal convictions in Poland or, if a different country is applicable, the relevant authority in that country. At this stage, reliance is placed by the NBP on the entrepreneur. The certificate must be renewed annually. During each onsite inspection, the NBP checks whether, in practice, all persons required not to have a criminal conviction have a valid certificate. Where the certificate is older than three months, the NBP checks the person with the National Criminal Register. Inspections have led to cases where convictions of entrepreneurs were discovered by a regional office. The registrations of those entrepreneurs were withdrawn, and they were forbidden from carrying out currency exchange

activities. There were four cases in 2017, five cases in 2018, one case in 2019, three cases in 2020, with no cases being identified in 2021 prior to the AT's visit to Poland. The NBP is content that only a very small minority of currency exchange offices carry on business despite their owners having received a conviction after registration and that any person operating with a criminal conviction will be found as a result of the frequency of inspections. There is no current legal basis to review the criminal records of beneficial owners during onsite inspections, but legal changes later in 2021 will alter this position. To date, no criminality by beneficial owners has been drawn to the attention of the process.

541. Copies of applications for registration and related material are provided by the regional office to the headquarters of the NBP, which considers the accuracy of the application after the business' registration. In practice, the currency exchange office is considered by the NBP as having dual registration with both headquarters and the regional office. However, registration of a currency exchange office is, in effect, automatic, and there are no legal grounds to prevent a currency exchange service provider from being registered or operating, or an individual from owning or operating within such a FI, except the legal requirement for such a person not to have a conviction and discovery of persons with convictions during onsite inspections (see above). There is no legal basis for consideration of individuals from the perspective of whether they might be associates of criminals.

542. The annual updates and checks during onsite inspection processes are positive; there is also scope to increase the level of checks by, for example, reviewing the media/internet and seeking input from third parties.

543. **NACSCU and UKNF – Credit Unions** – No new credit unions have been established since 2006; the possibility of an unlicensed credit union being established is remote and would be easily detected. While there are no legislative provisions on prevention of control through ownership or beneficial ownership, the shareholdings of all 23 credit unions are widely spread; usually, each member holds a single share and always has one vote. The Credit Union Act applies to all members of the supervisory and management boards and specifies that they must not have been convicted of an offence against property or documents. The NACSCU considers board members to be low risk, as the credit unions themselves are low risk, and presidents are normally recruited from within the credit union. All presidents are Polish citizens and well known in the sector and to the NACSCU even before they are appointed as president.

544. A suitability test is applied by the UKNF before a person takes on the post of president. A certificate from the central register of convictions evidencing absence of a criminal conviction is required, the CV is reviewed, and input is sought from GIFI and the NACSCU. A number of individuals proposed to be presidents were rejected at the early stages of supervision of the sector, albeit on the grounds of suitability/experience rather than for AML/CFT-related reasons. Nevertheless, this shows the commitment to ensuring high standards. Credit union management boards normally comprise three individuals; a suitability test is applied to boards on the same basis as for banks. There are no ongoing checks in relation to criminality after a credit union has been established, although legislation requires that members of management and supervisory boards must not have been convicted.

545. **Ministry of Finance – Casinos** -The Ministry of Finance is responsible for issuing concessions (analogous to licences) to casinos (with the KAS participating in the licencing process where applications are invited for a concession which becomes free but not otherwise). There are 11 officers in the licensing team at the MoF; this seems to be sufficient. Concessions are issued

for a period of six years; casinos must be owned by Polish limited liability companies or joint-stock companies or by companies with similar rules established in EU or EFTA countries. There are nine entities with a total of 50 concessions for operating casinos. Of these, one concession is an online casino owned by the State, while a very large majority of the others are owned by a major group, or the company is listed on a stock exchange.

546. Before issuing a concession, the Ministry of Finance seeks input from GIFI, the ISA, the CBA and the Police on shareholders holding 10% or more of the shares, and members of the supervisory and management boards, members of the audit committee and any representatives they appoint. Board members must provide certificates from the National Criminal Register and, where relevant, an EU Member State (which leaves a potentially small gap in relation to other jurisdictions). Negative information has never been received. The information which helps to confirm the legality of the source of capital is also required from shareholders, namely the latest corporate financial statements and the most recent personal tax returns, although this information is not passed on for consideration outside the casino licensing and supervision team (e.g. to the tax department of the KAS). These checks would be of some value in ascertaining whether individuals are associates of criminals. Beneficial owners are not yet checked (although legislative changes will make this possible later in 2021). Senior management outside the supervisory and management boards, the audit committee and their representatives are not assessed (although some applications include lists of employees, there have been examination requirements since 2017 for compliance officers, and whistleblowing in relation to criminality is possible).

547. The Ministry must be notified within seven days of a change of shareholder. New shareholders are subject to the same process as that described above. Every two years, the Ministry requests GIFI, the ISA, the CBA and the Police whether they have any negative information about the company, shareholders and members of the management board; no negative information has been received.

548. **MoJ – Notaries** – A head of department and four other members of staff work in the MoJ's department for notaries; the department has had significant staff turnover and is under-resourced as a result of this and an absence of at least one subject matter specialist. Additional capacity would also enable additional proactivity. There are 250 to 300 applications to be notaries each year.

549. There are two access routes to the notarial profession. One consists of taking the notarial examination after completing notarial training or taking the notarial examination without training but after completing a professional internship. The second mostly relates to "transfer" from other legal professions such as judges, prosecutors, advocates and legal advisers who have practised the profession for at least three years.

550. Persons who wish to be notaries submit an application to the MoJ; the Minister appoints notaries by administrative decision. The applicant must provide an opinion from an employer, supervisor or patron about their employment and may provide other supporting information if they wish to demonstrate their impeccability of character or ability to be a notary. Before a decision is issued, the Minister must consult the council of the relevant regional chamber of notaries, with an absence of response within the specified time frame constituting a positive opinion from the chamber. The Ministry provides a copy of the application package to the chamber.

551. The Ministry does not maintain a list of notaries who have been appointed or who are currently practising, but the AT was advised that, following complaints made to it, the Ministry contacts the council of the relevant chamber of notaries and requests information or clarification as to whether there has been any irregularity in the activity of a notary; the Ministry has indicated that there are several such cases each month. Most of the complaints are not about potential criminality, but there is, nevertheless, a process for dealing with queries. Following the appointment of a notary, express checks in relation to criminality are not made by the regional chamber after registration of a notary. However, the regional chamber provides the Minister with copies of its onsite inspection reports for notarial offices for consideration – this has led to the MoJ ordering further inspections or initiating proceedings.

552. This contact between the chambers and the MoJ is relevant to the fitness of notaries. The AT notes that there is scope to establish routine dialogue between the MoJ and regional chambers, which would add to the existing liaison. There is no communication between the MoJ and GIFI or between the notarial chambers and GIFI to ascertain if GIFI has relevant information on the fitness of notaries. There are, however, cases of law enforcement agencies notifying the Minister that criminal proceedings have been initiated against notaries. In the event that criminal proceedings are instituted and completed against notaries, the Public Prosecutor's Office is obliged to notify the board of the appropriate chamber of notaries (statistics are not maintained on the number of notifications by LEAs or on completed proceedings). The Minister or the council of a chamber of notaries may also submit a request to the disciplinary court of the relevant chamber to initiate disciplinary proceedings. The Minister made 18 requests between the beginning of 2018 and the end of March 2021. These requests arose from complaints about violation of proper processes such as the drafting of a notarial act or the obligation to read out notarial acts in their entirety, the result of analysis of protocols of inspections or vetting of notary offices. Thirteen proceedings were concluded with a sanction; in five cases, the notaries were reprimanded, while eight cases were discontinued. Three proceedings are still pending.

553. **MoJ and SRBs - Attorneys and Legal Advisers** – A head of department and eight other members of staff work in the MoJ's department for lawyers; the same resource issues apply as those described above in relation to the Ministry's role for notaries.

554. Applications for registration for advocates/legal advisers are made to the relevant regional council of advocates or legal advisers as appropriate. By way of context, there were 3,348 applications for registration for advocates and legal advisers in 2020 alone. Decisions on registration as an advocate are made by the district bar councils and, for legal advisers, councils of the regional chambers of legal advisers, after examination as to whether the candidate fulfils the prerequisites for entry (which include impeccable character). They require to be provided with a certificate from the National Criminal Register evidencing that the applicant has not been convicted in Poland, together with information supporting the impeccability of character of the candidate. Similar evidence of non-criminality is required, when relevant, in relation to foreign jurisdictions. Should a positive decision be made, the regional council sends the Minister of Justice a copy of the resolution on entry of the individual on the list of advocates/legal advisers, together with the candidate's application. The Minister has the right to object to the entry within 30 days of receiving the information. An absence of objection is de facto consent to the registration.

555. The MoJ emphasised to the AT the importance it attaches to seeing evidence of lack of criminality by means of certificates of non-criminality in both Poland and elsewhere. Queries by the Ministry on applications have been made to the Ministry of Higher Education on the equivalence of foreign legal qualifications with Polish qualifications, but no checks are

undertaken by the Ministry to verify absence of criminality or association with a criminal. Negative responses by the Ministry on an application for registration have been based on lack of equivalence of foreign educational qualifications with the Polish requirements for lawyers.

556. Ongoing checks are not undertaken by the MoJ or the regional councils following registration. The MoJ advised the AT that it is advised by local prosecutors when proceedings are being undertaken against advocates and legal advisers and that, upon a conviction, the processes for proceedings operated by regional councils are commenced to consider the case in question and can end with expulsion/suspension of professional registration. Since 2016, the Higher Disciplinary Court of Advocates has expelled 44 advocates and suspended 338 advocates for varying periods. Sixteen legal advisers have been expelled, while 71 have been suspended for varying periods.

557. The MoJ has been able to obtain the statistics mentioned above specifically for the purposes of the evaluation; there would be merit in formalising ongoing liaison between the regional councils and the MoJ in connection with the ongoing fitness of registered advocates and legal advisers. As GIFI's input is not sought, there would also be merit in establishing a formal mechanism so that it can contribute both at the time of the application and after registration.

558. **Other FIs, other DNFBPs and VASPs** – Other types of FI (such as factoring businesses), DNFBPs not referred to above and VASPs are 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). This means that such FIs (not mentioned above) are not subject to market entry tests and express assessment to verify absence of criminal control; accountants are limited to an accountancy role and are not able to carry out activities captured by the FATF in that role, but there are no operational measures for registration or market entry for other DNFBPs listed by the FATF and there are no market entry controls to prevent criminals from controlling VASPs (although there is AML/CFT supervision by GIFI and this might help in preventing such criminality).

### *6.2.2. Supervisors' understanding and identification of ML/TF risks*

559. The issues raised in IO.1 and IO.4 mean that understanding of ML and TF risks by supervisory authorities cannot yet be comprehensive. In addition, not all DNFBP sectors are covered by a registration requirement, and DNFBPs subject to supervision are not formally risk rated.

560. **UKNF** - Understanding of ML risk is generally good. Each supervised FI has been risk rated under the UKNF's ORION methodology since 2015. The end product is a numerical score rather than a specific rating. Sixteen criteria are considered, with each criterion being allocated to one of three scored weightings. The systemic significance of a FI is key. The banking sector is the highest risk, with universal banks receiving the highest score; banks that are less systemically important and have a lower risk customer base have a much lower score. TF is considered from the perspective of internal AML/CFT policies, and there is a component that includes screening and freezing of assets. The UKNF comprehensively understands its methodology and intends to it in order to take account of the 2018 changes to the AML/CFT Law and to enhance the methodology's sophistication and coverage. As part of this objective, the scope of data collected from banks and investment sector firms (but not payment institutions) will be widened. Overall, the approach currently taken is thoughtful; nevertheless, the AT has a concern that too great a focus might be given to the systemic nature of banks and, in addition, the factors articulated in

ORION, which form the basis of the risk scoring, could usefully be extended (i.e. made more detailed) to more forcefully cover TF and demonstrably allow more detailed interrogation and assessment of the various components of risk such as customer risk (including beneficial owners) and geographic risk, the whole of country approach in the NRA, and vulnerability (such as internal controls). Data collection from payment institutions could also usefully be increased.

561. The risk scoring for each entity is reconsidered on an annual basis at the time of the preparation of the following calendar year's onsite programme. It is also reconsidered after an onsite inspection and as a result of trigger events, such as a media report, information from another authority or customer complaints, which could lead to a change of data in ORION. There were 134 changes of risk scoring from 2018 to 2020 (a significant proportion being in relation to banks), and in a significant number of cases, this led to inclusion of the FI in the onsite inspection programme. The AT regards this recalibration of risk as positive and showing enhanced understanding of the risk profile of individual institutions in light of developments.

562. The UKNF receives information from quite a comprehensive range of sources, including both offsite and onsite supervisory engagement. This information (see below and IO.5) informs completion and use of ORION for risk assessment (with one of the benefits of extending ORION as mentioned above being to further articulate the quantum of information used in risk assessment and how it is used).

563. Banks are required to complete questionnaires for the UKNF each quarter covering the number of customers, their risk ratings, the number of PEPs and the number of SARs. Separately, banks are requested to provide information on relationships with payment institutions.

564. The UKNF obtains information from the NCR and the CRBO. Also, prior to an onsite or offsite inspection, the NCH is requested to provide information on bank accounts, including the number of relationships with Polish companies and on the beneficial owners of such companies; the NCH provides the information (and its analysis) to the UKNF upon request. The NCH also provides information on individuals who are BOs if they are connected to more than one customer of a bank and when they are a BO of customer accounts in more than one bank. This enables the UKNF to extend its consideration of customer accounts at one bank during an inspection to customer accounts at other banks. In addition to requests made pre-inspection, information is sought from the NCH several times each month. Information from the NCH (and the CRBO) is also checked against information provided by the bank under inspection for each legal person which the bank has as a customer. Checks are also made against NCR data on a sample basis. The UKNF looks for connections between companies and considers the relationships between BOs and the jurisdictions to which they are linked, including jurisdictions assessed as high risk by the authority; as part of this process, the UKNF looks for high-risk companies. The checks include the frequency and accuracy of banks in updating the two registers and the NCH database.

565. The UKNF places great stock on business risk assessments by FIs and issued a model template by way of guidelines in 2015. These have improved over time, and in general, the quality has developed and matured, and the UKNF sees them as useful to institutions and the supervisor. They are considered during the onsite process; anonymised business assessments seen by the AT indicate they provide a good source of information to the UKNF on risks to individual FIs and sectors.

566. The UKNF also uses the information it obtains during onsite and offsite inspections. As part of this, it keeps quite detailed information on its findings, including breaches found, and has

analysed these. An improved approach to risk has meant that the number of potential customers rejected by banks has tripled since 2019, and this also informs the UKNF. In addition, meetings with FIs and substantial contact at outreach events inform the UKNF's understanding of risk.

567. For the purposes of the NRA, the UKNF required all FIs subject to its supervision to provide information on cross-border transfers, enabling it to develop a thematic analysis of flows. Linked with this, it has taken steps (see below) to understand the combination of risks within the relationships between banks and payment institutions.

568. Significant information is collected by the UKNF in relation to use of banks by fraudsters, including from liaisons with compliance teams to enhance joined-up approaches. A similar approach is taken concerning virtual assets and the development within Poland of virtual asset and foreign exchange platforms. FIs in Poland have introduced new distribution channels, which are mainly internet-based. In turn, this information on developing technologies and approaches to technologies informs the supervision of individual FIs.

569. The UKNF spoke well about its understanding of the main risks, the most important being the use of fictitious companies. Understanding of TF is less than understanding of ML.

570. **NBP** – The NBP has an understanding of the number and pattern of currency exchange offices across Poland. The main currency exchanged is the EUR, with the USD some way behind. Legal persons are a small part of the customer base. The highest risks are seen as the ability to undertake CDD only when the value of a transaction meets the designated threshold and the face-to-face cash nature of the transaction (i.e. cash transactions under the threshold are anonymous). Large transactions are also seen as a threat, although these are rare and dependant on the location of the currency exchange office. In practice, offices carry out analysis of their customers even where transactions have a value below the threshold and also where customers appear regularly, or irregularly but many times, and require CDD from them. The NBP notes that offices themselves have a concern about the implications of customers carrying out transactions routinely. TF is seen as difficult to understand in the context of the currency exchange sector but is treated as a threat notwithstanding this. The NBP's understanding of risk benefits from these approaches by offices.

571. The NBP comprehensively understands its risk rating methodology, and overall understanding of ML risks is generally good. It had a clear view of the components of a good business risk assessment; it issued guidance to currency exchange offices in 2018 on the composition of such assessments; and benefits from the outcomes generated by supervised entities. The NBP also issued its own assessment of the currency exchange sector in 2018.

572. Currency exchange offices have been risk rated since 2019. Each currency exchange office is rated as high (587 offices), medium (794 offices) or low risk (1 130 offices) under the methodology. The rating is considered annually and is informed by the results of onsite inspections. While the smaller number of high-risk entities compared with low-risk entities is consistent with a standard risk pattern, the relatively high number of high-risk currency exchange offices might suggest that the number can be reduced further in order to further develop risk-based supervision. A distinction is not made between ML risk and TF risk – ML/TF risk is considered as a whole. The NBP indicated that there is a link between its risk rating methodology and the NRA and noted that it had contributed to the NRA based on its understanding of risk. Overall, the approach is relatively simple but treated in a developed way through familiarity and use, with a series of factors that are weighted and which suggest elevated or diminished risk compared with medium risk. These include size, location, the concentration of offices, the combination of business activities within the office, the products offered, the results of previous

inspections, the number of transactions each day, quarterly turnover and the scale of purchase transactions. There is some degree of focus on factors which are to do with size/structure/impact. Customer and geographic risk are covered through the factor on location of the office (e.g. a location in a shopping mall suggests a particular client base while a location near a border might suggest geographic risk). There is scope to enhance the model to consider customer, geographical, transaction (including information on the number of transactions) and TF risks; the whole of the country picture in the NRA; and controls, more discretely and forcefully. The weighting attached to size/structure/impact could be considered at the same time. There is also scope to consider whether the number of high-risk entities should be reduced. Any changes would be an enhancement to an existing approach, which positively differentiates between offices. There would also be merit in considering whether a review of the criminal records register on occasions other than inspections, together with any other external input, might be an appropriate explicit factor. The AT notes that newly registered offices are considered to be high risk and treated as such, but there is no obvious reference to this in the methodology; this factor could therefore be added.

573. **GIFI** – GIFI assesses the ML/TF risk of each FI using a methodology (introduced in July 2018) based on nine weighted criteria. The ratings are revisited every six months; trigger events do not lead to reconsideration of ratings, although the AT notes that reconsideration is in any case relatively frequent. GIFI was authoritative when discussing the methodology with the AT (i.e. it has a comprehensive understanding of the methodology) and advised that it takes account of the NRA when rating FIs.

574. GIFI's risk rating methodology is different from that used by other supervisory authorities, and it completes its risk rating for each FI separately to, and without explicit input on the rating from, other supervisors. Each FI is therefore rated under two different and independent risk rating methodologies by two different supervisors. If this approach of using two different perspectives is to be continued, there would be merit in bilateral discussions of the risk rating for each FI so that each supervisor understands the precise perspective of the other. In addition, there is scope to enhance the model to consider customer, geographical, beneficial ownership and TF risks, the whole of the country picture in the NRA, as well as controls, more discretely and forcefully. Any changes would be an enhancement of an existing approach that positively differentiates between the risks of FIs.

575. GIFI has concluded a risk rating for each DNFBP sector, although individual DNFBPs are not risk rated.

576. While the AT notes that inspections are largely undertaken to FIs, GIFI receives information from quite a comprehensive range of sources, including its offsite and onsite engagement (such as quarterly returns, offsite inspections (which have been held since 2019 and are similar to onsite inspections in practice and include customer file reviews but not interviews of representatives of the institution), meetings with obligated institutions, onsite inspections, and contact through training events) and input from other supervisory authorities. It closely monitors the number and type of breaches found during onsite inspections. It also leverages SARs, transaction reports and other intelligence it receives, such as whistle-blowers. In addition, as the secretary to the NRA process, it is very well placed to see the wider risk picture. It is well placed to leverage this information to understand risk.

577. On or before 15 November each year, GIFI provides each supervisory authority (and the regional office/court of an authority where the regional office/court has responsibility for

supervision) with a letter on areas and sectors particularly exposed to the ML/TF risk for consideration. GIFI advised that the letter is based on the NRA and judgments made by GIFI from information it has received and considered during the previous year. The documents inform the plans that each supervisory authority provides to GIFI and differ between supervisory authorities; they reflect factors relevant to the supervisor in question. In addition, the information is amended from year to year. There is scope to refine this guidance to more assertively address the main risks facing Poland. Although the AT notes that there is no explicit reporting mechanism by the supervisory authorities (and that the introduction of such a mechanism would be beneficial), GIFI is comfortable that supervisors follow the guidance because of the patterns evident in the annual onsite inspection plans provided by the supervisors. Separately, while the UKNF has its own risk rating model and has developed its own programme of inspections, it has advised GIFI that the risk areas it has identified are consistent with those GIFI has identified and that GIFI's guidance is followed.

578. **Appeal Courts** – Notaries are not subject to risk rating by the Appeal Courts. Judges met by the AT had not been involved with the NRA but advised that they found the NRA to be helpful in understanding risks. They agreed with the views expressed by notaries and the notarial business risk assessments they had seen that the risk profile of the profession is low. CDD is undertaken, beneficial owners are identified, and further questions are asked after identification; anonymous transactions are not permitted. The responsibility of notaries to report suspicion was noted by the judges, together with the checks necessary to meet that responsibility. By way of reinforcing this point, it was also noted that only one SAR had been filed by the notary sector with GIFI (see IO.4 for the AT's concern as to this level of reporting). Digitisation assists notaries to search for higher threat companies, and further digitisation of notarial processes was advised to the AT as a distinct benefit in allowing enhanced understanding of risk. Absence of company information in the CRBO or outdated information is seen as a red flag by notaries, and co-operation by the sector with the authorities is seen as improving identification of fictitious companies. The requirement since 2018 to register extracts from notarial deeds was also seen as a benefit by the judges. The seriousness with which notaries carry out their role is noted during interviews by the judges onsite. Fraud was seen as a possibility, although cases were described as being exceptional. The regional Appeal Courts have not risk rated notaries and are not aware of GIFI's ratings.

579. The AT is concerned that there is a disconnect between the perceived risk profile of notaries and the gatekeeper role of notaries in relation to legal persons and the continuing abuse of companies for VAT frauds. Notaries are required for real estate transactions; such transactions are not seen as presenting a particular risk. Notaries were not considered to be susceptible to TF risk.

580. **KAS** – The KAS has indicated that the regional offices have risk analysis units that risk rate casinos based on a model template used throughout the organisation (albeit minor modifications might be made by regional offices in practice), and the outputs are used to prepare the onsite inspection plans; while, based on experience, considering the risk assessments as using advanced approaches, the head-quarters of the KAS does not possess information on any specific modifications or detailed outputs of the assessments, including the individual risk ratings for casino operations. The risk analysis and rating cover a range of risks; ML risk is one of the components. The KAS pointed to the small number of casino operators and frequent inspections of casinos as risk mitigants. The casino sector was seen as distant from the risk issue of tax fraud, and the KAS was not aware of any case of a casino or casino operator being involved with ML or

TF. More specifically, casinos are considered by the KAS to be low risk for ML or TF in light of the comfort it takes from its overall programme of supervision, registration of clients, audio-visual recording of games, maintenance of records for five years and the lack of anonymity for winners – who must be registered as winners. However, GIFI considers casinos to be high risk and has devoted focus to them. The KAS has pointed out that each authority is considering risk from its own perspective. Nevertheless, the difference in the conclusions of the two supervisory authorities suggests there is scope for greater risk assessment, coordination and joined-up understanding of risks.

### **6.2.3. Risk-based supervision of compliance with AML/CFT requirements**

581. UKNF – In addition to the Director, the AML Compliance Department has 13 officers engaged in supervision, three analysts, and two officers engaged in co-operation with other parts of the UKNF and third parties. The AT considers that there would be merit in adding a small number of additional officers to the team. Staff are experienced, and the team includes substantial private sector experience. They were authoritative in the discussions with the AT. Training is wide in scope and undertaken in relation to both AML and CFT (with CFT modules), although the focus is on ML.

582. In addition to receiving offsite questionnaires from FIs, offsite inspections have been undertaken as a result of the first lockdown of the pandemic. These inspections go beyond desk-based analysis and include interviews. Depending on the findings, an offsite inspection can lead to further engagement, such as an onsite inspection. These inspections involved meeting virtually with FIs and focussing discussion on the customer base, CDD and transactions, together with checks on compliance with other obligations and discussion with the FI on seeming anomalies. These inspections led either to the completion of the inspection or a decision to undertake an onsite inspection when conditions permitted. Since April 2020, the UKNF has conducted only offsite inspections. Depending on its conclusions on risk, offsite inspections were full scope or thematic in nature and were guided by a methodology.

583. As with other supervisory authorities, the UKNF provides its schedule of onsite inspections for the next calendar year to GIFI at the end of the previous year. This is informed by consideration of ORION and articulates the sector for each FI to be visited, the types of inspection (e.g. comprehensive or targeted, such as a focus on internal control systems) and the reason for the inspection. Ad hoc inspections are also carried out.

584. Prior to an onsite inspection, the UKNF requests a list of information to be provided. There is also a methodology to help guide the inspection. The AT considers there is scope to add some detail to guide separate consideration of TF as well as ML, and sectoral and national risks as well as the FI’s own risks. The UKNF has advised that it considers coverage of TF to be adequate.

585. The pattern of offsite and onsite inspections by the UKNF for each year since 2017 and the first four months of 2021 is as follows:

**Table 6.1 Onsite and offsite inspections conducted by the UKNF (2017- April 2021)**

	<b>2017 (onsite)</b>	<b>2018 (onsite)</b>	<b>2019 (onsite)</b>	<b>2020 (mostly offsite)</b>	<b>April 2021 (offsite)</b>

<b>Banks</b>	32	15	16	16	6
<b>Securities</b>	3	6	1	1	2
<b>Branches of credit institutions</b>	4	0	4	0	2
<b>Investment funds</b>	3	0	1	3	0
<b>Insurance</b>	2	0	2	2	0
<b>Credit unions</b>	5	0	3	1	0
<b>Payment institutions</b>	1	16	9	1	2

586. The difference in the number of inspections over the period in the table and the pattern of inspections suggests that overall, the volume of inspections should be increased.

587. In 2018 and 2019, the large majority of onsite inspections were conducted on banks and payment institutions. This is in line with overall sectoral risks. All banks considered by the UKNF to be high risk have been subject to inspection since 2017 (also see IO.5). Payment institutions became more prominent in the inspection programme as a result of the EU issuing information in 2017 on the risk profile of the payment sector, the transformation of the sector in Poland in terms of the size and product range, and awareness of the importance of responding to developments and address virtual currencies as an emerging international and domestic risk. In addition, the UKNF is conscious of the importance of its inspection programmes in understanding the combination of risks as a result of the relationships between banks and payment institutions. This illustrates the importance the UKNF attaches to monitoring developments across FIs, the interplay of relationships and mitigating emerging risks. It wishes to address any potential shift from traditional asset classes into virtual currencies and non-fungible tokens as soon as possible. During 2020 and 2021, the focus has been on inspecting banks.

588. The main focus for a full-scope inspection is the overall understanding of risk by the FI, ongoing and transaction monitoring and CDD, including measures taken in relation to updating information on customers and the identification and verification of beneficial owners. There is also a focus on controls for higher risk customers and the coherence of transactions for such customers. This includes a review of red flags and how they are addressed in practice; this includes a review of a sample of 50 to 100 alerts and how these are dealt with, including the substantiation for closing an alert; the process for generating internal reports of potential suspicion and the way these are handled, including the substantiation for not filing a SAR with GIFI. Beneficial ownership is considered, to some extent, from a top-down perspective rather than focussing only and specifically on fictitious companies and VAT fraud from a bottom-up perspective. Nevertheless, the UKNF does consider this risk to a substantial degree in its inspections, as indicated here and in IO.5. Currently, 50% of each full-scope inspection on average has been devoted to beneficial ownership. Overall, inspections also cover the criteria included in ORION and the elements added to the AML/CFT Law in 2018, such as the inclusion of the new requirements for training. Considerable attention is paid to the IT architecture of FIs, and the UKNF is provided with direct access to the IT system in order to assess the currency and

calibration of the system, including the date and implications of any upgrades. The use of IT and data analytics is of particular merit. Between 20 and 100 customer files (the number depending on the size of the FI as opposed to ML/FT risk per se) are checked. Adequacy of identification and verification of beneficial ownership is considered as part of the sample. The AT considers that there is scope to pay more focussed attention to the specific risks of Poland during inspections.

589. In light of a report issued by the European Commission in 2017 on EU risks, 18 onsite inspections in 2018 to banks and investment institutions were thematic, focussing on treatment of beneficial ownership and safety deposit boxes. There is a specific methodology for these inspections (there is scope to add some further detail). At least 100 customer files were sampled at each inspection to assess the adequacy of standards in relation to verifying beneficial ownership and CDD. In addition, the 16 inspections in 2018 to payment institutions were thematic and included consideration of how these institutions fulfilled training obligations towards their agents.

590. Ad hoc inspections in relation to CDD have been undertaken.

591. A minimum of three staff participates in onsite inspections. The size of the team is extended depending on the size and risk of the FI and, on some occasions, officers from the cybercrime or other departments also participate. Inspections usually last five days but can take longer.

592. **NBP** – The headquarters of the NBP is responsible for coordination of supervision. This has included the development of inspection methodologies and procedures (including a template to guide inspections) and guidelines on co-operation, organised training twice a year for all inspectors; held meetings with regional offices on the contents of the risk assessment approach for individual currency exchange operations; risk rated each currency exchange office; considered inspection reports prepared by the inspectors after inspections as a means of quality control; and, since 2018, imposed sanctions for breaches detected by any regional office. The headquarters sees its focus on providing routine training for staff across Poland (at least annually) as a particular strength; staff cannot undertake inspections without attending training at least every two years, and training attendance must be reported to HR departments. Coverage of the training is considered by the NBP to be comprehensive – its approach is that staff must have the knowledge to effectively conduct the inspection. It has included risks, including risks presented by entrepreneurs (although TF is not included). This is additional to any other training which might be offered (e.g. by GIFI) or undertaken at the regional level. In addition, the headquarters provides operational support. Where an entrepreneur has operations in Warsaw and in other cities, there is coordination by the headquarters so that onsite inspections are synchronised across the NBP network.

593. The headquarters of the NBP has ten staff and is sufficiently well resourced. It is a matter for the 16 regional offices to decide whether they have adequate resources, but, at the time of visit by the AT to Poland, the headquarters was comfortable that the regional offices are sufficiently resourced. In general, staff levels at each regional office reflect the differing number of exchange offices subject to supervision, and there is a formal support programme in place in which officers in one regional office support any shortfall in another region. There are some 120 full-time and part-time staff altogether. The regional offices report to the President of the NBP and, if those offices advise that they need additional resources, the headquarters is supportive and report as such to the President.

594. The NBP has recommended currency exchange offices undertake CDD for transactions with a value lower than the designated threshold so as to mitigate the risk of anonymous transactions. The NBP also focuses attention on training of currency exchange offices, in particular the training of entrepreneurs.

595. The timing of an inspection is coordinated by the headquarters when an inspection is to be carried out by more than two regional offices. Offsite information in the form of purchases and sales for each currency and the cash balance at the end of each quarter is received on a quarterly basis; the form also allows the turnover of each office to be determined. This informs risk rating of currency exchange offices.

596. The NBP has developed time frames for onsite inspection, with high-risk exchange offices subject to inspection every two to three years, medium risk offices every four to five years and low risk offices every six to seven years. This is a slightly longer time frame for each risk category than was the case previously – the NBP advised that this change in frequency results from a risk analysis completed each year. There have been exceptions in meeting these time frames, at one period to a staff shortage, or when currency exchange offices have been suspended. New currency exchange offices are rated as high-risk and are inspected within a year of registration. As with other supervisory authorities, the annual plan is provided to GIFI at the end of the year. The plan is not rigid – it is adjusted in relation to ad hoc inspections. The AT expects the natural consequence of the reduction in number of high-risk currency exchange offices indicated in paragraph 572 to be an enhanced frequency of onsite inspection to such offices.

597. The table below shows the pattern of the NBP's onsite inspections for each year since 2017 and the first four months of 2021, divided into risk categories. Ad hoc inspections are undertaken and have been carried out in response to requests by GIFI and LEAs. Information from dissatisfied customers leads to inclusion of the currency exchange office in the following year's inspection programme.

**Table 6.2 Onsite inspections conducted by the NBP divided into risk categories (2017-April 2021)**

	High risk	Medium risk	Low risk	Total	Number which are ad hoc inspections
2017	no risk assessment			652	8
2018	no risk assessment			411	6
2019	239	243	285	767	5
2020	103	120	115	338	6
01.01-30.04.2021	46	31	27	104	2

598. The number of inspections undertaken is substantial; a minimum of two staff undertakes each inspection, but the number can be higher. Inspections have taken between 2 and 26 days depending on the size and number of outlets of the currency exchange office as well as the geographical spread of the office and its outlets. All inspections are full scope inspections with the same approach undertaken for each regardless of risk and are conducted based on a template. There is, therefore, scope for intensity of supervision to be altered so as to be risk-based.

599. Compliance with all AML/CFT obligations for all customer transactions during the previous year is checked during an inspection. The inspection includes whether the entrepreneur understands risks and whether all relevant transactions have been reported to GIFI. AML/CFT controls and procedures are reviewed to consider if they are consistent with the nature and size of the business. Inspections also check the level of training undertaken and whether or not entrepreneurs and customer-facing staff have attended the e-training provided by GIFI. It is positive that NBP officers are using a guide to focus the inspection; there is scope to enhance the guide and, therefore, the approach in practice so that inspections are more detailed in relation to risks.

600. **GIFI** – GIFI is responsible for supervising approximately 329 000 obliged institutions (out of which around 12 000 entities belong to the financial sector, and around 317 000 entities belong to the non-financial sector). These numbers do not include business entities that become obligated institutions by accepting the amount of €10 000 in cash. However, the GIFI did not provide an exact number but the most accurate estimation possible. The AML/CFT supervisory team had seven staff in 2017; while this figure had increased to 12 at the time of the AT’s visit to Poland, there is a need for additional, substantial staff resources. The current staffing level means that GIFI, as the “lead supervisory authority”, can coordinate the preventive framework to a partial rather than a comprehensive extent.

601. As it receives the inspection plans of other supervisors, GIFI is able to provide input to those supervisors in relation to the institutions which are the subject of the plans. It also receives onsite inspection reports, including for ad hoc inspections and SARs, which it factors into its input. For example, in 2019, it suggested to the UKNF that it should check the SAR reporting system of a bank which the GIFI considered had issues in that area. A convincing number and type of other examples were also provided to the AT to demonstrate the proactivity and benefit of this input.

602. GIFI’s inspection programme for each calendar year (finalised at latest by the end of January) is informed by the level of its resources, the information it possesses and its conclusions on the annual inspection plans of the other supervisory authorities which it receives by 30 December prior to the year which is the subject of the plan. GIFI does not hold joint inspections and, where a sector has another supervisor, will select institutions for inspection not selected by that other supervisor – for example, GIFI undertook two inspections of banks in 2019 in addition to the banks inspected by the UKNF; the two banks were the next most risky under GIFI’s methodology after the banks selected by the UKNF. Ad hoc inspections, as well as planned inspections, are carried out. Planned inspections are full scope, while ad hoc inspections are targeted. Ad hoc inspections arise in response to an issue and usually focus on CDD measures, beneficial ownership and reporting of suspicion.

603. The number of inspections has been significantly affected due to the low level of staff resources. The table below provides information on the number of onsite inspections for each year since 2017 and the first four months of 2021. The risk ratings are individual ratings for FIs and sectoral for other entities, including VASPs. The shortfall in staff resources means that further staff are needed to increase the scale of the onsite (and offsite) inspection programme in line with Poland’s risks. The table below contains the number of onsite inspections undertaken by GIFI and also shows the split between FIs and DNFBPs by the FATF on the one hand and other entities on the other to show the split of the GIFI’s supervisory engagement:

**Table 6.3 Onsite inspections conducted by the GIFI divided into risk categories (2018-2020)**

Obligated institution	Number of on-site controls	Risk rating	Full scope	Thematic control	Planned control	Ad-hoc control
<b>2018</b>						
Banks	3	low -2; medium -1	1	2	2	1
Payment institutions	1	high	1	0	0	1
Investment fund companies	1	low	1	0	1	0
Entrepreneurs operating in the field of trading in metals or precious and semi-precious stones	1	medium	1	0	0	1
Notaries	2	medium	2	0	2	0
<b>2019</b>						
Banks	2	high	2	0	1	1
Payment institutions	2	high	1	1	0	2
Investment fund companies	1	medium	1	0	1	0
VASP	1	high	1	0	1	0
Notaries	3	medium	3	0	3	0
Attorneys	2	medium	2	0	2	0
Legal advisers	2	medium	2	0	2	0
Tax advisers	2	medium	2	0	2	0
Intermediaries in real estate trading	5	low	5	0	5	0
<b>2020</b>						
Banks	3	high - 2; medium - 1	2	1	2	1
Investment fund companies	1	medium	1	0	1	0
Betting operators	1	high	1	0	0	1
Notaries	2	medium	2	0	2	0

604. GIFI uses a procedure to guide each inspection. The document for full-scope inspections covers PEPs; the appointment of compliance officers; business risk identification and assessment; customer risk identification and assessment; the application of CDD measures (including EDD); procedures; training; internal reporting of breaches; provision of information on wire transfers; TF TFS; transaction analysis for higher risk customers; maintenance of transaction records; suspension of transactions and blocked accounts; and control of obligated institutions. The

procedure reflects requirements of the AML/CFT Act and, for each requirement, simple guidance on how to verify fulfilment of the obligation.

605. Customer files are reviewed. The inspection leader selects several files based on the risks of the institution and includes PEPs, legal persons for which a PEP is included in the beneficial ownership and customers with high geographical risk.

606. The scope of individual inspections increased in 2019 after the revision of the AML/CFT Act. In discussion, GIFI was convincing about its approach and advised that, during inspections, the inspection team considers in what areas to strengthen its control activities, for example, by increasing the number of files sampled to check compliance with a particular requirement in more detail. Documents seen by the AT imply (but do not wholly demonstrate) good quality inspections, which are stronger than suggested by the control document in relation to ML (but with TF not addressed separately within the overall approach to AML/CFT except for basic TFS checks). The AT has been advised that the scope of inspections varies depending on the type of obligated institution and particularly considers whether the institution has a business relationship with the customer; where such relationships exist, the scope of CDD measures is different, and this guides the sample of files sampled. GIFI has also advised that, where there is enhanced risk, it deepens its approach. Nevertheless, while GIFI has indicated that the procedure allows flexibility for the inspection to be adjusted to the situation in particular institutions, there is scope for a more comprehensive risk-based approach, which would include a more detailed procedure for each of ML and TF, intensity of supervision and a demonstrable treatment of national and sectoral risks (e.g. fictitious companies).

607. VASPs have been included in GIFI's programme. In 2019 it conducted a full-scope inspection of one of the largest VASPs (a crypto-currency exchange), while another inspection was carried out by the KAS. In 2020 GIFI arranged for the KAS to inspect an exchange. In addition, GIFI's inspections to banks consider how those FIs approach customers in the cryptocurrency sector. Its inspection plan for 2021 includes four further inspections to institutions in the sector. GIFI has recognised the risks of VASPs, and its programme will benefit from the additional staff resource recommended by the AT.

608. **Appeal Courts** – Under the AML/CFT Law, the President of each Appeal Court has the lead AML/CFT responsibility for each Court. In practice, as neither the Presidents nor the Appeal Courts have been provided with staff to undertake day-to-day supervision, AML/CFT supervisory engagement is delegated to a judge or several judges of the Court – or temporary visiting judges. This is creative and positive, but, nevertheless, judges of the Court have existing responsibilities and, with regard to visiting judges, AML/CFT duties are in addition to their judicial duties and duties related to internal administrative supervision. The President decides to what extent to “sign off” engagement, and the AT understands that, in at least some cases, there is no systematic reporting of supervisory activity to the President. The combination of resource issues and use of individuals for whom AML/CFT is one of many responsibilities in at least the majority of the system means that the scope of supervision and the effectiveness of supervision across Poland cannot be comprehensive or easily measured.

609. The judges met had participated in the three briefing events held by GIFI in May 2019 and January and December 2020. Training is not compulsory and not systematic or coordinated (and no central record of training is maintained). Overall, other than provision of onsite inspection plans to GIFI and addressing requests by GIFI to undertake inspections of specific notaries, each Appeal Court acts independently.

610. As with the other supervisors, an onsite inspection plan is provided by the President of each Appeal Court to GIFI at the end of each year (based on guidance issued by GIFI). In addition, for one of the regions for which the AT met a visiting judge, there is a procedure which indicates that, in developing the plan, account must be taken of the dates and findings of previous inspections and information from the Council of the regional chamber of notaries. Furthermore, the judge advised the selection process was risk-based to the extent of selecting notaries who are not based in small towns; in this case, the visiting judge makes the decisions as to which notaries to select for inspection and when. A judge from a different region advised that all notaries in that region are inspected every four years based on the gap between inspections and statistics on the number of transactions and that a number of ad hoc inspections had been undertaken. However, the number of inspections has been continually decreasing, as follows: 2017 (171), 2018 (135), 2019 (126), 2020 (110).

611. There are two types of inspections, planned inspections and ad hoc inspections requested by GIFI, the latter being full scope or targeted. GIFI provides the reason(s) for the request. The most recent request for one judge met by the AT was to review transactions as there had been delays in notifications by the notary to GIFI.

612. The resource issues have had a negative impact on the number of inspections. Inspections include interviews and checks of a random sample of files and notarial deeds. Shortcomings detected have been minor such as an absence of the certificate required where training has been undertaken. One judge checked medium-risk transactions during his inspections. Inspections include TF at least to some extent (e.g. whether it is covered by the business risk assessment and whether training has been undertaken). Business risk assessments by notaries are developed with the help of the regional chamber of notaries. During inspections, cases have been found of transactions that had not been reported to GIFI and were subsequently advised to GIFI by the judge (penalties had not been imposed as the failure to provide reports had arisen due to technical issues). The judges met by the AT were convincing about the seriousness of their approach. Anonymised reports of visit findings seen by the AT are systematic and serious and broadly cover the scope of obligations. Nevertheless, in the absence of external input and coordination, there is scope for inspections (and their intensity) to be more demonstrably detailed and demonstrably in line with Poland's risks. Offsite supervision is not undertaken. Outside of the Appeal Court system, an inspector of the relevant regional council of notaries conducts an inspection within one year of registration of the notary and every four years thereafter. The AT has been advised that these inspections cover AML/CFT and that there is close communication between the notarial chamber and the Appeal Court.

613. The Polish authorities have noted that notaries are not guardians for the correctness of companies' operations and that whether the company is created for fictitious purposes is beyond the control of the notary. They also note that: the notary has the possibility and legal obligation to control a specific transaction for signals that may indicate ML or TF; the procedure, risk assessment and awareness (gained through mandatory training) of the notary to check whether a transaction might be related to ML/TF; and the control of notarial duties by the Presidents of the Appeal Courts, together serve to correctly guard against suspicious transactions. Nevertheless, the AT retains a concern about the overall robustness of AML/CFT supervisory engagement (and that this is within the context of an ongoing issue with regard to fictitious companies), and the quantum of other risks in relation to legal persons is not known.

614. **KAS** – The KAS has 72 staff engaged in casino supervision and considers it has sufficient and sufficiently well-trained staff to undertake AML/CFT supervision. Staff combine AML/CFT

with other responsibilities and are located in the headquarters (six staff) and 16 regional offices. Forty-six staff have been trained in AML/CFT by means of presentations, conferences and workshops, while some of these and other staff have participated and are participating in an e-training course provided by GIFI. This is positive, and the number of staff participating in training is growing, but an enhancement so that a systematic approach to training is developed would be beneficial. Each regional office makes its own decisions, and any coordination by headquarters is not substantial.

615. GIFI is provided with an onsite inspection plan by the headquarters and each of the regional offices of the KAS, together with general reasoning behind the plan, at the end of each year; the plan takes account of risks. All regional offices of the KAS are provided with GIFI's guidance in November.

616. Offsite supervision is not undertaken by the KAS. It has carried out the following number of planned inspections covering casinos' AML/CFT responsibilities: 2017 (14), 2018 (8), 2019 (2), 2020 (4) and 2021(0). The AT notes that operations by casinos were limited by the pandemic in 2020. The number of inspections has decreased on the basis that the casino sector has only nine operators, of which two own 34 casinos between them. The KAS and provides the exit report to the MoF, who liaises with the KAS to review the seriousness of the findings, progress by the casino in remediation of breaches and whether any issues might lead to revocation of a concession. GIFI is also provided with a copy of the report. At least two people carry out each inspection. The content of inspections arises from the general guidance issued by GIFI each November to the headquarters and regional offices of the KAS. From the visit material seen by the AT, thought is given to checking compliance with AML obligations. A control procedure, albeit very high level, is used for inspections. The KAS advised that it focuses on operations rather than procedures. CFT is not separately considered from AML. Overall though, AML/CFT is an addition to the wider supervision of casinos, and there would be merit in the KAS and GIFI working together to develop inspections with greater depth and so that they are risk-based (including in relation to intensity).

617. The table below shows the number of onsite inspections undertaken by KAS to casinos and also to other entities, which go beyond the FATF standard but are relevant for the purposes of showing the split of priorities for the KAS between casinos and other e-gambling entities.

**Table 6.4 Number of controls conducted by KAS to casinos and other e-gambling entities (2017- Q1 2021)**

<b>CONTROLS IN CASINOS, GAME ROOMS AND MUTUAL BETTING POINTS</b>					
	2017	2018	2019	2020	1st quarter 2021
<b>Games rooms</b>	8	6	124	67	48
<b>Including targeted only at the AML area</b>	0	1	1	1	0
<b>Mutual betting points</b>	297	463	479	259	91
<b>Including targeted only at the AML area</b>	5	0	1	1	0
<b>Game casinos</b>	119	109	124	56	8

<b>Including targeted only at the AML area</b>	14	8	2	4	0
--	----	---	---	---	---

618. **Other supervisory authorities** - For the purposes of completeness, the table below contains information on onsite inspections undertaken by other supervisory authorities.

**Table 6.5. Total number of inspections conducted by each institution (2018-2020)**

<b>Total number of inspections conducted by each institution</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>
<b>National Association of Cooperative Savings and Credit Unions</b>	12	6	4
<b>Governors of provinces or governors of districts – associations</b>	15	16	0
<b>Ministers or governors of districts – foundations</b>	0	0	1
<b>Customs and Tax Control Offices</b>	19	27	18
<b>Total</b>	46	49	23

#### *6.2.4. Remedial actions and effective, proportionate, and dissuasive sanctions*

619. Until 13 July 2018, only GIFI had statutory power to issue administrative sanctions. From that date, three supervisory authorities have been able to impose sanctions in connection with violations they have found, namely the UKNF, the NBP and GIFI. Other supervisory authorities do not have the power to impose penalties, and they must send the results of onsite inspections to GIFI, which imposes penalties where it considers this appropriate. In addition, administrative penalties became applicable to individuals for the first time from 13 July 2018.

620. **UKNF** – Remediation of breaches is always required by the UKNF. Deadlines for remediation are set if justified by the severity of the breach and the significance of the recommendation by the UKNF. In the most significant cases, the UKNF monitors progress monthly, including by meeting monthly with officers of the FI. In other cases, reports on progress are required from the FI every three months. There is a procedure in relation to the issue of penalties. The UKNF's approach is to issue a written warning where the breach is relatively insignificant and to initiate use of stronger sanctions for other breaches. In 2018, 89 breaches identified led to the issue of five warnings; in 2019, 141 breaches identified led to three warnings and two fines; in 2020, 290 breaches identified led to no warnings and one fine; the UKNF advised the AT that offsite rather than onsite inspection handicapped the supervisor's ability to impose penalties. The fines were PLN 100 000 / €22 000 (a payment institution), PLN 450 000 / €99 000 (a commercial bank) and PLN 1,200,000 / €261 296 (a commercial bank). This last case was decided by the court of last instance (i.e. the institution appealed the penalty but the UKNF's conclusion was upheld by the court). For 2021, up to the end of May, the UKNF identified 117 breaches and has initiated six sanctions, which had yet to be resolved at the time of the AT's visit to Poland. Until March 2021, the UKNF was not able to issue more than one sanction (e.g. a warning and a fine) for a breach. The UKNF noted that it has been developing its approach and that, in 2020 and 2021, it has strengthened the approach to sanctions, including potentially in relation to individuals (no penalties have been issued to individuals to date). It also wishes to improve the promptness of imposition of sanctions as the process of imposition has taken about a year from the date of the inspection. In March 2021, a separate sanctions unit was established

with one lawyer so that supervisory officers are not also responsible for enforcement; the intention is to add further staff resources to the unit. Information on the sanctions imposed is provided to GIFI for publication by that body.

621. **NBP** – Remediation is required where the NBP detects breaches, and it makes recommendations for remediation; the currency exchange office is required to respond within 30 days as to what actions have been taken. There are procedures for the imposition of sanctions. Sanctions are issued by the headquarters, and those applied are specified in the table below. While quite a substantial number of fines were issued in 2017, the level of penalties in 2018/2019 diminished and is not consistent with the size of the sector and number of inspections; this pattern was attributed to the amendment and bedding down of the AML/CFT Law. However, since 2019 the number of fines imposed has been growing, with all fines being published (including the name of the person subject to the penalty) on the Ministry of Finance website and issuing its highest ever fines in the first few months of 2021. Penalties have been imposed on individuals (i.e. sole traders) as well as on legal persons. The table below shows the number of sanctions imposed by the NBP on entrepreneurs conducting currency exchange activities between 2017 and April 2021.

**Table 6.6 Number of sanctions imposed by the NBP on entrepreneurs conducting currency exchange activities (2017- April 2021)**

	Number of sanctions	Number of financial penalties	Sanction of publication	Total value of penalties (PLN)	The highest penalty (PLN)	Number of individual persons
2017 (imposed by GIFI)	50	-	-	-	-	-
2018 (imposed by GIFI)	7	-	-	-	-	-
2019	6	6	-	13 200 (= €3 100)	7 000 (= €1 600)	5
2020	36	31	5	69 200 (= €15 700)	8 000 (= €1 800)	27
January to 30 April 2021	8	8	-	23 000 (= €5 000)	6 000 (= €1 300)	3

622. **GIFI** – The completion of an inspection and communication with the institution is subject to a written process. The obligated institution receives the report, has an opportunity to make reasoned objections, and the process is ended by the issue of the final report by GIFI. Inspections result in the issue of a follow-up statement to the inspected institution. Examples seen by the AT were structured and systematic in approach. Breaches are advised to the institution with recommendations, the time frame for remediation and reporting to GIFI.

623. GIFI imposes sanctions under a Code of Administrative Procedures and has a long history of imposing penalties. It imposes sanctions except where a breach is not material and where the

obligated institution has remediated the breach. Such cases are rare. While the GIFI has issued only fines, it has also published each penalty (including the identity of the recipient) on its website since July 2018. The legislative changes in 2018 also provided GIFI with an ability to order obligated institutions to cease specified activities, but it does not regard any breach or series of breaches as having been sufficiently serious to warrant using this power. GIFI has provided explanations and other information at the request of prosecutors and appeared in court as a witness. It has advised that it has received feedback on proceedings (including discontinuation of them), but it is not clear to the AT to what degree liaison between the PPO and GIFI is systematic, and enhancement of the links would be positive.

624. There is scope for a greater number of sanctions to be imposed in areas such as the notary sector if a greater number of inspections were to be carried out.

625. The table below contains an overview of the total number of administrative proceedings conducted after the controls undertaken by GIFI and other supervisors between 2016 and 2021 up to the time of the visit to Poland by the AT for each type of obligated institution; the total amount and the maximum amount of penalties imposed and the number of notifications sent by the GIFI to the PPO. These notifications principally date to the pre-2018 legal changes, which provided GIFI with greater powers of sanction. Information on the outcomes of the notifications to prosecutors is not available to the AT.

**Table 6.7: Overview of the total number of sanctions imposed by the GIFI and other supervisors**

Type of obliged institution	Number of administrative proceedings in first and second instance conducted after controls of GIFI and other supervisors						Total amount of penalties (PLN)						Maximum financial penalty (PLN)						Number of notifications sent by the GIFI to prosecutors					
	2016	2017	2018	2019	2020	2021	2016	2017	2018	2019	2020	2021	2016	2017	2018	2019	2020	2021	2016	2017	2018	2019	2020	2021
Domestic banks, branches of foreign banks	36	13	14	1	4	0	1177500	498000	97500	0	4010000	0	200.000	125000	25000	0	3700000	0	5	4	0	0	1	0
Cooperative Savings and Credit Unions	11	0	1	0	0	3	49.500	0	3000	0	0	12000	25.000	0	3000	0	0	5000	0	0	0	0	0	0
Payment institutions	2	1	2	1	3	1	0	15000	36000	15000	25000	300000	0	15000	35000	15000	15000	300000	0	0	0	1	1	0
Brokerage houses	4	2	2	0	0	0	37.000	10000	5000	0	0	0	25.000	5000	5000	0	0	0	1	0	1	0	0	0
Investment companies (TFI)	1	1	0	0	0	1	30.000	10000	0	0	0	15000	30.000	10000	0	0	0	15000	0	2	0	0	0	0
Notaries	3	4	4	0	1	1	18.500	16000	2500	0	5000	5000	9.500	6000	1000	0	5000	5000	1	2	1	0	0	0
Entities operating in the field of games of gambling	1	4	3	0	1	0	1500	21000	20000	0	5000	0	1500	10000	10000	0	5000	0	0	0	1	0	1	0
Life insurance companies	3	2	0	0	0	0	360.000	550000	0	0	0	0	300.000	30000	0	0	0	0	1	1	0	0	0	0
Entities offering currency exchange services	29	52	19	0	1	0	174.400	334200	46600	0	500	0	150.000	100000	22000	0	500	0	0	0	2	0	0	0
Entities operating auction houses	2	1	0	0	0	0	80.000	5000	0	0	0	0	50.000	5000	0	0	0	0	0	1	0	0	0	0
Foundations	2	0	0	0	0	1	5000	0	0	0	0	1700	4500	0	0	0	1700	0	0	0	0	0	0	0
Entrepreneurs	2	4	2	0	1	1	15000	37200	9000	0	9000	5000	10.000	30000	6000	0	9000	5000	0	0	0	0	0	0
Precious metals dealer	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Real estate agent	0	0	0	0	2	1	0	0	0	0	507000	500000	0	0	0	0	500000	500000	0	0	0	0	0	0
Legal adviser	0	0	0	0	2	0	0	0	0	0	10000	0	0	0	0	0	5000	0	0	0	0	0	0	0
Lawyer	0	0	0	0	1	1	0	0	0	0	5000	2000	0	0	0	0	5000	2000	0	0	0	0	0	0
Tax advisor	0	0	0	0	1	0	0	0	0	0	18500	0	0	0	0	0	5000	0	0	0	0	0	0	0
Accounting office	0	0	0	0	0	1	0	0	0	0	0	1300	0	0	0	0	0	1300	0	0	0	0	0	0

### ***6.2.5. Impact of supervisory actions on compliance***

626. GIFI, the UKNF and the NBP have created a positive difference in compliance by obligated institutions at various levels. There are better quality AML/CFT policies; implementation of new and better procedures; better business risk assessments and understanding of risk; better provision of training; better CDD mitigating measures, including in relation to beneficial ownership; purchase of more IT software; an increase in the number and upskilling of compliance staff; strengthening of internal controls; and an increase in focus in AML/CFT compliance. The larger institutions demonstrate more of these improvements. FIs, in particular, have responded well to training by supervisors.

627. GIFI provides outreach across the FI and DNFBP sectors. In addition to what is said in the paragraph above, it considers its positive impact is evidenced by increased training activities by obligated institutions. Its supervision of banks, with a particular focus on SAR filing in 2020 and 2021, has had a positive effect on transaction monitoring and SAR processes. Overall, it has seen positive effects in terms of better compliance with AML/CFT provisions brought both by a combination of outreach, supervision and post-inspection recommendations, as well as the imposition of administrative penalties, e.g. publication of information about penalties on its website and notifications of suspicion of committing a crime of money laundering or financing of terrorism submitted to the Public Prosecutor's Office.

628. In line with its priority to address emerging risks, the UKNF has successfully raised awareness of technology issues and channels for potential ML and TF. Banks and payment institutions have responded positively to this. The UKNF sees the positive impact of outreach and training activities it conducts as crucial as it has positively affected the entire financial sector. Awareness of the AML/CFT obligations by credit unions has also been positively affected by actions taken by UKNF as well as the NACSCU.

629. Inspections carried out by the NBP, as well as fines imposed, have contributed to the currency exchange office sector, demonstrating a stronger awareness of its AML/CFT obligations.

630. The Appeal Courts (i.e. the judges acting for the Presidents) have also made a positive difference; notaries treat AML seriously. The controls carried out by the Presidents of appeal courts and GIFI have had a positive impact on the whole notary sector; this includes their professional bodies, which have mobilised to raise awareness of AML. In addition, GIFI has noted the positive impact of its outreach and training activities with respect to notaries.

631. The KAS has noted that supervision has led to improved customer identification and monitoring of game play and that its inspections of casinos have a positive effect, evidenced by the few irregularities in this sector.

### ***6.2.6. Promoting a clear understanding of AML/CFT obligations and ML/TF risks***

632. GIFI has undertaken significant outreach to supervised entities over the period under review, notwithstanding the limitations imposed by the pandemic and the consequential reduction of opportunities for outreach. It has mainly covered non-FI sectors as much of the financial sector is subject to outreach by the UKNF.

633. GIFI has developed a free e-learning course for all obligated institutions, which was launched in February 2019 and has been completed by over 34,000 participants. It provides significant information (including FAQs) on its website and has issued a range of communications

such as risk documents and guidelines on matters such as the updating of the AML/CFT Law in 2018; control procedures; non-face-to-face business; restrictive measures; CDD for currency exchange offices; beneficial owners; virtual currencies; and the scope of notarial activities subject to AML/CFT requirements. Training has included events such as meetings or seminars.

634. In 2018, training was provided to VASPs in relation to their obligations under the revised AML/CFT Law. There were also four meetings with groups of obligated institutions, including on sanctions. These were followed in 2019 with four seminars on sanctions to a range of FIs and DNFBPs. In 2019 GIFI worked with the Security Council of Banks in relation to suspicion, cross-border transfers, fiscal crime, virtual currencies, and payment institutions; and participated in a meeting with banks on security and AML structures. In the same year, it undertook meetings with and training for the gambling sector. In 2020 cooperative banks were provided with training on sanctions and the NRA.

635. GIFI has also made presentations to a range of individual institutions. In addition, it has provided training on AML and CFT (including restrictive measures in particular) to other supervisory authorities, which informs outreach undertaken by those supervisors.

636. The UKNF maintains information on its website and has issued guidance (also placed on the website) on verification of identity by video; the issue of questionnaires by banks to obtain information from payment institutions; risk assessment; publication of the NRA; and crypto-currency and other virtual asset exchanges. Notification of the revisions to the AML/CFT Law in 2018 was made by letter and several seminars, each of which was dedicated to a particular sector.

637. It has actively engaged with obligated institutions to raise awareness about risk and its mitigation; this included the issue of guidance in 2018 on risk assessment and sector-specific seminars. This theme of raising awareness of risk has also included working with FIs in meetings and workshops to raise awareness of and address the risks of virtual currencies before they become a feature of the Polish system. As part of this theme, in 2018, the UKNF published an announcement on the functioning of virtual exchanges and crypto-currency exchanges and the UKNF's expectations with regard to establishing and maintaining business relationships with virtual asset service providers. In addition, the UKNF has encouraged enhanced communication between banks and payment institutions so as to improve communication between those two sectors. Under the Innovation Hub programme, the UKNF has held meetings with obligated institutions, applicants and other stakeholders on technological advances and solutions. More than 1,000 representatives of obligated institutions from all of the sectors under the UKNF's supervision (together with several hundred law enforcement officials) have attended seminars led by the UKNF as part of the Education Centre for Market Participants (CEDUR) programme. This programme provided additional opportunity for the UKNF to present its expectations on the implementation of AML requirements and new trends and risks – this has included risks posed by VASPs. Dedicated training on TF has been provided to the banking, investment and payment sectors. Meetings have been held with the Polish Bank Association to discuss approaches to meeting AML/CFT obligations and the changing technical requirements for wire transfers, and with the Polish Organisation of Non-Payment Institutions and the Polish Banking Association with regard to obligations for payment institutions and co-operation between banks and payment institutions. The UKNF has also worked with LEAs and prosecutors, among other authorities, in providing training to the private sector. On a substantial number of occasions, officers of the UKNF have made presentations to the private sector at conferences or training courses.

638. The NBP maintains information on its website. In 2018 the NBP informed all entrepreneurs by letter of the changes to the AML/CFT Law. In 2019 the NBP arranged two meetings on the revised legislation, which were attended in total by 200 entrepreneurs.

639. More generally, all three authorities respond to queries from obligated institutions and work closely together (GIFI in particular) on promoting better understanding of AML/CFT by institutions. They provide outreach to obligated institutions by supporting joint training to such institutions through joint sponsorship or contribution by participation or providing information for use in the outreach. Also, Communication No 30 on investment decisions in relation to virtual currencies, information on legal changes, meetings after onsite inspections and the provision of model procedures have involved inter-authority liaison.

### ***Overall conclusions on IO.3***

640. The market entry licensing verifications checks carried out by 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 some 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's supervisory team would benefit from a relatively small number of additional staff. There is no supervision of DNFBP sectors which are subject only 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.

641. **Poland is rated as having a Moderate level of effectiveness for IO.3.**

## 7. LEGAL PERSONS AND ARRANGEMENTS

### 7.1. Key Findings and Recommended Actions

#### ***Key Findings***

##### ***Immediate Outcome 5***

- a) Information on the types of legal persons is maintained in the public domain;
- b) 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);
- c) 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.
- d) The overall approach to transparency is multi-faceted. 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. There is very good operational exchange of information between authorities;
- e) Basic information is maintained in the NCR. A significant number of applications for registration is refused or dismissed. The NCR team undertakes wide-ranging checks prior to registration and also after registration, including checks on foreign databases, which have a positive effect on the quality of registered data. The checks at the application stage 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;
- f) Poland has taken the positive step of establishing 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. The KAS, the UKNF and GIFI routinely use the information on the register, which has the effect of checking the information used;
- g) The team responsible for administering the CRBO information has commenced verification of data to ensure it is adequate, accurate and current by undertaking a major sampling exercise and strong checks of the data selected. It is planned for a systematic programme to be undertaken once prospective additional staff

have been recruited;

- h) Poland has also established a database of information provided by banks on owners and beneficial owners of bank accounts and transactions made using the accounts (the NCH). The NCH team checks that the data is complete but does not verify its accuracy. The KAS, the UKNF and GIFI routinely use the information on the register, which has the effect of checking it.
- i) The basic and beneficial ownership registers and the NCH database 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. Significant attention has been paid by the UKNF (in particular) and GIFI to assessing the adequacy of beneficial ownership information held by banks. The AT found a range of very positive aspects to banks' approaches to beneficial ownership, and the UKNF, GIFI (as supervisor and FIU) and the KAS have found the information held by banks to be generally reliable. Banks' approaches, including recognition of control through forms other than ownership, have improved and continue to develop;
- j) GIFI (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. In addition, a project has commenced analysing legal persons that had not registered information with the CRBO against transactional data. It has also passed cases to the KAS for its analysis and investigation;
- k) 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. This includes information from a wide range of sources and searches for disguised links and control. 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;
- l) 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). 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.
- m) The above key findings are not only relevant to fictitious companies but also to other forms of misuse and ML.

## ***Recommended Actions***

### ***Immediate Outcome 5***

- a) The Financial Security Committee should develop its approach so that it ensures that the strategies and operational activities (including enhanced multilateral co-operation) of the relevant authorities are coordinated to:
  - i. understand and address the risks of misuse of legal persons, including by documented and joined up strategies;
  - ii. measure and monitor to what extent basic and beneficial ownership information held by registers, the NCH database and obligated institutions is adequate, accurate and current and verified as such on the basis of risk;
  - iii. monitor the effectiveness of (i) individual authorities in mitigating the risks of misuse of legal persons and (ii) the framework as a whole in mitigating the risks (including the approach to, and application of, sanctions);
- b) The national risk assessment should be developed so that the risks of legal persons should be comprehensively assessed;

The CRBO team should:

- c) as planned, recruit additional staff and develop its approach so that it is comprehensive and risk-based in relation to (i) verification of the accuracy, adequacy and currency of data received and (ii) the prompt filing of changes to data;
- d) ensure that the CRBO is fully populated as soon as possible;
- e) develop the approach to the consideration and imposition of fines so that the sanctions framework is proportionate and dissuasive and also to notify the relevant NCR Court and the KAS team administering the VAT register upon the imposition of a sanction;
- f) document its operational activities relevant to ensuring adequate, accurate and current data in writing (by procedures or otherwise);
- g) refine the reporting to the regional head of the KAS and to MoF so that the above elements can be measured;

The NCR team should:

- h) enhance the existing mechanism for coordination and monitoring of the effectiveness of the regional court system;
- i) enhance the process for verifying data (including by risk-based approaches), and document operational activities for ensuring adequate, accurate and current data so as to ensure consistency of approach through the system;
- j) develop the approach to the consideration and imposition of fines (and the maintenance of statistics in relation to fines and provision of information when a fine is imposed to the KAS team administering the VAT register and the CRBO team) and document expectations and processes where information on coercive

- proceedings is passed to the PPO;
- k) enhance the approach to training so that it is systematic;
  - l) The KAS should enhance its approach to statistics so as to facilitate further analysis of effectiveness.

642. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37 and 40.<sup>65</sup>

## 7.2. Immediate Outcome 5 (Legal Persons and arrangements)

643. At the end of December 2020, there were 573 800 legal persons established in Poland. The concept of commercial the company covers all kinds of legal persons subject to the Commercial Companies Code and includes limited liability companies, joint-stock companies, limited partnerships, partnerships and limited joint-stock partnerships. Business activity is carried out by a wide range of legal persons. Statistics are not available on the number that are inactive, but a few tens of thousands seem likely. Inactive companies are those which have confirmed they have no staff and have applied to the NCR to suspend economic activity for between 30 days and two years. Applications can be made on a repeated basis. The authorities have advised that the inability to conduct business and absence of current income means the legal person cannot be used for ML. However, it would still be possible for suspended companies to have been used for ML and to be dormant, pending future use for ML. Companies that have not applied for suspension but are nevertheless inactive can be detected and struck off the NCR.

**Table 7.1: Legal persons in Poland**

Type of legal person	Number as of December 2020
Limited liability companies	446 732
Joint-stock companies	9 546
Limited partnerships	43 292
Professional partnerships	2 426
Limited joint-stock partnerships	3 390
Societas Europea	8
European Economic Interest Grouping	8
Foundations	11 537
Associations	7 227
Cooperatives	10 934

644. Legal arrangements cannot be formed in Poland.

<sup>65</sup> The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

### ***7.2.1. Public availability of information on the creation and types of legal persons and arrangements***

645. The commercial legislation that governs the creation and operation and specifies the types of legal persons is publicly available.

646. The Ministry of Justice (MoJ) is responsible for the NCR (which is operated by the district courts), which is the register of legal persons and holds basic information. The registers are kept in electronic format and are publicly accessible via the website of the MoJ.

647. The Central Register of Beneficial Owners is publicly available via the website of the Ministry of Finance (MoF), which administers the register. The website also contains information about the register, including FAQs and a user guide prepared by GIFI.

### ***7.2.2. Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities***

648. Poland has assessed elements of the ML/TF risks associated with legal persons. Understanding is greater than the picture provided in the NRA. However, a significantly more comprehensive assessment and detailed report will be of benefit to the authorities and the private sector in ensuring and demonstrating a comprehensive and joint understanding of the risks. This would include gathering relevant information on which to inform countermeasures and the effectiveness of those countermeasures in one place.

649. There is some information on the creation and operation of business entities in the NRA report. It is clear from the report, further material provided to the AT and discussions with the authorities that the most serious risk of abuse of Polish companies is uniformly regarded as VAT fraud (and linked ML) facilitated by the use of fictitious companies (i.e. limited liability companies which have no substance and which are established only to facilitate VAT fraud) and “straw men” (who are Polish citizens recruited to act as the single shareholder/beneficial owner and chief executive of the company). While there are features common to VAT fraud schemes that have used legal persons, such as the operation of numerous companies from a single address, inevitably, the absence of substance and commercial activity only becomes apparent after incorporation. This narrative is supported by the NCR team, GIFI from its financial intelligence, the PPO and the Central Investigation Bureau of the Police. VAT fraud has mostly been related to fuel (prior to recent legal changes), electronics (prior to recent changes in tax regulation), rapeseed oil and biofuels, coffee and food products, investment gold and silver (prior to recent changes in regulation), plastics and scrap metal.

650. In line with this theme, a significant number of notifications by GIFI to the KAS for analysis and investigation indicate suspicion of VAT fraud. These notifications include common features such as potential understatement or non-disclosure of turnover due to forgery or concealment of invoices, by undue reimbursement of value added tax, “missing trader” fraud and carousel fraud in relation to intra-European Union transactions. In addition, a significant proportion of the notifications contain information regarding the suspicion of concealing the object of taxation, understatement of revenue, undisclosed income, or fraud in the import of goods. The KAS has analysed and, in a significant number of cases, investigated these notifications.

651. In addition, the NRA report indicates that, to a much lesser degree, ML by misuse of legal persons involves cross-border transfers; the opening of bank accounts with funds from several sources and which do not trigger the CDD threshold, with the aim of transferring the entire

balance to another account at a later stage; and the transfer of large amounts to a single account. This understanding has been agreed by the authorities on the FSC.

652. Other risk scenarios not specified in the NRA report have been identified. GIFI advised the AT that LLCs are misused for ML in other ways, specifically where the company is legitimate and engaged in business. In these cases, typically, payments representing the proceeds of crime are made through a bank account in Poland, probably for a commission. In addition, the AT was advised that criminal groups establish complex structures in which control is concealed, with legal persons being established in a range of jurisdictions (in particular offshore jurisdictions) and BOs located in a separate range of jurisdictions are added after establishment. In these situations, individuals acting as representatives of legal persons are used as a cover for the BOs.

653. GIFI has developed a model typology for the establishment and use of fictitious companies. This typology is detailed. As part of the process for achieving a common understanding of risk, GIFI has shared its conclusions on the use of legal persons in training seminars for the criminal justice, tax and supervisory authorities, and, to a lesser degree, the registries and the NCH database. GIFI representatives have also regularly taken part in conferences, workshops, seminars, and briefings it has organised (particularly for banks, insurers, notaries and lawyers) or organised by other authorities or obligated institutions and provided information about risks posed by legal persons. Events with the private sector institutions mentioned above also covered specific topics, namely the use of legal persons in relation to trafficking in works of art and cultural property; VAT fraud and ML in connection with fuel market transactions; carousel fraud offences; and tax fraud in light of the Panama papers. Information with sanitised cases and typologies related to legal persons misuse and "carousel" offences is a regular part of GIFI annual reports, which are publicly available. This outreach by GIFI enables improved understanding of risks but, in the view of the AT, is not a substitute for sharing a comprehensive assessment and typologies such that all stakeholders have a common and detailed platform of information from which to work.

654. The KAS holds and has access to significant information on and relating to legal persons, including on their purpose; directors, representatives, shareholders and beneficial owners; and transactions. The information is subject to comprehensive analysis (see below), which informs the KAS to a very substantial degree of the risks of use of legal persons for tax frauds – and the laundering of the proceeds. There is a very good level of co-operation by the KAS with other authorities (see below), especially the teams administering the NCR, the NCH, and the CRBO, and the GIFI. There would be a benefit in coordinating a review of the data held by the KAS, and its findings and conclusions, together with the information held by the other authorities for the more comprehensive ML/TF risk assessment by the authorities articulated above.

655. The recent establishment of the CRBO meant that its contribution to the NRA was narrow. It has provided statistics to the AT which break down the country of residence and citizenship of BOs, which indicate that (in order of prominence) 86.9% of BOs are Polish, 2.5% are Ukrainian, and 2% are German. The remainder includes a wide range of nationalities. In addition, 73.79% of beneficial ownership is by direct ownership (in which the legal owners are individuals); 16.54% by indirect ownership (where there is at least one layer above the legal owner(s)) and 9.67% by control by other means or through a senior managing official. The MoJ sits on the FSC and contributes to the NRA from that position; the NCR team demonstrated awareness of differences in the geographical distribution of shareholdings of companies to the AT based on its use of foreign beneficial ownership and company databases. The statistics, which can be developed from a complete register of beneficial ownership information and mining of the information held on

the NCR and CRBO and activities by the registry teams, would provide a more comprehensive basis for the next NRA than was the case in 2019.

656. The NRA identifies high-level TF risk scenarios, pointing out the potential misuse of legal persons both directly in acquiring funds to support terrorist activity as well as indirectly as a means of transferring those funds. The most vulnerable types of legal persons were identified as related mainly to real estate, trade in electronics, the used car market, precious metals, textiles. Furthermore, linked with these business activities, the NRA also mentions the fusion of funds acquired for TF purposes with the legal revenue of a legal person in order to hinder the identification of TF. The authorities have confirmed that they have seen no examples of legal persons being used for TF.

### *7.2.3. Mitigating measures to prevent the misuse of legal persons and arrangements*

#### ***Policy Initiatives and Registries***

657. In recognition of the risks of misuse of legal persons posed by VAT fraud, there has been a national initiative to address these risks. An amendment to the Value Added Tax Act (the VAT Act), which came into force in January 2017, introduced changes to restrict the operation of companies used for criminal activities and gave the KAS an ability to strike off a company from the VAT register in specified conditions. Strike off means that the company cannot trade or hold itself out as trading. The conditions for strike off include companies for which taxpayers do not exist, companies that do not respond to documented communications by the KAS; companies that provide incorrect data in the application for registration on the VAT register; companies that have issued blank invoices; and companies that the KAS knows, or has legitimate reason to suspect, have engaged in tax fraud. In addition, legislation that came into effect in early 2018 amended several other acts in order to prevent the use of the financial sector for tax fraud and provide the KAS with additional powers such as the ability to block/freeze the assets of legal persons, including on the basis of risk scoring.

658. In addition, in 2019, the KAS replaced a tax blacklist of persons with a whitelist, which it publishes on its website; as a result, anybody can verify the bank account number of any person (including legal persons) registered for VAT. Also, in early 2020, the KAS took the decision to introduce a new system to enable the issue, acceptance and clearance of VAT invoices in electronic form, which will enable more consistent approaches to form completion by registered persons, quicker analysis by the KAS and further opportunities for data mining. 2020 also saw a new requirement from KAS on the payment route for VAT payments so as to reduce the possibility of VAT fraud.

659. An amendment to the Commercial Companies Code in 2019, which came into effect in March 2021, requires registration by joint-stock companies and joint-stock partnerships of bearer shares. The authorities are not aware of any breaches of this provision, and a breach would, in any case, mean that shareholder rights cannot be exercised. The binding nature of bearer shares automatically expired in March 2021 and registration of the shares in the shareholders register was automatic. Based on their operational experience, such as analysis of financial intelligence by GIFI and the findings of onsite inspections by supervisors, the authorities have confirmed that bearer shares were in any case rare. While there were mitigating measures in place prior to March 2021 so as to prevent the sale of bearer shares on an organised market,

they could still potentially have been transferred privately for almost all of the period under review.

660. Other policy measures taken in the period under review by the AT also have a direct or indirect effect on preventing the abuse of companies. These include the establishment of the CRBO in 2019.

661. The system for ensuring adequate, accurate and current data is available is multi-faceted. The number of registers, their coverage and the links between them are a strength of the Polish system. The NCR (which also includes the register of entrepreneurs who are not sole traders) and the CRBO are complemented by other registers such as the NCH; the Central Register of Entities – National Taxpayers Register (a register of all taxpayers), the VAT register (which is public); the National Criminal Register; the Register of Insolvent Debtors; the TERYT Register of Territorial Administrative Divisions (which holds information on business and residential addresses of legal persons and individuals); the Central Register and Information on Economic Activity (CEIDG); the National Official Register of National Economy (REGON); and the Universal Electronic System for Registration of the Population Register (the PESEL Register). The PESEL Register is a database of Polish citizens. When a citizen is added to the database, a personal identification number known as a PESEL number is allocated to that person, which is used for that person throughout their life and in other databases maintained by public authorities. This means that the entry of an individual in any database can be cross-referenced across several databases. A range of authorities has direct access via digital link to the PESEL Register, including the court officials administering the NCR (described as the NCR team for ease of use), the CRBO team and the KAS. A change to an individual's details in the PESEL Register is transferred automatically to other registers if the information relevant to the change is contained in those other registers. The REGON is a national business register maintained by Statistics Poland; all legal persons that are businesses must be registered. Entrepreneurs who are sole traders must be registered in the CEIDG. A range of authorities (including the KAS, LEAs and the PPO, although not the court officials administering the NCR or the CRBO or NCH teams) have direct digital access to the CEIDG database. The NCR, the CRBO, the KAS and, for specific cases, GIFI have direct access to the National Taxpayers Register.

662. There is also a central registry of electronic extracts of notarial deeds, the Central Repository of Notarial Deeds, which is maintained by the National Notarial Council. Notaries and the courts administering the NCR have access to this registry.

### ***Operational Coordination***

663. All authorities met demonstrated commitment to their functions and ensuring high quality basic, and beneficial ownership information is available. There are elements of coordination, and there is very good exchange of information at the operational level to combat misuse of legal persons, particularly in relation to VAT fraud. However, coordination is not multi-faceted in addressing misuse of legal persons, and the useful activities of authorities are not externally reported and drawn together into a “whole of government” approach with monitoring of the overall effectiveness of the framework and development of the approach.

664. By way of illustration of co-operation, the NCR team receives information from the Central Repository of Notarial Deeds, the PESEL Register, the REGON, the CEIDG, the National Criminal Register and the National Taxpayer Register via its ICT system. In addition, the NCR team receives information from other authorities (e.g. the PPO or local prosecutors and regional offices of the KAS) regarding outdated data disclosed in the NCR (e.g. the address of the entity's registered

office). This has led to coercive proceedings by the NCR team against companies. Also, in the NCR team's proceedings for deletion of inactive legal persons from the NCR, the team requests and receives information from other authorities as to whether the entity is active and has assets. The NCR team has advised the AT that information from other authorities has enabled it to strike off 21 313 legal persons in total from the NCR during the period 2017 to 2020.

665. A range of authorities have provided information to the CRBO in relation to the lack of an entry in the CRBO (164 occasions), entry into the CRBO after the deadline (38 occasions) and inconsistencies of data held by the authority and data in the CRBO (6 occasions). These authorities are the KAS (122 occasions), GIFI (76 occasions) and the NBP (10 occasions). The CRBO is looking to formalise arrangements with other authorities via the signing of MOUs.

666. As part of its checks on 20 000 companies, the CRBO team has requested the KAS to verify the registered office address of legal persons, and this, in turn, has led to the KAS making notifications to the NCR team for potential strike off of legal persons from the NCR. The KAS also has made numerous other notifications to the NCR team for potential strike off by the Court as a result of its tax responsibilities (these requests are part of the KAS's countermeasures, including revocation of taxpayer numbers and strike off from the VAT register.) GIFI has requested verification of data from the CRBO team, which has also led to the NCR team checking its records and, in some cases, strike offs by the Court.

667. In addition, both the NCR and CRBO teams have confidential information, which has been made available to requesting authorities upon receipt of an application confirming the legal basis of their request and that the information will be kept confidential. Statistics on the frequency of these notifications and accuracy of the data arising from these exchanges of information are not available.

### ***NCR – Basic Information***

668. While the MoJ is responsible for maintaining the NCR, the register (kept in computerised form) is operated by district courts situated in major Polish cities. It comprises three registers in total, one of which is focussed on entrepreneurs (which include, inter alia, legal persons and basic information in relation to them). There are 590 court officials in 21 registration courts across Poland involved in registration and review of registered information, although they are also engaged in other court activities; these officials, described as the NCR team in this MER, are supported by over 120 other staff. The MoJ considers that there are sufficient staff within the Ministry and the courts to administer the NCR.

669. Presidents of the Appeal Courts have a monitoring responsibility in relation to the NCR and the activities of the NCR team; this is complemented by the responsibility of the Presidents of the District Courts to the structure and staffing of the NCR team and related Courts. The MoJ receives combined statistics on this monitoring on a monthly basis, which show their activities, e.g. the number of applications, refusals/dismissals, legal persons registered, coercive proceedings initiated, the number of strike offs, the punctuality of court processes, and staff numbers. It monitors the operation of the NCR through these statistics (which show monthly, quarterly and annual data) and also exercises "external administrative supervision" of the operation by using court officials delegated to the MoJ. This is positive and has led to the MoJ encouraging swifter approaches in relation to coercive proceedings. In addition, visiting judges from the District Court conduct onsite inspections periodically (perhaps every two years) and, inter alia, examine the activities of the Courts responsible for the NCR and the activities of the NCR team. These inspections include examination of the files for legal persons and the adequacy,

accuracy and currency of the data on the NCR. The reports of the visiting judges are retained within the Court system, and recommendations are provided to the NCR team. These monitoring and coordination processes are very positive external checks relevant directly and indirectly to the adequacy, accuracy and currency of information in the NCR; there is scope to enhance these processes by, for example, recording and circulating statistics on the number and level of fines and provision of this information and relevant information on the findings of the visiting judges to the MoJ. More generally, the AT's understanding is that at least some parts of the court system in Poland are under resourced, and it has a concern that a logical outcome of this would affect the functioning of the NCR. Training for judges, registrars and other judicial staff is organised by the National School of Judiciary and Public Prosecution. The training programme includes AML/CFT, but there is scope to develop training programmes so that they are systematic and focused on risk and transparency of information.

670. Prior to entry in the NCR, a limited liability company and a joint-stock company can be considered to be "in organisation" for a maximum of six months from the date of conclusion of the articles of association. This is a historic process dating to when registration processes took much longer, its purpose being to allow such companies to undertake the organisational tasks necessary to prepare for future business activity, such as opening a bank account. The UKNF and GIFI confirmed that banks treat such entities at this stage as high risk (also noted by the AT in examples of bank documentation it has seen), including measures specific to these entities, such as a limitation on use of the account and monitoring of timing of receipt of information from the NCR on registration. Both authorities advised that they have not seen examples of inadequate CDD in relation to such entities. Acquisition of legal personality by such companies requires entry into the NCR within the six-month period. Failure to meet this deadline has led to the NCR team rejecting entry on the register.

671. Applications for registration in the NCR are received in paper form. The application (with the attached documents) is verified in several ways and not only from the point of view of compliance with the completeness of the data with regard to applicable provisions of law.

672. First, the NCR team cross-checks the information in the application with its own records.

673. Second, the team cross-checks the information in the application with the data on all the registers mentioned above, except for the NCH. By way of illustration, this involves checking all directors, representatives mentioned in the application and all shareholders with the National Taxpayers Register (and the former blacklist and current whitelist of taxpayers administered by the KAS), business and residential addresses on the TERYT Register. It also includes a check on the National Criminal Register in relation to any individual who can represent the legal person in any way. This representation includes directors and other named representatives and, automatically, shareholders of all legal persons other than LLCs and joint-stock companies as to whether they have been convicted of crimes or received any prohibition to conduct business activity or perform functions in legal persons. It is rare for shareholders of joint-stock companies to be able to bind the company, while for LLCs, it is common for shareholders also to be directors. The NCR team notes that there are also legal provisions that, in specified circumstances, prevent individuals who have been convicted from being directors, representatives and shareholders. Access by the NCR team to the significant amount of registered data on both individuals and legal persons is a notable benefit.

674. Third, the team checks the directors, any representatives of the legal person mentioned and shareholders in the application with the publicly accessible beneficial ownership registries of the UK and EU Member States.

675. Fourth, the team uses the E-Justice system to check the directors, any representatives of the legal person mentioned and shareholders with the company registers of EU Member States.

676. Fifth, some types of FIs that are legal persons, in particular any person linked with banking, are checked with the UKNF to ensure they have the necessary permissions from the supervisory authority.

677. Sixth, the existence and content of the notarial deed is checked against legal requirements (including that the Central Repository of Notarial Deeds has been updated), as well as consistency of the notarisation and deed with the rest of the application. A notarial deed must be provided by a notary (subject to AML/CFT requirements) for some types of transactions. For the purposes of incorporation, the completion of articles of association of a limited liability company, a joint-stock company, a limited partnership and a limited joint-stock partnership comprise such a transaction and must therefore be in the form of a notarial deed. The deed includes, among other information, the names, surnames, parents' names and place of residence of natural persons, the name and seat of legal persons or other entities participating in the deed; and the names, surnames and place of residence of persons acting on behalf of such legal persons/entities, their representatives, and other persons present when the deed is drafted.

678. A large number of applications to establish legal persons have been refused or dismissed by the NCR team. For example, in 2017, there were 63 100 applications, of which 9 164 were refused and 2 577 dismissed; in 2018, there were 61 812 applications of which 9 320 were refused and 2 942 dismissed; in 2019, there were 66 547 applications of which 9 957 were refused and 3 192 were dismissed; in 2020 there were 66 523 applications of which 8 432 were refused and 3 448 dismissed; and in the first quarter of 2021 there were 19 205 applications of which 2 237 applications were refused and 827 dismissed. An application is dismissed by the NCR team due to irregularities of a substantive nature, while an application is refused due to formal irregularities or deficiencies. The NCR considers that its checks and the number of refused/dismissed applications have led to a significant number of legal persons not being formed, which would otherwise have been misused. The entirety of the application, along with the fact of refusal or dismissal, is publicly accessible.

679. The NCR team's first step in dealing with the risks of legal persons post-incorporation is to advise the KAS when a legal person is entered on the NCR so that the KAS can begin to consider the implications from its perspective. This enables the KAS to undertake its analysis and to advise the NCR of any issues.

680. Changes to information already provided to the NCR must be advised to the NCR team within seven days of the change. These changes are subject to the same checks by the team as those undertaken for the application for incorporation.

681. There have been rare occasions when incorrect data has been found by the NCR team after incorporation – this is followed up and coercive proceedings initiated. These proceedings comprise an instruction to a legal person to provide updated/correct to the NCR by a specified date or pay a fine – the level of the fine is specified in the letter.

682. As the information held by the NCR team includes the date of the end of the financial year for each legal person, it is able to maintain an automated diary of the date when financial

statements should be provided to it. The team initiates coercive proceedings each quarter for legal persons that have not provided financial statements for a specific financial year ending within the previous quarter and requires them to submit the overdue financial statements within seven days from the delivery of the decision on the initiation of the proceedings. This process has enabled the NCR to detect and strike off fictitious companies. A report on the activities of the company is required at the same time as filing the financial statements, which also provides the names of the directors and shareholders as at the time of submission of the report. The report must be authorised by the directors. The information on directors and shareholders is used to check whether the register is up to date.

683. The NCR team also checks its records when it receives information from another authority such as the KAS, GIFI or the social security authority, which suggests there might be an issue. Some 90% of total coercive proceedings (generally for strike off) are initiated by the NCR team as a result of information received from the KAS.

684. The NCR team must be advised within seven days of a legal person ceasing to do business. This triggers the procedures for strike off and removal of the legal person from the register. At the time of removal, a notification is made to the KAS, the National Taxpayers Register and the REGON so that they can remove the legal person from their records as an active business.

685. The NCR team considers that it is very rare for information on the NCR not to be up to date (i.e. the seven-day deadline for filing changes to registered information has not been met or a business has not advised that it has discontinued business). Overall, it considers that the system of updating records is highly effective; failure to update information would automatically lead to a fine or strike off. The MoJ also noted that, on the very rare occasions where updates have not been made to the NCR by the legal person, the level of co-operation between the AML/CFT authorities means that those authorities, particularly the KAS, advise the NCR team of an update where it is known to them, thus enabling the NCR team to take action. The KAS supports the view of the NCR team.

686. Overall, even with the existing positive approaches and outcomes, there is some scope to further enhance the checks by the NCR team by, for example, use of the internet, use of an IT tool provided by a private sector data service provider, enhanced checks on the address of the registered office on the basis of risk, further extending checks at the National Criminal Register to LLCs on the basis of risk, liaison from the NCR to the KAS both at the application stage and post-incorporation on the basis of risk, checks on the registered office (e.g. to review if the records specified in c.24.4 and 24.5 are up to date), a more specific approach to risk generally. There is also scope to complement the specific statutory data requirements and approaches of the NCR team by preparing a procedure for review and verification of data so as to more easily demonstrate a systematic approach that can be used and monitored by all regional Courts and the MoJ.

### ***National Clearing House - Beneficial Ownership***

687. As a result of amendments to the tax legislation in 2018, the NCH has become a database of information provided by banks on owners and beneficial owners of bank accounts and transactions made using the accounts. It is fully populated and holds the following beneficial ownership information: full name; PESEL number; type and number of identification document; date and country of birth; nationality; address; and contact details. Changes to bank account information and new bank accounts are notified to the NCH electronically. Officials at the registry check that the information is complete (i.e. in line with legislative requirements) but do not

otherwise verify it. The activities of the KAS, the UKNF and GIFI, which use information from the NCH, directly or indirectly, have the effect of checking the accuracy of the database; the KAS liaises with the NCH on a daily basis. The NCH is part of the system for preventing misuse of legal persons by facilitating the roles of other authorities, including by providing the initial risk scoring for VAT purposes and, on a daily basis, feeding information directly into one of the more significant software tools operated by the KAS. The NCH has a separate department, with ten staff, which deals with STIR (see the section on KAS below), and the KAS has a positive view of the NCH's and the department's IT and other systems and staff skills. The AT is not aware of the overall number of staff which operate the NCH.

### ***CRBO - Beneficial Ownership***

688. The CRBO team has 15 staff and falls under the overall authority of the KAS. The staff complement has steadily increased since the CRBO was established in October 2019, and the team is recruiting three further staff; the MoF considers that 20 staff in total are needed. Support has also been provided by the legal department of the KAS (which is based in the same building as the CRBO team) when needed. A systematic training programme for AML/CFT is not yet in place. On a monthly basis, the CRBO team reports statistical data to the regional head of the KAS and the MoF. While there is scope to refine this, the reports are a good basis for reviewing the effectiveness of the team in relation to transparency and combatting misuse of legal persons.

689. Legal persons registered at the NCR after 13 October 2019 were required to insert BO information on the CRBO within one week of registration. The deadline for population of the register by legal persons on the NCR on 13 October 2019 was moved from 13 April 2020 to 13 July 2020 in light of the Covid-19 epidemic. At the time of the visit to Poland by the AT, the CRBO held data on more than 366 000 legal persons. It, therefore, contained beneficial ownership information on the majority of legal persons. Entry on the register is achieved via a digital portal by a designated representative of the legal person; the representative is required to confirm that the data is correct. This is a positive check on ensuring the entry is correct. The representative can be any person appointed by the legal person and is generally not a lawyer subject to AML/CFT obligations. An average of 450 notifications is made each day.

690. Quite a substantial number of legal persons in existence on 13 October 2019 had not registered beneficial ownership data by the deadline of 13 July 2020 or by the AT's visit to Poland. The pandemic will be relevant to this. The CRBO team's plan to address the gap is (a) to further publicise the registry and the legal requirements for its population and (b) to work with the NCH team and other authorities to identify and check legal persons whose data has not been provided.

691. There is no review of data when it is input in the CRBO. To date, entries on the register have been verified randomly, with data on 20 000 legal persons being verified to date. Of this number, some 1 000 (5%) had an element of inaccuracy, such as an incorrect NCR registration number, an incorrect tax identification number or a misspelling of a person's name. These are suggestive of error rather than abuse of legal persons. Data on the BOs were cross-referred by the CRBO team with the data in the NCR, the KAS's VAT register and the other aforementioned registers, except the NCH and the CEIDG. The internet and the CRBO's Bisnode database were also checked whenever a mismatch with the NCR was detected and prior to any decision to initiate coercive proceedings. By virtue of its accountability and reporting link to the KAS, the CRBO team has direct access to the KAS' databases. Where the CRBO team has a concern that a company is a fictitious company or does not appear to be undertaking commercial activity, a red flag is raised with the KAS for investigation. Importantly, verification of the data for each of the 20 000 legal

persons extended to cross-checking of all the individuals and other persons mentioned in the registered details of the legal person, meaning that persons linked to the company being verified (such as BOs of the company) were also checked across the CRBO team's database and with other registers maintained by public authorities. This extensive approach to verification of the selected company is welcomed by the AT.

692. The CRBO team intends to utilise the same approach as that mentioned in the paragraph above for a sample of at least 6 000 companies each month.

693. Within three days of detecting an inaccuracy, the CRBO team wrote to the representative of the relevant legal person requiring it to update the information on the register or, where the tax information number (TIN) was not correct, to provide the correct TIN – the representative can update all of the information on the register itself except the TIN. By 15 May 2021, 475 legal persons had been requested to provide updates.

694. Changes to registered BO information must be made within seven days of the change. To date, 39 000 changes have been made as a result of updates to registered information. In addition, 44 000 revisions have been made by the representatives of legal persons correcting mistakes they had made in registering information. These later revisions indicate the general wish to ensure registered information is correct as understanding increases; this can be seen not only in the overall level of corrections but also the in pattern of corrections, with a steady decline each month since the register was established. The number is now low, indicating better quality information at the time of the visit to Poland by the AT.

695. Changes to registered data are visible to the CRBO team when looking at an entry (although there is no specific notification to the team that a change has been made). The register is checked in general to see if changes might have been made, and, more specifically, the adequacy of notification of changes in relation to a registered person is reviewed when fines are being considered. However, this process cannot be systematic, and there would be merit in establishing a notification system.

696. GIFI has provided input to the CRBO where it has had a concern in relation to a legal person. This results in a cross-check by the CRBO with the aforementioned registers (paragraph 661) and seeks to ascertain whether the company and the specified registered address exist, together with, for example, whether there has been a tax identification number and its status, the VAT status, whether the legal person has property, whether it makes purchases or sales, and whether it has any arrears or bailiff seizures. This has led to the issue of coercive proceedings requiring information to be corrected within three days and, in three cases, to financial penalties (amounting to PLN 32 000 / €7 000). Where correspondence is returned by the post office as having no deliverable address (either as a result of activity arising from input by GIFI or from other activity), the CRBO advises the KAS and the NCR team and requests that their processes, e.g. removal of the TIN and strike off from the various registers they administer are put in train. In addition, the KAS visits the address specified for the legal person and checks the business partners and transactions of the legal person and provides feedback to the CRBO team.

### ***Obligated Institutions***

697. CDD information held by banks and other obligated institutions is key in ensuring high quality basic and beneficial ownership within Poland. Since 2018, all Polish legal persons making or receiving payments arising from economic activity where the other party to the transaction is an entrepreneur and where the value of the transaction (regardless of the number of payments) is in excess of PLN 15 000 (€3 300) are required to have bank accounts. When added to the need

for legal persons to have a bank account for commercial and transactional purposes, including engagement with registries and other authorities like the KAS, as opposed to legal requirements for a bank account, almost all and possibly all legal persons are covered by a need to have a bank account at least at some point during their lives. Within this context, the KAS has noted that there have been examples of companies used in fraud schemes that established a bank account at the incorporation stage but gave up the bank account later (i.e. a bank account was still needed at the start of the company’s life). This means that the supervisory roles of the UKNF and GIFI are important – see IO.3 for additional information. The quality of beneficial ownership held is reviewed during onsite inspections by supervisory authorities. As part of this, the UKNF and GIFI check what data sources have been used by banks, whether these are reliable and whether verification of beneficial owners by banks is consistent with the risk exposure of the legal person.

698. The table below shows the pattern of onsite and offsite inspections (all of which cover beneficial ownership) by the UKNF for the 15 banks which the UKNF considers to be the highest risk. Most legal persons are customers of these banks; the table shows the number of customers who are legal persons for each bank. Prior to each inspection, the UKNF has obtained a copy of the information on all the bank’s customers (including beneficial ownership information for legal persons) from the NCH since 2020. This is used to inform the inspection, including the selection of customer files for legal persons that are sampled. In practice, the inspections check the information provided by the bank to the NCH for those customers and the extent to which the measures and processes leading to the provision of information to the NCH are consistent. Therefore, the inspections are also relevant to the checking of the wider information package provided to the NCH. The UKNF has found the beneficial ownership information at the NCH to be consistent with data held in banks and for the data held by banks to be consistent with the risk of the legal person. The same approach applies to sampled customer files vis a vis the information held on the NCR and the CRBO.

**Table 7.2. Pattern of onsite and offsite inspections by the UKNF to the highest risk banks (2017 –April 2021)**

	<b>Inspection (year)</b>	<b>Number of customers (legal persons)</b>
<b>Bank 1</b>	2017, 2019, 2020	484 060
<b>Bank 2</b>	2018, 2019, 2020	408 768
<b>Bank 3</b>	2017, 2020	255 243
<b>Bank 4</b>	2018, 2019, 2021	82 995
<b>Bank 5</b>	2017, 2019	56 967
<b>Bank 6</b>	2017, 2018, 2020	This bank does not exist anymore
<b>Bank 7</b>	2018, 2019, 2021	547 247
<b>Bank 8</b>	2018	540 630
<b>Bank 9</b>	2017, 2019	20 327
<b>Bank 10</b>	2017, 2018	263 564
<b>Bank 11</b>	2017, 2019	9 442
<b>Bank 12</b>	2018	1 336
<b>Bank 13</b>	2016, 2018, 2020	4 217
<b>Bank 14</b>	2016, 2018	186 758
<b>Bank 15</b>	2018, 2019	10 666

699. Also, the UKNF carried out 18 thematic onsite inspections during 2018, which included a focus on beneficial ownership. Twelve of these inspections were to banks. A dedicated methodology was developed and used for these inspections.

700. GIFI has subjected 11 banks to onsite inspection since the beginning of 2017; each inspection considered adequacy of beneficial ownership information.

701. Outreach, offsite supervisory engagement, inspection activities carried out by the UKNF and GIFI, and SAR reporting have shown that the approach taken by banks towards risk identification, assessment and mitigation; identification and verification of beneficial owners; EDD; and ongoing monitoring has changed positively over the last five years. Banks approaches to beneficial ownership, including recognition of control through forms other than ownership, has improved and is continuing to develop. The improvement mostly arises from better understanding of ML-related risks and, in consequence, more effective ways of mitigating these risks. The actions taken by banks to address beneficial ownership risks and the risks of misuse of companies include, inter alia:

- introducing automated API-based connections with companies providing access to information available in registers (open-public register and paid bases);
- ensuring access to web-based databases containing information on beneficial owners and ownership structures of customers;
- introducing more and more sophisticated AML/CFT IT systems in order to detect abnormal activity of the customers and to detect potentially suspicious transactions;
- the development and use of red flags and typologies;
- establishing more sophisticated compliance approaches to dealing with red flags and unusual transactions or other abnormal activity;
- producing more detailed and comprehensive business risk assessments related to risk exposure of obligated institutions, which are the most often based on the NRA and take into account the Guidelines on the risk assessment of the obliged institutions published by the UKNF in 2020;
- introducing more detailed internal AML/CFT procedures;
- more intensive training efforts by institutions.

702. These actions have led to an increase in the detection by banks of companies established to facilitate tax fraud and launder the proceeds, and a consequential increase in the filing of SARs by banks relating to fictitious companies and/or hidden controllers of companies not named as directors, shareholders and beneficial owners.

703. The UKNF provided the AT with information on AML/CFT breaches by the banking sector, which are currently under consideration for the imposition of potential penalties. Three of five banks in this position had issues relating to the verification of beneficial ownership. The issues relate to a very small number of accounts, and in any case, the number of breaches has reduced markedly since 2018. In addition, the UKNF's records indicate that the breaches are very small in nature.

704. While acknowledging that there is room for further development, the foregoing and the increase in the detail of such SARs also provides the UKNF and GIFI (from its positions as supervisory authority and FIU) with evidence that banks are successful in identifying potential misuse of companies and hidden controllers.

705. As specified in IO.4, the AT found a range of very positive aspects in relation to banks' approaches to beneficial ownership. The application of CDD and EDD and updating of CDD/EDD data are graduated depending on the rating assigned by risk scoring systems. Regarding

beneficial ownership, in particular, banks adopt measures to understand the structure of ownership and control of their customers and satisfy themselves that they have identified the BO(s). These measures include information provided by customers and checks of independent external sources, such as external databases or public registers (national and international), including the NCR and the CRBO. Nevertheless, there is some degree of reliance on customer declarations, and ascertaining the source of wealth is almost exclusively limited as an EDD measure to business relationships with PEPs. The combination of these two factors might contribute to the continuing risk of shell companies being used for VAT fraud (for which there is no apparent link to PEPs).

706. Termination of business relationships when unable to pursue CDD (including determining the BO in some cases) is a widespread practice among banks. Banks periodically review and update the BO information (the frequency varies depending on the risk from once a year for high-risk customers to five years for low risk and whenever there is an alert, including through internal audit function) of the whole customer portfolio to detect any changes in ownership and to ensure the ongoing validity and relevance of the data they hold.

707. The KAS makes a large number of queries to banks each year. The number has increased as a result of the increased and more complex analysis (described below), with some 10 000 to 11 000 in all (i.e. for both individuals and legal persons) estimated as having been made in 2020 and 7 800 being made from the beginning of 2021 to 21 May. The queries are wide-ranging in nature and include information relevant to asset blocking/freezes, the customer, the financial history of the account, the current balance, the identities of directors of legal persons, the identities of representatives of the customer and beneficial owners of legal persons. Information received is cross-checked with the KAS's records and, inter alia, the NCR, the NCH and the CRBO. The information and cross-checking of it are also relevant to whether there are hidden controllers of legal persons with bank accounts. The KAS has found bank information to be generally accurate.

708. Turning to the other key gatekeepers, there is significant use of notaries and lawyers by legal persons. The authorities estimate that some 50% of applications use a lawyer (subject to AML/CFT requirements). Most transactions after incorporation require a notarial deed. These gatekeepers perform CDD on their customers, including conducting background checks by utilising external sources (registers and lists). The UKNF and GIFI have noted that the improvements to AML/CFT measures described above for banks are, in a less sophisticated way, generally applicable to other obligated institutions, particularly but not only for FIs. Notaries, in particular, undertake a more developed approach to ascertaining beneficial ownership than was the case five years ago. Whenever company incorporation is involved, the measures are stricter than in relation to individuals, and BO identification and justification of the source of funds (but not the source of wealth) is pursued. In the particular case of notarial deeds, the physical presence of all parties involved in the notarial deed is always required; hence, there is no possibility for anonymous parties. The statements made in the notarial deed are based on information held in Polish public registers and lists (such as PEPs) and/or customer documents CDD by notaries and lawyers have benefit but, as with banks, overall, the approach to EDD does not match the sophistication of those wishing to abuse companies for criminal purposes.

709. A significant number of legal persons (and their basic and beneficial ownership) are subject to AML/CFT measures by more than one obligated institution.

## **KAS**

710. In light of its role, the KAS has a long history of analysing legal persons, directors, representatives of legal persons, shareholders and beneficial ownership. As part of the national initiative against fictitious companies, there was a step change in 2017, with steady further development since that time. The KAS undertakes sophisticated and multi-faceted analytical and investigative activity relevant to both combatting the misuse of legal persons and ensuring the adequacy, accuracy and currency of basic and beneficial ownership information in Poland. In addition to increasing staff resources, the KAS has implemented an IT analytical environment by using established and innovative analytical methods, including statistical and econometric modelling, machine learning and big data processing. A wide range of software tools, using an equally varied range of algorithms, is used. Some of the tools engage in permanent analysis of all data, while others are focused on specific data sets such as VAT transactions above a certain threshold or VAT transactions in specified sectors. These also harness information in registers to which the KAS has direct access, such as the NCR, the NCH and CRBO and the other registers mentioned above (in paragraph 661), amongst others. These systems also harness the legal requirement for bank accounts for economic transactions over PLN 15 000 (€3 300). Through its analysis and investigatory activities, the KAS cross-checks information provided, inter alia, in the CRBO. This includes control by means other than share ownership as the analysis and investigation also include searches for disguised links and control. All legal persons which criminal elements intend to use for tax fraud have a bank account at some stage (even if quite a few companies surrender the bank account soon after the company is established); the KAS will only pay VAT refunds to a bank account. The KAS is a lead authority for obtaining basic and beneficial ownership information and for verification of that information.

711. All legal persons registered for VAT have been subject to a “basic” analysis check by the KAS (271 829 legal persons being covered from the beginning of 2021 to May 2021). In practice, the check is a highly sophisticated search by artificial intelligence of all of the data of the legal person possessed by the KAS (e.g. including directors, representatives, shareholders, beneficial owners and the purpose of the company) and its links to the information on all the registers with which the KAS has direct access. This basic analysis check has been undertaken since 2018. Similar (if less comprehensive) types of analysis were applied before that year.

712. A large number of legal persons are subject to more intense analysis from a series of different perspectives using IT and staff. The analysis department of the KAS has some 100 staff, enabling it to devote focus to addressing risk. Within this department, there are separate sections that deal with cash flow analysis and bank information.

713. Since 2018, the KAS has used an automated risk scoring tool predicated on VAT fraud risk for legal persons with bank accounts (STIR). The tool commenced as a result of the establishment of the NCH and legislation requiring the NCR to score risk and directly supports the management and mitigation of risks of legal persons registering for VAT and of fictitious companies, but it also supports recognition, management and mitigation of risk with regard to other tax frauds. There is coordination of use of the tool throughout the KAS by the headquarters, with minor variables being fed into the system at the regional level individually by regional offices. The objective of the tool is to identify which legal persons should be considered by the KAS for more intense analysis from a VAT fraud perspective. The scoring comprises the automated allocation (using bespoke, sophisticated software) of a numerical score to the legal person based on five criteria specified in the tax legislation, namely economic risk; the geographic risk of jurisdictions with a high risk of tax fraud with which the legal person has links; the risk of the type of business; the nature of links between the legal person and persons with high fraud risk, and non-standard patterns and

behaviours. Information on entities associated with a legal person (including directors, known representatives, shareholders, and beneficial owners and persons known to be associated with a legal person) are important components of the scoring. NCR, NCH and CRBO information, amongst other sources, are taken into consideration within the scoring.

714. In addition, also in 2018, the KAS introduced two other risk scoring models for VAT taxpayers, one for persons at the time of registration (the SKORP-registration tool) and one for persons after registration (the SKORP tool). Each takes account of STIR, amongst other factors, including information provided by the applicant and other sources. The main objective of the two models is to provide KAS officers with quick and structured access to information and proper risk management of the VAT register and taxpayers. Both the SKORP-registration and SKORP tools involve IT assessment supported by manual assessment. Risk assessment by the SKORP tool is updated every two weeks.

715. There are three online levels of risk arising from the scoring process, namely low, increased and high. A significant number of legal persons has been risk rated, although only figures for all individuals and legal persons combined is available: 2018 - 3.41 million; 2019 - 3.42 million; 2020 - 2.95 million; 2021 up to the departure of the AT from Poland - 1.18 million. Legal persons (and individuals) scored as increased or high risk are subject to potentially greater likelihood of refusal of VAT registration and enhanced monitoring after registration.

716. High-risk legal persons are subject to comprehensive analysis by staff. This includes:

- checking that they have bank accounts and far-reaching analysis of patterns of payments and transactions in cash, electronic or digital form;
- the potential for misuse of the legal person and how the transaction and payment types and patterns tie in with the purpose of the legal person and the names, addresses and other information available on named directors, known representatives, shareholders and beneficial owners, as well as any other person who might be a controller;
- extending the analysis beyond the legal person, directors, known representatives, shareholders and beneficial owners to cover any other person to whom they are linked, and to any person to whom those additional analysis subjects are linked. Furthermore, the software used by the KAS enables the progressive analysis of all links, no matter how many links or how many chains there might be;
- scrutiny of whether the legal person or the directors, shareholders or beneficial owners might have formed groups of linked structures engaging in tax fraud or are otherwise linked.

717. Staff scrutiny also extends to use of various bespoke software tools which enable, for example, groups or other potentially linked legal persons to be identified and the patterns of cash and electronic transactions by legal persons to be intensively interrogated. This more comprehensive analysis means that the KAS is analysing and checking information it possesses; information possessed by the NCR, the NCH and the CRBO; information provided from the other registries mentioned above, as well as other registries both inside and outside Poland; information provided by banks; information provided by other authorities, including GIFI and the UKNF; and other external information such as websites.

718. The KAS has found the risk scoring to be very useful as it has enabled the authority to narrow down which legal persons should be subject to more comprehensive analysis without having to rely on manual checks alone, to close down fictitious companies and prevent and detect

VAT and other tax fraud. As part of this process, the overall number of cases subject to analysis and investigation activities has been reduced slightly in favour of a more intense and targeted approach so as to benefit from using the risk scoring model. The KAS sees this approach as demonstrating the effectiveness of the system.

719. Second, the KAS has developed red flags, typologies and other indicators of potential fraud and, as a separate exercise to use of the risk scoring tool described above, since 2018 has analysed all legal persons against these indicators. These indicators take account of the NRA. Where the profile of a legal person is consistent, or might be consistent, with one or more of these indicators, the legal person and those attached to it are subjected to the same comprehensive analysis as described above.

720. Third, since 2018, the KAS has analysed the directors, representatives of the legal person, shareholders and beneficial owners of legal persons after incorporation and registration in the NCR. The legal persons are subject to a separate risk scoring to that mentioned above using this data and the purpose of the company. Depending on the score, the legal person and those attached to it are subjected to the same comprehensive analysis as described above.

721. Informed by the results of the measures described above, the KAS analyses each legal person (and its directors, representatives, shareholders and beneficial owners) applying to be added to the VAT register. A substantial number is rejected as a result of the screening process, which process the KAS considers to be an important component in preventing misuse of legal persons. The rejections are public.

722. VAT transactions are scrutinised from various software and staff perspectives. Some 100 million invoices are analysed each month. Notifications are sent to taxpayers when there appears to be a discrepancy so as to provide an opportunity to correct mistakes (more than 480 000 notifications in 2018, some 270 000 in 2019, nearly 160 000 in 2020 and under 50 000 in the first four months of 2021). The resulting corrections enable the KAS to concentrate on invoices with the greatest risk to the authority, for example identifying over 51 000 entities in 2020 seeking to deduct VAT several times on the same invoice (involving over 132 000 invoices in total and a VAT amount of PLN 128 million / €28.16 million). Use of the software has meant that PLN 1.9 billion (€0.42 billion), which would almost certainly have been successfully defrauded, has been secured by the KAS.

723. Separately, individuals and legal persons are analysed with regard to the amount of VAT to be refunded or offset in relation to future transactions. In addition, a separate in-depth analysis targeting VAT irregularities was carried out in 2019.

724. The following number of individuals and legal persons have been analysed using VAT-specific software: 2017 – 1.22 million; 2018 – 1.21 million; 2019 – 1.23 million; 2020 – 1.28 million; 2021 up to when the AT left Poland – 1.09 million. While the foregoing includes individuals as well as legal persons, the combined figures are indicative of the commitment and the scale of activities of the KAS. In addition, focus on individuals is relevant to legal persons as some individuals registering for VAT are also involved for legal persons, and their data can be analysed and linked to legal persons.

725. The AT considers the use of software and risk scoring (which is embodied in a range of the software, not only the tool mentioned above), together with comprehensive analysis by staff, considering legal persons from several perspectives, to be a very positive addition to Poland's armoury against fictitious companies and other types of misuse of legal persons. For example, it means that even where the risk scoring tool mentioned above might have led to a medium or low

risk rating for a legal person, potential abuse by those legal persons can still be identified. In all, 83 514 legal persons were subject to comprehensive analysis from the beginning of 2018 to the end of April 2021. The KAS considers that it has, and has access to, significant data which can be mined and that it has the appropriate tools to use the data properly by cross-checking it and detect and prevent misuse of legal persons, including in relation to companies where a bank account has been surrendered by criminals. It has detected examples of such companies.

726. Depending on the results of the various analyses, a case is passed to the control supervision department for investigation. This department has some 100 staff. The main difference between the analysis and control supervision departments is that the latter undertakes onsite inspections.

727. The tables below show VAT inspections undertaken by the control supervision department. The total number of inspections has decreased. This is attributable to entities subject to inspections being selected more precisely and verification activities being applied to a greater extent and in a more targeted way. The pandemic has also had an effect. The effectiveness of inspections has increased.

**Table 7.3. Number of VAT inspections undertaken by the control supervision department (2017-21st of May 2021)**

<b>VAT inspections undertaken by the control supervision department (tax offices, customs and tax control offices)</b>					
	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>Up to 21 May 2021</b>
Findings (million PLN)	18 081	14 759	11 475	8 467	2 379
Total number of inspections	18 781	14 036	11 427	9 289	3 700
Number of inspections finding irregularities	15 907	12 336	10 486	8 835	3 511
Number of inspections finding irregularities/total number of inspections	83%	87%	89.5%	94.5%	94.1%

728. The table below provides information on bank accounts of legal persons blocked by the KAS. The substantial increase over time is attributable to the benefits of using risk scoring and the specific focus this permits.

**Table 7.4. Number of legal persons with assets blocked/frozen by the KAS (2018-21st of May 2021)**

	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>Up to 21 May 2021</b>
<b>Number of qualified</b>	23	120	196	95

<b>entities blocked</b>				
<b>Number of legal persons</b>	23	113	175	91
<b>Number of bank accounts of qualified entities blocked for up to 72 hours</b>	41	565	1020	519
<b>Number of bank accounts of legal persons</b>	41	550	901	490
<b>Number of bank accounts of qualified entities in which the lockout period was extended for a fixed period of time not exceeding 3 months</b>	41	561	1020	519
<b>Number of bank accounts of legal persons</b>	41	546	901	490
<b>Total amount of blocked cash</b>	PLN 10.2 million (€2.24 million)	PLN 69.6 million (€15.37 million)	PLN 96.1 million (€21.14 million)	PLN 26.1 million (€5.74 million)
<b>Estimated depletions</b>	PLN 132.1 million (€29.06 million)	PLN 591.6 million (€130.15 million)	PLN 660.9 million (€145.39 million)	PLN 220.8 million (€48.57 million)

729. The table below shows the number of fictitious invoices uncovered by the KAS (for individuals and legal persons) as a result of its analytical and investigative activities. Risk scoring and the use of other software and algorithms have had a positive effect on reducing the number of fictitious invoices.

**Table 7.5. Fictitious invoices uncovered by the KAS (2016-21st of May 2021)**

	2016	2017	2018	2019	2020	21 <sup>st</sup> of May 2021
<b>Number of invoices</b>	421 330	255 827	270 769	229 030	153 352	66 417
<b>Gross invoice amount (in billion PLN)</b>	103.85	56.86	53.92	37.23	22.2	4.8

730. The case study below uses a cross-jurisdictional scheme to illustrate the KAS's wider approach to addressing misuse of legal persons.

#### CASE BOX 5.1.

Following risk scoring, analysis and investigation, the KAS unearthed a potential tax fraud involving a UK company, a subsidiary of the company in the Slovak Republic and seemingly unrelated individuals and companies in Poland, but who were nevertheless part of the fraud. Information was sought from the tax administration in the UK. Moreover, a related legal person entity with the same name as the UK company was registered in Poland at the time the KAS's tax audit was being carried out. This legal person appeared to be part of the tax fraud.

The UK company had been established for the purpose of holding a brand but did not conduct any business activities in the UK and was not registered there for VAT purposes. The company did not establish a subsidiary or branch in Poland, had not registered for VAT purposes in Poland, had not been assigned a Polish VAT tax identification number and had not submitted any VAT returns to the KAS.

The UK tax administration provided information to the KAS, including that the UK company had a website that was not active; and that the company had no trading or advertising, no suppliers or customers, and no bank account and had made no cash payments. It was also apparent that a director of the UK company made daily business decisions from Slovakia but did not store goods there. The UK company's activity was purported to be the online sale of electronics (mainly smartphones) both to private consumers and entrepreneurs. All of this indicated that the company might be using bank accounts in Poland for tax fraud or activities aimed at tax fraud, based on not declaring the turnover from sales made in the territory of the country from which the VAT settlement obligation arose.

Considering the totality of the case, there was a high probability that the UK company was selling commercial electronic goods by mail order to which the Polish legislation on tax on goods and services applied. The UK company was supplied with cash from sales during the period from 1 January 2019 to 31 December 2019 for the total amount of PLN 142 219 076 (€31 288 196); the Head of the KAS calculated VAT at the rate of 23% (PLN 25 882 099 / €5 694 061).

The case is under investigation under the supervision of the Prosecutor of the Regional Prosecutor's Office with co-operation with the KAS and the ISA. The investigation is being conducted against a Polish citizen and a citizen of the Slovak Republic, who are suspected of acting jointly and in agreement with a third party for the period from 1 January 2017 to 8 January 2020 to avoid taxation. This exposed the State Treasury to a reduction in public-law receivables of approximately PLN 40 000 000 (about €8 815 000). Related to this, from January 2019 to January 2020, a Polish citizen also transferred funds of at least PLN 27 million (about €6 million) related to the commission of prohibited acts to lower the tax on goods and services in order to prevent the determination of their criminal origin.

Pre-trial detention was imposed on a Polish citizen in 2020, after which this measure was changed to property bail - PLN 200 000 (about €44 000) was paid. The case is ongoing.

731. The KAS has been effective in addressing misuse of companies. The KAS has become significantly more sophisticated and assertive during the period covered by the table and, against this background and the national initiative to address fictitious companies, the overall pattern of a decreasing level of fictitious invoices uncovered and the more significant fall in the value of fictitious invoices uncovered demonstrates that the KAS is effective in combating misuse of companies. The significant number of companies struck off the VAT register about which the KAS has had concerns also addresses misuse and cleansing of beneficial ownership data held in Poland. In addition, the statistical gap in VAT receipts in national statistics has reduced significantly, and VAT receipts have increased significantly, also indicating success in addressing the problems of fictitious companies, straw men, tax fraud and laundering the proceeds of tax fraud.

### ***GIFI***

732. GIFI has interrogated information it holds on legal persons in several ways. This information includes reference to legal persons in SARs, the data it receives on transactions and all other financial intelligence held. All cases of financial intelligence that include a legal person or a person who is a director, named representative, shareholder or beneficial owner of a legal person are analysed by staff. This analysis uses various factors to score each case, which leads to cases that are subject to more intense analysis. Scoring factors include the number of companies to which a director, named representative, shareholder or beneficial owner is linked; the jurisdiction of residence of each beneficial owner (using an internally generated list which divides jurisdictions into risk categories); and the profile of directors, named representatives, shareholders and beneficial owners within the overall financial intelligence held by GIFI.

733. GIFI has direct access to the NCR and the CRBO and has matched its records with the two registers, taking account of information on the CRBO and why information might not yet be on the CRBO. The approach appears to have been comprehensive. As at the time of the AT's visit to Poland, GIFI had compared its data with some six thousand of the legal persons with data on the CRBO, thus providing external analysis of the quality of that information. In addition, GIFI began a project in 2020 in which it analysed legal persons that have not provided information to the CRBO against transactional data within a specific period to ascertain which companies were active in that period. The number and value of transactions reported to GIFI were scored, and, in the most active cases, further analysis included comparison with SAR data provided by obligated institutions. As of April 2021, some five thousand of these legal persons that had not yet reported to the CRBO were subject to analysis by scoring and, following the scoring, have begun a process of subjecting some legal persons to deeper analysis, including their directors, shareholders, named representatives and beneficial owners. At all levels of analysis, GIFI is considering whether there are links between companies and hidden/disguised control, and it has found examples of such companies. Feedback has been provided to the CRBO and the supervisory department of GIFI, as well as informing FIU activity. The project is ongoing.

734. GIFI has also passed cases to the KAS for that body's analysis (as described above) and investigation for potential fraud. Around 2 000 cases have been passed to the KAS since 2017.

735. In total, GIFI has subjected 17 186 legal persons and their directors, named representatives, shareholders and beneficial owners to analysis since the beginning of 2017. This figure is larger than the two figures above if added together as it includes all legal persons subject to analysis, not only those which were on the CRBO and those not on the CRBO but subject to transactional analysis.

#### ***7.2.4. Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons/arrangements***

736. The NCR and the CRBO are public and are used by the authorities. The CRBO team also holds non-public information.

737. Discussions with public authorities and the private sector while in Poland have led the AT to conclude that 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. The AT is also mindful that “straw men” are used by criminals for fictitious companies. Therefore, the nature of the main issues in relation to whether beneficial ownership is adequate, accurate and current is two-fold, namely the “straw man” through ownership and hidden actors through control. There may well also be inaccurate data for other reasons.

738. The PPO obtains information from the NCR each time it deals with a case involving a company (i.e. in most ML cases). It considers the information from the NCR to be accurate, although not always fully up-to-date (noting that fictitious companies do not update their data in the register and that such companies and “straw men” come together as a package).

739. The CRBO is widely considered by the authorities to be useful, notwithstanding its recent establishment, and as needing time to ensure its data is high quality. GIFI has requested information from the CRBO team to verify data held by GIFI and found it to be correct. GIFI considers the information in the CRBO to be accurate.

740. The Border Guard, the ISA, the CBA and the PCBI have direct access to a significant number of registers/databases, obtain information from registers and databases to which they do not have direct access and also obtain information through use of their formal powers. They routinely access and use NCR and CRBO data in their operational activity, and there have not been any issues of access.

741. No concerns have been expressed to GIFI or the criminal justice authorities in Poland by their foreign counterparts about the quality of basic or beneficial ownership information provided to them which has been obtained from the NCR or CRBO or which has been obtained from another source, for which there is consistency between the NCR/CRBO data and that other source.

#### ***7.2.5. Effectiveness, proportionality and dissuasiveness of sanctions***

742. Following the 2017 amendment to the VAT legislation described above, from January 2017 to August 2020, more than 415 000 entities (individuals and legal persons) have been struck off the VAT register by the KAS. Both refusals to permit registration, as well as removal from the register once registered, are considered as strike offs by the KAS. The (rounded) numbers are as follows: 2017 – 110 000; 2018 – 118 000; 2019 – 92 000; 2020 – 123 000; and the first four months of 2021 – 20 348. The fact of former registration and the strike off is apparent to all persons viewing the register. In addition to companies involved with VAT fraud, a significant number of individuals engaged with such companies (e.g. strawmen) have been struck off the VAT register; the public nature of this militates against the use of these individuals again for criminal schemes. While the KAS does not have a procedure on sanctions, there are legal criteria for removal of a business from the VAT register, and the KAS has been effective in its strike off processes. In addition, information provided by the KAS to the NCR team has also led to

the strike off of numerous companies from the NCR by the Courts. Information provided by GIFI has also led to strike offs.

743. In addition, when the KAS blocks a bank account and when it extends the block for a period of up to three months, it notifies the PPO. In addition, the KAS should notify the PPO when it suspects a specific person has committed tax fraud. See IO.7 for further information.

744. The NCR team operates under the NCR Act and Code of Civil Procedure and does not have a procedure for the imposition of penalties. Notwithstanding this, there is a relatively simple process in place. Any failure to provide information leads to coercive proceedings, *i.e.* a letter specifying a requirement to provide the relevant information within a specified period or pay a fine. Fines are also not paid in practice if a company is no longer operational or can no longer be contacted at its registered office address. The relevant Court rather than the NCR team imposes penalties. Where the legal person continues not to provide information, it is struck off by the relevant Court. Not all strike offs will be coercive in practice, *i.e.*, a sanction, as opposed to an administrative step, desired or needed by the owners of the legal person.

745. With regard to failure to provide financial statements, the company and its management board is advised that fines of up to PLN 10 000 (€2 200) are applicable unless the financial statements are provided. Each member of the management board is subject to this level of fine. In addition, the coercive proceedings and the fines are publicly available on the record of the legal person. It is rare for companies not to provide the statements on the first occasion in which the NCR team follows up failure to provide them. The normal process where financial statements are not provided is then for the relevant Court to strike off the company, although there are rare occasions when a non-filing has led to a requirement to pay a larger fine unless financial statements are provided within a revised deadline – this is when a company still appears to be active. Return of the Court’s letter by the post office is strongly indicative that a company is no longer operating. It takes approximately six months from the point at which the financial statements should have been provided for strike off to take place; the AT considers there is scope to speed up this process.

746. As indicated above, the following number of coercive proceedings (which can be initiated by the NCR team) have been undertaken in relation to incorrect information: 2017 – 98 109; 2018 – 123 103; 2019 – 153 760; 2020 – 133 358 and up until March 2021- 44 182. While a fine is indicated in each case as potentially payable if information is not provided, the aim is to obtain the information. The NCR team does not keep statistics as to how many of the 508 330 coercive proceedings from 2017 to 2020 resulted in fines or strike offs. Examples were provided of first fines of PLN 1 000 (€220) and 10 000 (€2 200), a second fine of PLN 10 000 (€2 200) and a third fine of PLN 20 000 (€4 400). It is very rare for a second fine (and even rarer for a third fine) to be imposed as the initial coercive proceeding is generally successful unless the registered address no longer exists or is no longer functioning as such.

747. The Court has coercively struck off the following number of companies for each year since 2017: 2017 – 3 329; 2018 – 4 882; 2019 – 6 176; 2020 – 5 894. Strike offs arise from two triggers, namely failure to provide financial statements and information received from another authority, particularly the KAS (and, to a much smaller extent, GIFI) that the company should be struck off. With regard to the former, a substantial number are likely to be fictitious companies, while input from the GIFI has a criminality-based concern attached to it. Strike off by the Court is, therefore, a key element in removing fictitious companies and other companies which have been misused from the system.

748. The NCR team has made a number of referrals to the Criminal Investigation Department of the Police for potential prosecution. One in 2019 involved the forced sale of a company, and the end result was strike off from the NCR by the Court. More generally, failure by a legal person to provide financial statements leads to a referral; proceedings are discontinued by the NCR team when it receives the financial statements. As indicated above, continuing failure leads to strike off. In a small number of cases, the PPO has requested strike off. The NCR team sees consideration by the Police and PPO as a separate and parallel process to its own strike off processes. However, there would seem to be an issue as to how any case might proceed when a company is struck off and, in any case, the NCR team does not seek or receive information from the Police or PPO on outcomes of cases.

749. Legislation enabling the CRBO team to impose administrative penalties for non-registration and for failure to update information came into force immediately before the AT's visit to Poland. Five hundred and seventy-five legal persons have been notified by the CRBO team that they must pay a fine unless they provide the required information for inclusion on the register within seven days (of which 286 had filed information before 21 May). As of that date, it was the team's intention to fine the legal persons that had not filed information (as opposed to allowing another opportunity to file information without a fine). This demonstrates commitment by the team, although the visit by the AT was so close to the issue of the notifications that legal entities had not yet been issued with a notification requiring payment of the fine, and it is too early to assess the dissuasiveness of the sanctions framework. In this regard, the AT notes that the very large majority of legal persons that have not yet reported information to CRBO had not yet been subject to a penalty (although the CRBO team intends to use its powers of sanction against such legal persons). The CRBO team operates under a Code of Administrative Procedure and an organisational regulation and has issued templates for use during proceedings; it also uses an analysis card for completion before initiating proceedings for fines. The CRBO team considers that these documents, together with internal documents on authority and scope of tasks, combine to form a procedure for sanctions; however, the AT considers that a unified policy or procedure would have merit.

750. In addition, as a result of information provided by GIFI to the CRBO, the latter's checks and subsequent notifications to KAS and the NCR team resulted in 83 legal persons being deleted from the VAT register by the KAS and 45 legal persons being removed from the NCR by the Courts.

751. See IO.3 for sanctions in relation to obligated institutions.

### ***Overall conclusions on IO.5***

752. Basic and BO information is publicly available in Poland. 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". Positive measures in the system have been addressing this risk with success; there is some scope for further development of the system. The NCR team undertakes wide-ranging checks both at the application stage (which has led to rejection of potentially fictitious companies) and after a company is registered; there is scope to improve the approach to fines. Legal persons registered at the NCR after 13 October 2019 were required to insert BO information on the CRBO within one week of registration. While the register is not yet complete, the CRBO has been proactively checking its database on a sample basis. Other sources of BO information include the obligated institutions, the NCH and the KAS. Virtually all legal persons have bank accounts. The KAS has rejected applications for VAT registration and struck off a significant number of companies from the VAT register (which has been successful in

reducing the effect of fictitious companies), and the Courts have fined and struck off legal persons. However, there is not a “whole of government” approach. All authorities met have an important role in relation to IO.5. In addition, obligated institutions and the VAT register are important, and the AT attaches significant weight to the activities of the UKNF and the KAS.

**753. Poland is rated as having a Substantial level of effectiveness for IO.5.**

## 8. INTERNATIONAL CO-OPERATION

### 8.1. Key Findings and Recommended Actions

#### ***Key Findings***

#### ***Immediate Outcome 2***

- a) Poland has a comprehensive legal framework to provide and request extradition and mutual legal assistance (MLA) in criminal matters, although only limited criteria and no guidelines exist with regard to the handling and prioritisation of the MLA requests. The EU legal instruments, as well as the existing bilateral agreements, provide for a more simplified and direct co-operation mechanism between the counterpart authorities. The majority of incoming and outgoing requests concern other EU Member States. When it comes to co-operation with some non-EU jurisdictions, especially those bordering Poland, the level of co-operation is less constructive, and this raises concern because of the ML/TF risks associated with these jurisdictions.
- b) The management and monitoring of the quality and timeliness of the execution of foreign MLA requests are fragmented, and no centralised case management system exists. The timeliness in relation to outgoing MLA requests might be affected by the restriction imposed on the local prosecutors' offices to communicate directly with the authorities of other EU Member States. It appears that the current management system has an impact on the effectiveness of the international assistance provided and sought, as also reflected in the feedback provided by other jurisdictions (difficulties when the requested actions regarding different Polish regions; inflexible approach regarding the requirements for providing assistance; not comprehensive enough outgoing requests). The timeliness of the provided assistance is difficult to assess as the available data indicates only the minimum and maximum time for the execution of the requests (the execution varies from 20 to 923 days for MLA and from 11 to 736 days for extradition).
- c) The lack of comprehensive statistics on MLA requests (incoming and outgoing) and other forms of international co-operation, which would include a breakdown by jurisdiction, prevents the Polish authorities to demonstrate that MLA is used constructively in order to address the specific ML/TF threats of international nature identified by the NRA and to assess the effective follow up of other forms of international co-operation.
- d) The GIFI and LEAs proactively exchange information with their foreign counterparts and demonstrated the ability to establish Joint Investigative Teams. The feedback received from the international community illustrates that both, the GIFI and LEAs, provide timely and good quality assistance to their foreign counterparts. The good quality of the assistance provided by the GIFI was especially highlighted. The CBA international co-operation outside the

framework of an agreement is under the condition of prior consent given by the Prime minister, which may impact its effectiveness/constructiveness, especially in relation to urgent cases.

- e) There is no systematic harvesting of incoming MLA requests by competent authorities with the aim of detecting potential domestic ML suspicions or TF cases related to these.
- f) The supervisory authorities (other than the GIFI) regularly exchange information with their foreign counterparts, but not for AML/CFT purposes. For this, they may rely on the GIFI, which has the power to exchange information on behalf of other authorities. Nevertheless, during the assessed period, this mechanism was not applied in practice for outgoing requests.
- g) 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. The AT has been presented with several examples in which the provided assistance, which included information on the BO, received positive feedback.

### ***Recommended Actions***

#### ***Immediate Outcome 2***

- a) Competent authorities (Ministry of Justice and the Office of the National Prosecutor) should develop mechanisms (including a case management system) and issue guidelines for the prioritisation and monitoring of the implementation of requests for legal assistance and extradition, with the aim of improving both the timeliness and quality of these.
- b) Accurate and reliable statistics should be systematically kept on requests for legal assistance and extradition (comprising those made through direct contact). These should provide indications on the number of requests processed, granted and/or refused, and include, among other things, the imposition of freezing and securing assets, which allows tracking the value of assets, and information on the breakdown of jurisdictions involved, as well as other relevant criteria as to the relevant risks and type of crime, etc.
- c) Ensure accurate and detailed statistics on the information exchanged by the LEAs.
- d) In relation to MLA assistance with EU countries, Poland should ensure that the outgoing MLAs can be sent directly by all levels of the prosecution, which are responsible for investigating predicate offences and ML.
- e) A more proactive approach is recommended in assessing the information received from foreign prosecutors or law enforcement agencies so as not to miss the signs of ML/TF activity within the competence of the Polish criminal justice system.
- f) Supervisory international co-operation should be regularly extended beyond prudential issues, including through the use of diagonal co-operation via the

GIFI.

- g) The Polish authorities should reconsider the requirement for CBA and ISA to cooperate with foreign partners only after prior approval of the Prime minister or clarify the existing mechanism to ensure that it does not prevent the co-operation in urgent matters outside the framework of an international agreement.

754. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40 and elements of R.9, 15, 24, 25 and 32.

## **8.2. Immediate Outcome 2 (International Co-operation)**

755. International co-operation is an important 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. Most of the co-operation, including on ML, is undertaken with other EU countries.

### ***8.2.1. Providing constructive and timely MLA and extradition***

756. Poland has a broadly comprehensive framework for international co-operation (described in detail in the TCA), complemented by the widely used EU legal instruments and the concluded bilateral and multilateral agreements, which provide a simpler and more effective mechanism of direct co-operation between countries. The provisions on MLA enshrined in the CPC enable courts and public prosecutors to provide legal assistance upon a request of foreign competent authorities in all types of cases, including ML and TF.

757. The process of executing MLA requests and extradition involves one or more authorities, be it the Ministry of Justice (MJ) who receives and transfers them to the competent body or the Prosecution Office who assigns another authority to assist. In case of the existence of an MLA treaty or other agreement, mutual legal assistance can be rendered directly by the Prosecution Office or a competent Court. In other cases, the MoJ accepts the request and directs it to the competent court or Prosecution Office.

758. Apart from regular channels of MLA, Poland uses the EU channels, such as Eurojust and the European Judicial Network in Criminal Matters (EJN), which facilitate the international co-operation within the EU.

759. As described under the TCA (R. 37), 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 direct co-operation between the authorities applies.

760. At the pre-trial stage of criminal proceedings, the 46 district Prosecutor's Offices provide assistance to MLA requests. In case of co-operation with EU countries, there is direct co-operation. When dealing with MLA requests from non-EU countries (in the absence of a specific bilateral agreement), the international co-operation department of the Public Prosecutor's Office appoints one of the 358 Regional Prosecutor's Offices.

761. From discussions conducted with the authorities onsite, it is apparent that co-operation is generally considered more effective and intensive with other EU countries and to a lesser extent to some non-EU jurisdictions, which raises concerns in the context of the ML threats and risks posed by those as mentioned in the NRA<sup>66</sup>. Regarding the non-EU countries, with some, co-operation is perceived to be more effective (Ukraine), while with others, this is an area for improvement (Belarus). The existence of a bilateral agreement with such countries positively impacts mutual assistance, e.g. the one with Ukraine, which provides for direct co-operation. The memorandum with Belarus on direct co-operation was suspended in 2011. As explained by the Polish authorities, this was done with respect to prosecution offices in order to ensure closer monitoring of the co-operation at the central level. Criminal courts can still cooperate directly based on an Agreement of 2009<sup>67</sup>.

762. In the previous 4th round MER, Poland was recommended to keep statistics on MLA (provided and sought). The Polish authorities have not yet fully and effectively implemented this recommendation, as the existing mechanism in place for keeping the relevant statistics is still insufficient. The MoJ only keeps data on the incoming/ outgoing requests, cumulatively, with non-EU countries (when acting as the central authority for international co-operation). In order to have a complete picture of international judicial co-operation, statistics should be collected individually from each common court and regional prosecutor's office, but this is not carried out systematically and, as explained onsite, was done on an ad hoc basis for the purpose of the present assessment (see Table 8.1). Additional explanations provided by the authorities at later stages of the evaluation implied that the data presented in the Table 8.1 would comprise only the incoming requests processed through the MoJ and not those subject to direct co-operation, which constitute a large portion of the total number.

**Table 8.1 Incoming MLA and extradition requests**

	All	ML	TF	Extradition
2014	71	54	0	0
2015	101	75	0	2
2016	42	36	0	7
2017	56	36	0	0
2018	64	47	3	3
2019	153	117	5	1
2020	393	2	0	60
Total	974	367	8	73

763. The AT remains unconvinced that the numbers, particularly those related to the assistance provided on predicate offences (incoming and outgoing requests), are accurate. The total number of incoming requests on ML is 367, constituting almost half of the total number of MLA requests, which appears unrealistic, especially when comparing to MLA statistics in other jurisdictions, and to the ratio between domestic cases of predicate offences (i.e., fraud, VAT, drug-related, smuggling etc.) many of which have international elements, with the number of domestic

<sup>66</sup> E.g. drug trafficking, human trafficking, smuggling, illegal immigration, cross-border cash.

<sup>67</sup> The Agreement between the MoJ of the Republic of Poland and the MoJ of the Republic of Belarus, the Supreme Court of the Republic of Belarus and the Supreme Commercial Court of the Republic of Belarus Economic Court of the Republic of Belarus on direct communication between courts in the field of rendering legal assistance of 13 February 2009.

ML cases. The data of 2020 support the unreliability of the statistics, indicating 393 MLA requests (which constitute about 40% of the total number of requests received during 2014 – 2020), of which the MLA on ML cases are negligible number (2). All this is indicative of the lack of systematic and accurate data collection of MLA by the Polish authorities.

764. The statistics provided by the Polish authorities on incoming and outgoing MLA requests do not include a breakdown by jurisdiction and, therefore, it cannot be demonstrated that MLA is used constructively to address specific ML/TF threats of international nature mentioned in the NRA.

765. The authorities stated (with no specific statistics) that the majority of incoming (and outgoing) requests relate to other EU Member States, so the importance of mechanisms such as the European Investigation Order (EIO) and the European Arrest Warrant (EAW) is essential. The volume of incoming requests varies from year to year, decreasing from 101 to 42 in 2016 and then increasing back to 153 in 2019. According to the authorities, most of the requests from other EU member states are submitted by Germany, Latvia, Lithuania, Estonia, Italy and Spain.

766. The scope of the requested legal assistance acts was outlined by the authorities as traditional investigative acts, namely hearing of witnesses, provision of documents (including bank documents) and service of court documents. As regards the requested actions specifically in connection with ML investigations, the authorities do not see any specificity compared to the requests related to predicate offences.

767. Although, according to the CPC, dual criminality may be a reason to deny MLA and extradition, it appears that it does not negatively affect the provision of legal assistance to foreign counterparts. According to the information provided by the Polish authorities, there are only a few refusal cases due to formal deficiencies in the application, missing information, or due to the political nature of the offence.<sup>68</sup> Nevertheless, the concerns regarding the reliability of the data remain, as the relevant statistics refer only to ML offence.

768. Timely and adequate MLA and extradition responses (actions) are possible according to the existing legal framework and, in most cases, appear to be implemented in practice. However, there are cases of serious delays in execution without specific objective reasons (execution varies from 23 to 923 days for MLA and 11 to 360 days for extradition – see Table 8.2).

**Table 8.2 Time of execution of incoming MLA and extradition requests**

	MLA	Extradition <sup>69</sup>
	Min/Max days <sup>70</sup>	Min/Max days
2014	30/120	N/A
2015	23/923	11/360
2016	28/345	36/200
2017	23/355	N/A
2018	25/300	270
2019	26/212	19
2020	N/A	N/A

<sup>68</sup> Refusals: 2014 – 2; 2015 – 1; 2016 – 3; 2017 – 1; 2018 – 2; 2019 – 1.

<sup>69</sup> The data refers only to ML cases.

<sup>70</sup> No information was provided on the average time for execution of MLA and extraditions requests, thus the data on the minimum and maximum days for execution are indicated.

769. The average period for execution of foreign requests from 2014 to 2019 could not be indicated even approximately, and conclusions can be made only in general terms. Apparently, some of the ML requests were answered by the Polish authorities in less than a month, while others took almost a year. During the onsite, the AT was assured that, in most cases, the requested actions are processed within 2-5 months. Nevertheless, the AT is of the opinion that the lack of such data needs to be addressed as a matter of high priority by the country, as the current figures do not demonstrate that Poland provides constructive and timely international assistance.

770. The time of execution depends on the complexity of the case or whether the request is coming from an EU country (with shorter execution time) or on the number of the requested activities, or whether a court decision is needed. According to the authorities, only objective reasons can justify a longer period of execution - difficulties in obtaining documentary evidence, finding the witness, technical deficiencies on the part of the applicant.

771. In practice, MLA requests are prioritised if urgency is explicitly stated by the requesting party or if urgency is justified by any circumstances, such as in cases where the person is prosecuted in custody or if it results from the request that its execution does not bear any delay, and fast action is needed (*e.g.* taking action until the date of a scheduled court hearing, etc.). The requests for obtaining and notifying data on telecommunications operations also have priority due to a possible timeout - data retention restriction. However, there are no statistics to demonstrate this, and the prioritisation is left to the individual discretion of the prosecutor in charge of the execution. There is no written criteria or system in which requests related to ML/TF crimes and/or deprivation of proceeds of crime can automatically be given priority or that allow monitoring the responses. When such guidelines and criteria are drafted, consideration should be given to the classification "urgent" by the requesting country, though this, in itself, should not be considered enough.

772. The execution of international requests is supervised by the MoJ or the head of the prosecutor's office (depending on whether legal assistance is sought through the MoJ or direct contact). In terms of requests from non-EU countries, MoJ monitors their execution by asking for reports on the stage of execution from the prosecutorial office every three months. In case of direct communication – the court is self-controlling, and the prosecutor is monitored by the head of the regional office. When actions in several regions are needed by the EIO, the MoJ monitors the process in practice, though no such obligation exists. The monitoring process includes entering the request and additional information into the calendar and checking the calendar regularly (by an appointed person). The AT is concerned that the described method cannot guarantee an accurate and timely execution of MLA and extradition.

773. The feedback from the international community indicates positive co-operation in general, although several countries have indicated that the process is not always effective and that the Polish authorities are not always flexible and are rather strict in their requirements when providing assistance. Other issues regarding the timeliness and the constructiveness of the provided assistance include infrequent updates, with insufficient details, and difficulties when the requested actions (gathering of evidence) should take place in different Polish regions.

774. The Polish prosecutors initiated 13 domestic ML investigations on the basis of MLA requests, with eight of them resulting in charges (in 2017) and two ending up in convictions (in 2017). The modest number is explained by the prosecutors with objective obstacles as the activity described in the request does not meet the features of ML, the perpetrator has not been identified,

or the requesting authority explicitly required its consent to be given if any of the information should be disclosed to third parties.

775. With regard to TF, Poland had received five MLA requests in 2019 (three from Ukraine, two EIO from UK), and three in 2018 (from Ukraine). The requested actions included: establishing the actual seat of 19 Polish companies, the credentials of their owners, founders, CEOs, accountants and other employees; examining witnesses in the manner required by the MLA; collecting physical evidence (digital copies of content recorded on electronic devices) and documents. The type of actions requested matches the already established profile. According to the authorities, the content of the MLA requests, as well as the testimony of witnesses, did not justify the initiation of a criminal investigation into TF (or terrorism). However, the AT has reservations about whether the Polish authorities took a proactive approach and left no stone unturned in this regard (please see IO.9).

776. More generally, there are no mechanisms and procedures for harvesting and using the information from the incoming MLA request, and the few numbers of such cases (as indicated above) indicates that LEAs should systematically do so.

777. Poland has demonstrated its capability to establish and to participate in Joint Investigative Teams (JITs), mostly with other EU Member States, during the period of 2015-2020. A list of 45 JITs is presented, of which five concern ML, and two concern an offence of a terrorist nature. The majority of JITs were in connection to crimes related to VAT frauds (nine cases, mostly with the Czech Republic), human trafficking (ten cases, mostly with the British authorities), car and truck theft (seven cases), drug trafficking (seven cases). Among the countries with which JITs are most often established are Germany and Great Britain. Four of the JITs involved the neighbouring country Ukraine. Since there is no obligation to formally initiate the procedure for setting up a JIT, e.g., by sending an official enquiry to a foreign party or a request for legal assistance or an EIO, it is not possible to determine at whose initiative such a team was set up.

778. As most of JITs target proceeds-generating crimes, the assessors welcome that three out of the five ML-related JITs concern stand-alone ML offences. The other two are in relation to ML associated with drug trafficking and tax fraud.

779. As discussed in more detail in the TCA, foreign confiscation orders can be enforced in Poland through the general mechanism of the CPC applicable to the recognition and enforcement of foreign judgments. However, according to Polish authorities, no foreign requests were received and processed under this legal framework during the assessed period.

780. Nevertheless, Poland received 39 incoming requests for applying seizure measures during 2014-2019. Out of 39 incoming requests, 33 are related to ML, which might indicate that the information regarding the requested seizure measures in relation to predicate offences was not provided. Although the reliability of the data is questioned by the AT, the available information indicates that almost in 40% of the cases the requests to apply seizure were denied (in 15 cases out of 39). The Polish authorities indicated that in some cases, the reasons for the refusal are objective (lack of funds in the bank account, which should be frozen), but no specific information on a case-by-case basis was available.

781. The execution of foreign requests to seize or freeze property that constitutes proceeds of crime or instrumentalities was mentioned by the authorities as representing the highest priority in judicial co-operation in criminal matters. Nevertheless, this is not supported by the available information. The value of assets seized upon foreign requests was presented only in a few cases

(2015 - €10 949; 2017 – €195 811; 2019 - €198 356) and there is no data on the total value of the seized (frozen) assets or the value of shared/returned to Poland assets for the period of concern.

782. In relation to the incoming extradition requests, the presented data refer only to ML cases. No statistics were presented in connection with other offences, the countries which most often submit extradition requests or the grounds of the refusals.

***8.2.2. Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements***

783. According to the Polish authorities, outgoing MLA requests are being sent regularly. This is only partially supported by the statistics (see Table 8.3.), demonstrating that in recent years about 80% of the outgoing MLA requests (e.g. in 2018 and 2019) are with regard to ML cases and only to a lesser extent to other offences. The number of outgoing MLA requests for the period 2017 – 2019 varies between 377 and 667. However, compared with 2014 (154 requests), the demand for international legal assistance has increased. Seeking mutual legal assistance is determined by the need for evidence to be gathered in the specific criminal proceedings with a foreign element.

784. The statistics provided on the number of MLA requests sent by the Polish authorities, the type of crimes to which they relate, the type of legal instruments used and the reliability of the figures for predicate offences are discussed in point 8.2.1. The same shortcomings described there are noted with regard to 8.2.2. and demonstrate the lack of systematic and accurate collection of MLA requests sought by the Polish authorities.

**Table 8.3. Outgoing MLA and extradition requests**

	All	ML	TF	Extradition
2014	154	125	0	3
2015	255	182	0	2
2016	257	192	0	7
2017	527	374	0	2
2018	500	386	0	4
2019	666	543	0	7
2020	N/A	N/A	N/A	N/A
Total	2 359	1 802	0	25

785. The authorities clarified that the requests are sent mainly to EU countries, and most of them are EIOs. Areas in which evidence obtained from abroad proved to be essential are ML and tax crimes, and the most frequently requested data from abroad are bank transfer information, account holders, telecommunications data, entity structure, hearing witnesses.

786. With regard to the duration of execution of MLA requests, the Polish authorities did not provide accurate statistics on the average time of execution. The shortest and longest term indicated on an annual basis can hardly serve as grounds for conclusions. The time frame obviously varies in an extensive range, as for the period 2014 – 2019 from 22 days to 1084 days concerning MLA, and from 137 to 1291 in extradition procedures.

787. According to the PPO, no deficiencies in the format, contents, or the legal basis of Polish requests or EIOs/EAWs have caused any delay or non-execution, particularly in the case of the

said EU instruments, where the formal and content aspects are determined by the format to be used.

788. Nevertheless, the timeliness of sought assistance could be undermined by a specific element of the procedure set by the Ordinance of the Minister of Justice of April 7, 2016 (Rules of internal operation of common organisational units of the Prosecutor's Office) in relation to direct co-operation with other countries (if there is legal basis for this), especially with other EU Member States, which restricts some prosecutors from sending MLAs directly. During the visit, it was confirmed that the local offices do not communicate directly with the authorities from other EU MS (only via the regional offices). This, according to the evaluators, may lead to unnecessary delays.

789. With regard to the quality of the MLA requests made, based on the feedback received from the international community, it should be noted that some countries indicated that often the requests are not comprehensive enough, do not clearly describe the offences and do not provide sufficient evidentiary basis to justify the assistance that is sought. This has an impact on the timeframe necessary for executing the outgoing MLA requests and caused the process to be prolonged.

790. For the period 2014-2019, the Polish authorities sent 62 requests for seizure and freezing (respectively 5, 31, 5, 6, 2, 13). All appears to be related to ML. Due to a lack of comprehensive data on the number of requests and the value of secured assets as a result of outgoing applications, no conclusions on the level of effectiveness can be drawn.

### *8.2.3. Seeking other forms of international co-operation for AML/CFT purposes*

#### ***FIU to FIU co-operation***

791. Since 2018, the GIFI has been able to exchange information regarding ML/TF with foreign partners, including spontaneously, without having signed a bilateral agreement on the basis of the AML/CFT Act. It enables the GIFI to exchange information on the basis of non-contractual reciprocity, in accordance with the rules and standard conditions for exchange of information within the Egmont Group, also respecting the relevant national law of the respective foreign FIU. The existing bilateral and multilateral agreements (92 bilateral and 2 multilateral agreements) are a broad basis for international co-operation, and only in rare cases did the GIFI send requests to countries with which it does not have an agreement (a total of 7 requests sent to Burkina Faso, Costa Rica, Dominica, Malaysia, Nigeria, St. Kitts and Nevis, Uganda).

792. The number of inquiries sent by the GIFI from 2014 – 2020 varies between 195 and 459 (see Table 8.4.)

**Table 8.4: FIU-to-FIU International Co-operation**

<b>International coopération</b>	<b>2014</b>	<b>2015</b>	<b>2016</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>
<b>Outgoing requests</b>							
<b>Requests sent by the FIU</b>	221	195	316	293	208	386	459
<b>Spontaneous sharing of information sent by the FIU</b>	-	-	-	-	16	-	5
<b>TOTAL (outgoing requests and information)</b>	221	195	316	293	224	386	464

793. Exchange of information between FIUs within the membership in Egmont Group is carried out through the secure and encrypted Egmont Secure Web (ESW). In addition to that, the Financial Intelligence Unit Network (FIU.NET) is also available between FIUs in EU member states, enabling FIUs connected to FIU.NET to compare their data with those of other FIUs without the use of sensitive personal data so as to identify various links to crimes in other countries. The GIFI communicates mainly with EU countries, among which France, Germany and the Czech Republic stand out as a frequency, and outside the EU - mainly with neighbouring Ukraine.

794. The information requested by the GIFI depends on the specifics of the case, but as the most frequently requested information, the following was indicated: whether a particular person or legal entity has been of interest to the other State; available criminal records; what is the source of funds received or transferred to Poland; financial information, tax information concerning subjects under analysis. In addition to that, the GIFI may also ask for the postponement of a transaction on a foreign bank account.

795. The AT was informed that on the basis of the results of analysis in the cases handled by the GIFI, it also sends spontaneous disseminations to foreign FIUs. During the analysed period, at least 21 such disseminations were made in 2018 and 2020 (no further statistics available, see Table 8.4.).

796. Since 2019, the GIFI also started sending out cross-border disseminations on the received SARs concerning other EU Member States<sup>71</sup>. In 2019, 475 and in 2020, 481 such reports were sent out, mostly to neighbouring countries, such as Germany, the Czech Republic, Lithuania and Hungary. The authorities also informed about a case in 2020, when information on suspected irregularities in a Dutch financial institution was proactively sent to the Dutch counterpart.

### **LEAs**

797. As described under the TCA (R. 40), Polish LEAs have the necessary tools and means to ensure the co-operation and exchange of information with foreign counterparts, including co-operation in relation to ML, TF and predicate offences. Nevertheless, it is difficult for the AT to assess the dynamic of such co-operation in the absence of the relevant or complete statistics (incoming/outgoing requests; breakdown based on the predicate offences, EU/ non-EU countries), or due to its classified nature (ISA).

<sup>71</sup> Pursuant to art. 53 (1) of the 4th AML Directive.

798. Additionally, the lack of such statistics broken down by jurisdiction 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 actually 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.

799. Overall, as an EU Member State, most of the co-operation activities are with the foreign counterparts from other EU Member States and that out of the three non-EU neighbouring countries (Ukraine, Russia and Belarus), the co-operation with Ukraine appears to be more intensive.

800. Police HQ is the national contact point for co-operation with Interpol and Europol. The AT was presented only with the information regarding the co-operation with Europol (through the SIENA channel). During the period 2015-2020, the number of exchanged messages has been steadily increasing: 732 070 (2015); 869 858 (2016); 1 005 610 (2017); 1 110 962 (2018); 1 243 943 (2019); 1 266 233 (2020). The number of new cases initiated by Poland also has increased over the period: 2015 – 424; 2016 – 520; 2017 – 641; 2018 – 759; 2019 – 915; 2020 – 983. The percentage of information related to ML in the newly initiated cases varies between 5% and 7%. During the period 2017 – 2020, Polish Police sent 543 inquiries on ML cases to foreign partners through the SIENA channel, including 97 by ARO. As explained by the authorities, the information on similar inquiries sent before 2017 is not available, as the SIENA system maintains the data only for a period of two years.

801. As an example of good international co-operation, the Polish authorities provided details on a drug-related ML investigation.

#### **Box 8.1 Money laundering by drug cartels**

The case concerns a current investigation carried out by the Central Bureau of Investigation of the Police (PCBI) of an international criminal organised group whose activity included, among others, the legalisation of the proceeds of South American drug cartels, including through the Polish financial system. The case was initiated based on the GIFI notification sent to the Police regarding ML suspicion. It was established that members of a Polish OCG, including one member who was specialised in creating financial solutions for legalising profits, using the activity of business entities - intermediaries of one of the largest cryptocurrency exchanges in the world, transferred funds in the amount of approximately 4 bln PLN (€0.88 bln) through the bank accounts of these entities. As a result of the investigation activities, assets in value of 1.2 bln PLN (€0.26 bln) were secured, which is the largest asset security in the history of the Polish LEAs. To prove the criminal origin of funds, the PCBI sought out assistance from EU countries, the FBI and the DEA. The PCBI officers also participated in many meetings organised by Europol and with representatives of the DEA and the FBI concerning the criminal activity of the OC group. Five suspects were charged for ML and participation in an OC group. Three suspects were temporarily arrested, and efforts are underway to issue an EAW against the other two suspects.

802. ARO carries out an intensive international exchange of information on the basis of the Act of 16 September 2011, not only for its own needs but also to assist other authorities in the field of ML and predicate offences. The reason for this is that they have faster and better channels for exchanging information. Most often, such exchanges take place with EU countries within SIENA,

but also with non-EU countries, such as Belarus, Morocco, Hong Kong, Russia, Panama within the CARIN network.

803. CBA has registered 31 outgoing requests in 2020 and 37 during the first 5 months of 2021. It is not clear if any of the requests concerned ML. Nevertheless, the authority informed the AT that at the pre-investigative stage, the co-operation is predominantly in relation to corruption or other predicate offences and that the co-operation on ML may occur at a later stage of the criminal investigation within the framework of MLA.

804. The international co-operation initiated by KAS (customs service) consists of 4 outgoing requests in 2019 (mostly to Germany in relation to excise fuel and smuggling) and 15 outgoing requests in 2020 (mostly in relation to excise tax and VAT and one request to UK and Sweden in relation to ML). Regarding tax exchanged information, during the period 2015-2020, there were 53 524 outgoing requests to EU Member States and 3 340 outgoing requests to non-EU countries (mostly to Ukraine and Belarus). Nevertheless, it is not clear how many of these concern criminal tax matters as the numbers include both criminal and civil related requests, which are handled in the same manner.

805. Border Guard does not keep statistics on the international exchange of information outside the SIENA channel. The available information indicates an average number of 500 incoming and outgoing requests via Europol over the period 2015-2020 (404 in 2015; 404 in 2016; 388 in 2017; 568 in 2018; 673 in 2019 and 634 in 2020).

806. Most LEAs, except for the CBA and the ISA, do not need an agreement in order to cooperate with their foreign counterparts. Those who need such a framework and do not have it with a specific country, in practice, can always rely on the assistance of the ARO. The authorities, in particular the CBA and the KAS, have expressed their satisfaction with the level of assistance for international co-operation provided by the ARO.

807. The concerns expressed by the AT under the TCA (R. 40) regarding the need for prior consent given by the Prime Minister in order to allow the CBA and ISA to cooperate with their foreign counterparts were clarified by the authorities to a certain extent. As explained, such consent is needed to establish the co-operation (agreement) with a country and is not required for each specific request. The CBA informed about receiving the consent of the Prime Minister to cooperate with 54 countries and 13 organisations, and that if there is a need to establish a framework for co-operation with another country, the general waiting time for the consent would be within the time limit established by the Code of Administrative Procedure (on average 30 days). Thus, the procedure for co-operation outside the framework of an agreement (including via ARO), under the condition of prior consent given the Prime minister, does not seem to be appropriate and may prove to be an impediment in relation to urgent cases (both, concerning outgoing and incoming requests). The same concern applies to the ISA, but to a lesser extent, as it had already obtained such consents to cooperate with more than 124 partners from 69 countries. The Polish authorities claim that this requirement creates no delays in practice. However, in the absence of relevant statistics, the AT remains concerned that it may impact, among other things, the timeliness of international co-operation.

### ***Supervisory authorities***

808. Both UKNF and NBP regularly exchange information with their foreign counterparts, but not for AML/CFT purposes.<sup>72</sup> In this area, both authorities rely on the GIFI, which has the power to exchange information on behalf of other authorities. Nevertheless, during the assessed period, none of the two supervisory authorities submitted via GIFI any outgoing requests for co-operation with their foreign counterparts. The GIFI is also a member of the Committee on anti-money laundering and countering terrorist financing of the European Banking Authority (EBA) and is able to cooperate with the European Central Bank (ECB). The Polish authorities informed about one received request from ECB submitted to the GIFI in the field of prudential supervision. No such outgoing requests were submitted by the Polish supervisory authorities. Overall, the exchange of information in the field of AML/CFT supervisory activity appears to be very limited.

#### ***8.2.4. Providing other forms of international co-operation for AML/CFT purposes***

##### ***FIU to FIU co-operation***

809. The GIFI provides information to foreign FIUs, both spontaneously and upon request, generally, in a timely and effective manner. GIFI conducts regular surveys regarding the quality and usefulness of the provided information, indicating overall satisfaction with the received information.

810. The GIFI clearly made an effort to improve the average response timeline with a median of 11 days in 2020 (17 days in 2019), compared to the legally established timeline of up to 30 days. The AT was informed that in 2020, about 25% of the received requests were of an urgent character which were dealt with, generally, in one day. The authorities also informed the AT about the plans for implementing an IT solution that would ensure increased timeliness of the responses.

811. The GIFI processes requests provided that the foreign request meets the minimum criteria as defined by the Egmont Group principles for exchange of information (link to the country to which the request is directed, sufficient reasons for ML/TF suspicion, an exhaustive description of the case). If the request does not meet these minimum requirements, the GIFI reaches out to the requesting counterpart to provide additional information and according to the authority, in nearly all cases (except one), it was able to obtain the additional information and provide the assistance. Nevertheless, in one case, when the request involved obtaining the information from a financial institution, the foreign counterpart managed to obtain the information faster via other channels (the foreign supervisory authority).

812. Likewise, in one case, only limited information was provided by the GIFI to the requesting country. According to the feedback provided by the international community, when asked whether the subjects were known in police information/intelligence, ongoing investigations or law enforcement systems, the response indicated that there is no available information without a specification on whether the checks were carried out or not. As informed by the GIFI, one of the main pillars of co-operation in the scope of exchange of information is that the GIFI is not obligated to provide information if judicial proceedings have been initiated in the case. It remains unclear to the AT whether such situations occurred as a result of the restrictive interpretation of the above-mentioned principle or of the level of co-operation between the domestic authorities. Notwithstanding these particular cases, the general feedback received from the international

---

<sup>72</sup> Due to the recent amendments of the AML/CFT Act, in force since July 2021 (Article 116a), the UKNF and NBP will be able to conduct direct information exchange with foreign counterparts on AML/CFT matters.

community is positive, and many of the foreign counterparts mentioned the high quality of the provided assistance by the GIFI. Before 2018, an agreement was a precondition for providing international assistance. With the new powers conferred in 2018 (AML/CFT Law), the GIFI is able to provide assistance outside the framework of a bilateral or multilateral agreement. Regardless, bearing in mind the extensive number of the existing agreements, such requests are quite rare – seven requests since 2018 coming mostly from the counterparts located in Africa and South America.

813. The majority of information exchange (70-80%) is conducted with the EU counterparts. Among the top requesting countries, Germany, Ukraine, Czech Republic and Switzerland were mentioned. The number of the received requests registered a slight increase in recent years (328 in 2014, compared to 475 in 2019; see Table 8.5.). As reported, no foreign requests were refused by the GIFI in the assessed period. Nevertheless, before 2018, there were cases of refusal due to the previous legal limitations requiring an MoU for co-operation (at least two requests were refused on that basis). Also, it remains unclear whether the GIFI refused to provide assistance in one case mentioned previously when it was unable to obtain the necessary additional information in relation to an incomplete foreign request.

**Table 8.5. FIU to FIU co-operation**

<b>International co-operation</b>	<b>2014</b>	<b>2015</b>	<b>2016</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>
<b>Incoming requests</b>							
<b>Foreign requests received by the FIU</b>	328	371	352	363	405	475	516
<b>Foreign requests executed by the FIU</b>	328	371	352	363	405	475	516
<b>Foreign requests refused by the FIU</b>	0	0	0	0	0	0	0
<b>Spontaneous sharing of information received by the FIU</b>	39	204	461	632	127 <sup>73</sup>	182	309
<b>TOTAL (incoming requests and information)</b>	367	575	813	995	532	657	825
<b>Average number of days to respond to requests from foreign FIUs</b>	N/A	N/A	N/A	N/A	N/A	17	11

814. The increasing number of foreign requests of information and spontaneous and cross-border disseminations determined the efforts to strengthen GIFI's capacity in the area by establishing a specialised unit with a staff of 5 employees (in December 2019). Nonetheless, the authority acknowledges the need for further development of the respective unit due to the increasing volume of co-operation.

<sup>73</sup> In the absence of the information on the exact number of spontaneous disseminations received by the GIFI out of the total 2893 received disseminations, which include the cross-border disseminations under the EU AML/CFT Directive, the number was calculated by extrapolation.

815. There is no formal procedure that would describe the mechanism for prioritisation of the received requests. The AT was informed that, in practice, requests are prioritised on the basis of specific factors: they were branded urgent by the requesting FIU; requests to postpone transactions/ block funds; an indicated timeframe for response; the underlying crime and the scale of the criminal activity; the need to obtain the information from third parties.

816. By default, the information exchanged may only be used by the counterpart FIU for analytical/intelligence purposes. Information can be further passed on to LEAs for intelligence purposes with the explicit consent of the GIFI. Foreign counterparts are also notified that if the information needs to be used as evidence in criminal proceedings, it is necessary to request it through MLA.

### ***LEAs***

817. As described under Core issue 2.3, the absence of the relevant or complete statistics (incoming/outgoing requests; breakdown based on the predicate offences, EU/ non-EU countries), or due to its classified nature (ISA), makes it difficult for the AT to assess the overall volume, timeliness, specific areas of co-operation and the countries to which Poland provided assistance. As an EU Member State, the co-operation activities with the foreign counterparts from other EU Member States prevail.

818. Police HQ is the national contact point for co-operation with Interpol and Europol. The AT was presented only with the information regarding the co-operation with Europol (through the SIENA channel). During the period 2017 – 2020, the Police have received 1 744 inquiries in relation to ML, including 125 inquiries received by ARO. The information on the period before 2017 is not available.

819. The CBA has registered nine incoming requests in 2020 and six incoming requests during the first five months of 2021. No information was provided on whether any of the foreign inquiries are in relation to ML. The concerns expressed by the AT concerning the procedure for co-operation outside the framework of an agreement (including via ARO), under the condition of prior consent given by the Prime minister, are valid for the ability of the authority to provide assistance, especially in urgent cases.

820. KAS (customs service) received three foreign requests in 2019 (mostly from Germany relating to money laundering and corruption) and 39 in 2020 (one request on ML from UK and others are in relation to excise tax, VAT, cigarettes smuggling). Regarding tax exchange information, during 2015-2020, KAS received 20221 incoming requests from EU Member States and 1000 incoming requests from non-EU countries (mostly from Ukraine and Belarus). It is not possible to determine how many of these concern criminal tax matters.

821. The available information regarding the assistance provided by the Border Guard was described under Core Issue 2.3.

822. The feedback received from the international community regarding the co-operation with the Polish LEAs is overall positive in terms of the quality and the timeliness of the provided assistance, although, in certain cases, the need for direct communication via a designated representative was expressed (regarding the Police).

### ***Supervisory authorities***

823. The analysis under Core Issue 2.3 is also applicable in the area of provided assistance to foreign counterparts. Additionally, the GIFI informed about four cases when the assistance was

provided to a foreign FIU, which acted as a supervisor (3 in 2021). Two cases of co-operation between the GIFI and foreign supervisory authorities, other than FIU, took place in 2020.

### ***8.2.5. International exchange of basic and beneficial ownership information of legal persons and arrangements***

824. The GIFI informed that no specific requests on BO information were received and that such information is usually provided in response to broader requests for information from foreign counterparts, in connection to legal entities or account information, etc. Primarily, the first source of information would be the reporting entities. It appears that it is a standard practice to require the information on BO when obtaining the information from the reporting entities on accounts held by legal persons. Other sources of information include its own database (if the subject of the request was a subject of a previous SAR), the registry on legal entities and the Central Register of Beneficial Owners. The feedback from the international community is positive regarding the quality of responses provided by the GIFI, and some confirm that the GIFI carries out by default the checks described above.

825. Police also informed the AT that usually, the requests on BO information are part of the more general inquiries. It also stated that almost all MLA requests include companies, which implies the verification of the information on the BO, although not specifically required. The primary source of information would be the court and BO registries. Additionally, when needed, it can initiate tasks for collecting more intelligence.

#### **Box 8.2**

##### **Case 1 - "TINTO" case (Spain)**

The Spanish request was connected to a case "TINTO" concerning fraud to the detriment of Spanish nationals and money laundering. The request concerned checks about some Polish companies (limited liability companies) and bank accounts.

The response consisted of data about registration data of the companies, ultimate beneficial owners (UBO), as well as information concerning an ongoing investigation led by the Polish police.

The Spanish authorities provided positive feedback on the received assistance (a "thank you letter").

##### **Case 2 - Co-operation with the HM Revenue & Customs (HMRC)**

British request was connected to a case led by HM Revenue & Customs (HMRC) concerning money laundering committed by an organised criminal group and which was connected to Polish companies, nationals, as well as British nationals.

The response consisted of personal data on Polish nationals and data about the Polish companies' ultimate beneficial owners (UBO), criminal records, OSINT information, information received from FIU, as well as of information concerning an ongoing investigation led by the Polish Police.

826. In the area of prudential supervisory activity, the UKNF shares the supervisory information, including about BO under the Capital Market Surveillance Act of 19 July 2005, with its foreign counterparts. In the years 2014-2019, the UKNF received from its foreign counterparts approximately 15-40 (varying depending on the particular year) requests for information on

basic and beneficial ownership concerning legal persons. The vast majority of these requests were sent pursuant to ESMA MoU and IOSCO MoU. None of the requests resulted in the UKNF's refusal to provide information.

### ***Overall conclusion on IO.2***

827. 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. The level of co-operation with some non-EU jurisdictions bordering Poland appears to be less constructive, despite the ML/TF risks associated with these. The statistics on international co-operation (both on incoming and outgoing MLA/extradition requests) do not include a breakdown by jurisdiction and by the predicate crimes involved and, therefore, could not assist in demonstrating that MLA is used constructively to address specific ML/TF threats of international nature mentioned in the NRA. The existing case management system is fragmented, and no guidelines exist with regard to the handling and prioritisation of the MLA requests. This impacts the quality and timeliness of MLA requests, both incoming and outgoing. There are cases of serious delays in the execution of incoming requests without specific objective reasons and delays in the execution of the outgoing requests (due to the quality of the requests submitted by Poland) This appears to be also reflected in the feedback provided by other jurisdictions. According to Poland, during the assessed period, no foreign requests were received for the execution of confiscation orders. This appears to be in contrast with the 39 incoming requests for applying seizure measures, received during the same period. Although the reliability of the data is questioned by the AT, the information indicates that in almost 40% of the cases, the requests to apply seizure were denied. The information on the total value of the seized (frozen) and confiscated assets or the value of shared/returned to Poland assets for the estimated period was not provided and do not support the conclusion on effective co-operation in this matter. There is no proactive harvesting of incoming MLA requests by competent authorities with the aim of detecting 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. The number of foreign requests refused or not executed, apart from the requests on seizure, is very low, according to the authorities. Nevertheless, the provided data refers only to ML and no conclusion can be achieved regarding the total number of granted and refused MLA/ extradition requests in connection to predicate crimes. In relation to the dual criminality standard and other technical deficiencies identified under R. 3 and 5, no cases were presented indicating that the provision of assistance has been hampered by these. The GIFI and LEAs proactively exchange information with their foreign counterparts and provide a good quality of assistance. In the absence of relevant data, it is difficult to assess to which extent this co-operation is carried out for AML/CFT purposes. Nevertheless, the modest contribution made by LEAs to ML identification (as described under IO7) is an indicator that LEAs do not actively seek to exchange information for ML 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 foreign counterparts for AML/CFT purposes.

**828. Poland is rated as having a Substantial level of effectiveness for IO.2.**

## TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations in numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.
2. Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2013. This report is available from <https://rm.coe.int/moneyval/jurisdictions/poland>.

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

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

#### ***Criterion 1.1 (Met)***

3. Poland performed its first National Risk Assessment (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 National Risk Assessment (PNRA) in co-operation with the International Monetary Fund (IMF). 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. Apart from the NRA, a risk assessment for entrepreneurs conducting currency exchange activity was developed by the NBP and contains more detailed information on the specific risks. This assessment is updated in November each year.

#### ***Criterion 1.2 (Met)***

6. The designated authority and the mechanism to coordinate 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 Narodowy Bank Polski (NBP), the Komisja Nadzoru Finansowego (KNF), the Supreme Audit Office (NIK)<sup>74</sup> and the obligated institutions.

#### ***Criterion 1.3 – (Met)***

7. 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.

#### ***Criterion 1.4 – (Met)***

8. 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

---

<sup>74</sup> the “cooperating units”

approval. After the approval, the GIFI shall publish the NRA in the Public Information Bulletin on the website of the Ministry of Finance (excluding the part containing classified information). The results of the NRA were published in the Public Information Bulletin in July 2019.

9. The results of the NRA were communicated to the public and the private sectors in a series of seminars organised by the GIFI. In January 2020, the GIFI organised a conference on the NRA attended by around 100 participants from the public and private sectors.

***Criterion 1.5 – (Partly met)***

10. 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 some measures that compound the re-allocation of resources according to the risk (*e.g.* measures related to the FIU’s human and technical resources dedicated to operational analysis). Nevertheless, due to recent adoption of the Strategy (three weeks before the onsite visit), no risk-based re-allocation of resources was in place.

11. 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.

***Criterion 1.6 – (N/A)***

12. Applicable legislation does not provide for disapplication of any FATF Recommendations requiring FIs or DNFBPs to take certain actions.

***Criterion 1.7 – (Partly Met)***

13. According to Article 43(1) of the AML/CFT Act, the obligated institutions shall apply enhanced customer due diligence 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 SNRA 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.

***Criterion 1.8 – (Partly Met)***

14. According to Article 42(1) of the AML/CFT Act, the obligated institutions may apply simplified customer due diligence 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 SNRA when identifying and

assessing their ML/TF risk exposure does not amount to a requirement meeting this criterion.

15. Article 42(2) sets out the circumstances that may substantiate a lower money laundering and terrorist financing risk. It is not clear if these circumstances referred to in the AML/CFT Act as possible low risk criteria are consistent with the country's assessment of ML/TF risks. 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.

***Criterion 1.9 – (Mostly Met)***

16. 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, the deficiencies described under R.26 and R.28 (particularly 26.5 and 28.5) impact this partial rating.

***Criterion 1.10 – (Mostly met)***

17. 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.

18. (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.

19. (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.

20. (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.

21. (d) Have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. 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 discretionary rather than obligatory requirement.

***Criterion 1.11 – (Mostly Met)***

22. (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)).

23. (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)).

24. (c) Take enhanced measures – There is no explicit requirement to take enhanced measures to manage and mitigate the risks where higher risks are identified.

***Criterion 1.12 – (Mostly Met)***

25. The obligated institutions may apply simplified customer due diligence 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 if 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. The obliged entities cannot apply simplified CDD where there is suspicion of ML/TF (Art 42 (3) and Art 35(1)(5) and (6)).

*Weighting and Conclusion*

26. Some of the criteria are met, but moderate deficiencies remain: no risk-based re-allocation of resources; 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; 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; 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 discretionary rather than obligatory; there is no explicit requirement to take enhanced measures to manage and mitigate the risks where higher risks are identified.

**R.1 is rated Partially Compliant.**

***Recommendation 2 - National Co-operation and Coordination***

27. In 2013, Poland was rated LC with former Recommendation 31. The assessment identified technical deficiencies related to the lack of a mechanism for facilitating a regular and joint review of the AML/CFT system and its effectiveness by competent authorities and the lack of a central coordinating body at the policy level in the area of AML/CFT.

***Criterion 2.1 – (Met)***

28. On the basis of the NRA, the GIFI shall draft the Strategy on counteracting money laundering and financing of terrorism. In the event of a change in the NRA, the Strategy shall be updated. Since the NRA must be updated regularly (see R1.3), the Strategy shall also be updated regularly.

29. By Resolution 50 of the Council of Ministers of 19 April 2021, the AML/CFT Strategy was adopted. The Strategy was informed by the NRA and includes an Action Plan and a list of measures to be implemented under particular priorities. The Financial Security Committee operated by the GIFI as a consultative and advisory body in the field of counteracting money laundering and financing of terrorism would be in charge of reviewing the Strategy if need be.

***Criterion 2.2 – (Met)***

30. Poland has designated the GIFI to be the authority responsible for national AML/CFT policies. The responsibilities of the GIFI are set in the AML/CFT Act and include

preparing the AML/CFT strategies in co-operation with competent authorities<sup>75</sup> and reporting entities.

#### ***Criterion 2.3 – (Mostly Met)***

31. According to Article 19(1) of the AML/CFT Act, the Financial Security Committee shall operate at the GIFI, acting as the opinion-making and advisory body in the scope of counteracting money laundering and financing of terrorism. All policymakers, including the national FIU, law enforcement authorities, supervisors and other competent authorities, are represented in the Financial Security Committee. An operative coordination platform or similar arrangements are missing.

#### ***Criterion 2.4 – (Partly met)***

32. As part of the Ministry of Finance, the Customs Department of the KAS cooperates with the GIFI and the Ministry of Economic Development, Labor and Technology in the scope of information exchange and consultation on proliferation matters and with the International Administrative Assistance in Customs Matters Unit of the Revenue Administration Regional Office in Wrocław as required by EC 2.4. However, there are no formal or factually functional co-operation or coordination mechanisms to combat the financing of proliferation of weapons of mass destruction.

#### ***Criterion 2.5 – (Met)***

33. Each draft legislative act (including in the area of AML/CFT) is subject to an opinion process consideration by all competent authorities, including the Office for Personal Data Protection. Data protection issues are particularly important and, within the framework of existing obligations to respect the EU and national regulations in this area, any comments submitted are consulted. This provides for a working basis. It can therefore be confirmed that there is a generally defined mechanism for co-operation as well as coordination between the competent authorities.

34. In addition, the Act of 14 December 2018 on the protection of personal data processed in connection with the prevention and combating of crime, the tasks of the Chairman of the Personal Data Protection Office ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules. In addition, the co-operation and coordination mechanisms are ensured through the application of the EU Regulation 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

#### ***Weighting and Conclusion***

35. All criteria but one are fully met. Minor deficiencies remain as there is no formal co-operation and, where appropriate, coordination mechanisms to combat the financing of proliferation of weapons of mass destruction, nor a formal platform for operative coordination. **R.2 is rated Largely Compliant.**

#### ***Recommendation 3 - Money laundering offence***

36. In the 4th round of evaluation, the relevant recommendations (R1 and R2) were rated Partially Compliant and Largely Compliant, respectively. The basis of the rating were

---

<sup>75</sup> According to Art. 2 of the AML/CFT Act, cooperating units shall mean any government and local government authorities and other state organisational units as well as Narodowy Bank Polski (NBP), the Komisja Nadzoru Finansowego (KNF) and the Supreme Audit Office (NIK)

deficiencies concerning the physical element of the ML offence and essential criteria missing in connection with conspiracy and association. In 2016 a new definition of the money laundering offence was introduced in the Criminal Code (amendment in force since 13 February 2016) to remedy the deficiencies identified.

***Criterion 3.1 – (Partly met)***

37. Poland is a party to the 1988 UN Vienna Convention and the UN Palermo Convention of 2000. The previous ratings (2013) were based on the fact that the offence did not cover every element according to the conventions, in particular, conversion, concealment, disguise, acquisition, possession or use were not covered in all circumstances. The amended, currently in force text of the Criminal Code (Art. 299) partially remedied the previous lack of physical elements in line with the two conventions. However, there are still outstanding issues based on which the disposition of the crime is not in line with the standards set by the conventions. The main concern is that while the conventions require the criminalisation of both an immaterial, intention-based form and a material, result-based form of money laundering, the Polish Penal Code limits its own scope and focuses solely on a potential result, a danger (“may frustrate or substantially obstruct the determination of criminal origin”) created by the action of the perpetrator. The physical element “transports abroad” seems to have an exclusively outward meaning, limiting the scope as well. Another inherent problem is the wording concerning the benefits of crime “that have been obtained from the benefits derived from a committed act”, which hints at an indirect, secondary connection to the illicit assets. The judicial practice (the Supreme Court of Justice) established that direct gains could also be subject to money laundering. Nevertheless, the jurisprudence of the higher courts is not recognised as a binding source of law, and the provision has to be amended.

***Criterion 3.2 – (Met)***

38. Concerning the predicate offences, Poland adopted an all-crime approach. Therefore, all offences provided by the CC and CFC are predicate offences for ML. Table 8 under para. 176 of the 2013 MER indicates the way the Polish legislation covers the FATF designated categories of offences. Tax offences are incriminated under Section II (special part) of the CFC.

***Criterion 3.3 – (N/A)***

39. Poland does not include a threshold or a combined approach; therefore, this criterion is not applicable.

***Criterion 3.4 – (Mostly met)***

40. The definition of property in Art. 299, supported by the legal framework outside of criminal law, covers any type of property, including virtual assets, through the phrase “property rights” (defined by Art. 44 of the Civil Code). The interpretation of the law that there is no difference between directly or indirectly gained criminal assets has been laid down in court decisions. However, the actual wording of Article 299 para 1, property “derived from the benefits relating to the commission of a prohibited act”, raises doubts whether directly obtained proceeds serve as a suitable basis of ML offence. The issue of directly obtained proceeds as property covered by ML offence is known to have raised concerns in the past among judges and prosecutors (para. 171 of the 2013 MER).

***Criterion 3.5 – (Met)***

41. The provisions of Art. 299 do not formally require that a person be convicted of the predicate offence in order for the property to be considered proceeds of crime. The article refers to property “derived from the benefits relating to the commission of a

prohibited act” (not of an “offence”).

**Criterion 3.6 – (Mostly met)**

42. The ML offence in Art. 299 of the CC does not explicitly address the issue of extraterritorial predicate offences. At the same time, the element of “transports abroad”, which appears to have an exclusively outward meaning, is limiting the scope of the ML offence with regard to the inward proceeds of crime. The general principles of the CC on Polish jurisdiction<sup>76</sup> do not answer the question of whether under Art. 299, the Polish authorities are able to prosecute ML connected to predicate offences committed abroad by foreigners and which are not linked in any way to Poland.

**Criterion 3.7 – (Met)**

43. Perpetrators of the predicate offence are not excluded from being liable for the ancillary ML offence, thus self-laundering is featured in the Polish criminal law, also supported by jurisprudence.

**Criterion 3.8 – (Met)**

44. In Polish criminal law, criminal liability is based on *mens rea* and free assessment of evidence by the judge, where the perpetrators’ intention and knowledge can be deducted from factual, objective circumstances.

**Criterion 3.9 – (Met)**

45. According to Art. 299 PC, the basic form of money laundering, is punishable by imprisonment from 6 months to 8 years. In case of collusion with other perpetrators or gaining “substantial material benefits”, the frame of sanction is 1 to 10 years. Preparation to commit ML, including conspiracy, is punishable by imprisonment from one month to 3 years. “Substantial material benefits” does not have an autonomous legal definition. Therefore the judicial practise treats it as a “property of substantial value” defined by Art. 115 para 5 CC, as property exceeding PLN 200 000 (€44 000) as of the commission of the crime.

46. If the perpetrator commits an ML offence acting as a member of an organised criminal group or association or as a permanent source of income, under Article 65 (1) of the Penal Code, the court may (discretionally) impose sanctions exceeding the original upper statutory limit, increased by half (in effect making it possible to impose imprisonment up to 12 years).

47. In addition, in the event of a conviction for ML, the court may go beyond the general framework of financial penalty (10-540 daily rates) and may impose in addition to the penalty of imprisonment, in the maximum amount of up to PLN 2 000 (€440) as a daily unit up to PLN 3 000 (€660) daily rates, which may potentially result in a fine of PLN 6 000 000 (approximately €1 430 000).

48. The framework of sanctions that can be potentially imposed on the perpetrator of an ML offence is proportionate and dissuasive.

**Criterion 3.10 – (Partly met)**

49. The criminal liability of legal persons is regulated in a separate act (Act of 28 October 2002 on the liability of collective entities for acts prohibited under penalty). The scope of the law sufficiently covers the ML offence-related conduct. The liability of the

---

<sup>76</sup> Articles 109 – 113 require the foreign offence to be committed i) by a Polish citizen; ii) by foreigners against the interests of the Republic of Poland, a Polish citizen, a legal person or an organisational unit; iii) by foreigners who have committed abroad a terrorist act; or iv) where the material benefit has been obtained within the territory of the Republic of Poland.

legal person under the law has a secondary nature and is inseparably tied to the prior determination of criminal liability of a natural person falling into the above categories, even if the prosecution does not lead to a formal conviction (due to voluntary acceptance of liability in tax offences or other circumstances which require the discontinuance of the criminal proceedings, or circumstances excluding the punishment of the perpetrator). There is no possibility under the mentioned law to hold liable a legal entity if the natural person (referred to in Art. 3) cannot be identified or takes flight, even in the presence of clear evidence indicating the culpability of the legal person. The respective law provides for a number of sanctions of administrative nature, including financial penalties (though in a limited way<sup>77</sup>), forfeiture and bans from relevant activities. The dissolution of the collective entity is not available as a sanction. Overall, the narrowing factors in the law limit the scope of corporate criminal liability and the limitations concerning the sanctions are detrimental to the dissuasiveness<sup>78</sup>.

### ***Criterion 3.11 – (Met)***

50. The Polish Penal Code includes, in general, every form of ancillary offences: participation, association in or conspiracy to commit, attempt, aiding, abetting, facilitating and counselling the commission. Preparation is punishable under Art. 299 § 6a.

### ***Weighting and Conclusion***

51. Poland criminalised the fundamental aspects of money laundering. Some shortcomings remained concerning: the requirement of a potential result, i.e. a danger to the determination of criminal origin resulting from the perpetrator's action, the physical element of transporting abroad and the concerns regarding directly obtained proceeds as property covered by ML offence, all potentially limit the scope of the ML offence as defined by the Conventions; and the need to establish a natural person's criminal liability as a basis for liability of legal persons is too narrow to fully cover the requirements of 3.10. **R.3 is rated Largely Compliant.**

### ***Recommendation 4 - Confiscation and provisional measures***

52. The 4th round MER rated former Recommendation 3 as PC due to the following: no clear provision allowing for confiscation of instrumentalities that have been transferred to third parties (as they have to belong to the offender); limited ability to confiscate criminal proceeds in financing of terrorism cases as the offence itself is limited and effectiveness issues.

### ***Criterion 4.1 – (Mostly met)***

53. The Polish Penal Code provides for a series of provisions (Art. 44-45a) on forfeiture (confiscation). These provisions are not ML or TF-specific but generally applicable for all crimes. Beyond the general rules on forfeiture, Art. 299 § 7 contains special rules concerning the ML offence, making confiscation mandatory for directly or indirectly gained items, derived benefits or their equivalent-in-value.

54. The system also features a special form, which is perceived as a specific type of instrumentality, forfeiture of an enterprise, which may be applied if the perpetrator

---

<sup>77</sup> Up to 5 mil. PLN (about €1 mil.), compared to the administrative fine – up to €5 mil., under the AML/CFT Law for the legal entities which are reporting entities.

<sup>78</sup> These limitations were also perceived as *potential legal barriers which could impede the investigation and prosecution of legal persons and could preclude the imposition of effective and dissuasive sanctions*, by the conclusions of the 2007 report of the OECD WG on bribery in international business transactions report (para. 157), <https://www.oecd.org/daf/anti-bribery/anti-briberyconvention/38030514.pdf>

directly or indirectly obtained material benefits using the enterprise (Art. 44a). The confiscation measures are applied only in relation to “items”. Previously, the Polish authorities stated that “items” cover only material objects<sup>79</sup>, thus, the intangible assets remained uncovered. As a more recent development, the authorities claim that the intangible assets could be potentially confiscated as “material benefit” gained from the commission of an offence (Art. 45 § 1) and informed about certain ongoing investigations dealing with virtual assets. Nevertheless, the AT was not presented with case examples to demonstrate the practical application and the broad interpretation of the legal provision (“items”), which would include the virtual assets.

55. (a) The laundered property is not expressly covered. According to the interpretation of courts (examples provided by the Polish authorities referring to judgements pronounced by court of appeal), the laundered property can be confiscated as property derived from ML or as benefits from predicate offence. Such interpretations have not a binding character, although the lower courts usually follow the precedents of the higher courts.

56. (b) Confiscation of items derived directly from an offence is possible under the provisions of Art. 44 § 1 of the CC. Any benefits from an offence, even if obtained indirectly, are subject to confiscation (Art. 45). Instrumentalities used or intended for use can be confiscated pursuant to the provisions of Art. 44 § 2 of the CC, although their application has a discretionary character.

57. (c) There are no specific provisions for the confiscation of the property used, intended, or allocated for use in FT and terrorism-related offences. However, such property may be confiscated as “items which served or were designed for committing an offence” (Art. 44 §2). Nevertheless, the application of these provisions is discretionary (“the court may decide”) and may not be applied if their imposition would not be commensurate with the severity of the offence committed. Compensatory damages to the state would be applied instead (Art. 44 §3).

58. (d) The provisions of the CC provide for the confiscation of property of corresponding value in respect of items derived from crime, instrumentalities used or intended to be used, enterprise and the benefits of crime (Art. 44§4, 44a§1, 45a§1).

59. Art. 45a of the CC establishes the possibility of forfeiture even in cases where a conviction is not possible (due to the perpetrator’s death, mental or serious illness, or absence).

60. Reversed burden of proof concerning material benefits extending to five years before committing the crime up to the sentencing (extended confiscation) carries a special weight since ML and TF offences fall into this category (a crime subject to the penalty of deprivation of liberty with an upper limit of at least five years).

#### ***Criterion 4.2 – (Met)***

61. (a, b, d) In the course of the criminal procedure, Polish authorities are obliged to collect information and evidence about the property and income of the perpetrator, the extent of damages, and take steps for securing assets in the form of seizure or a provisional measure, “security on property” with regard to forfeiture (Art. 213-214, 217, 291 and 297 of Code of Criminal Procedure). The general rules on forfeiture of proceeds and instrumentalities of a crime also cover those of financing of terrorism, terrorist acts or terrorist organisations. Property of corresponding value is subject to forfeiture based on Art. 44 para 4 PC, thus has to be traced and secured the same way.

---

<sup>79</sup> 2011 OECD report, page 17, <http://www.oecd.org/poland/2020928.pdf>

62. In March 2017, amendments to the legal framework (Penal Code, Act on the Police and connected laws). In addition to the traditional measures to identify assets in the criminal procedure, extended the powers of police to obtain information concerning assets, as well as a means to facilitate access to information from various registries and service providers.

63. (c) On the basis of the provisions of Art. 45 §3 of the CC, the Polish authorities have the ability to take steps in order to prevent or avoid actions that would prejudice the country's ability to freeze or seize or recover property that is subject to confiscation, despite any changes in the ownership, unless any interested person or organisation unit proves that it was legally received.

#### ***Criterion 4.3 - (Met)***

64. The protection of rights of bona fide third parties is recognised and guaranteed throughout the criminal procedure by the Penal Code, the Code on Criminal Procedure and by the Penal Fiscal Code. Claims of bona fide third parties concerning secured assets are in general an obstacle to forfeiture *in rem* and result in an equivalent-in-value measure (Penal Code Art. 44 § 5, 7, Art. 44a § 3, 6, Art. 45 § 5., Art. 299 § 7).

#### ***Criterion 4.4 - (Partially met)***

65. There is no established system to preserve and manage seized or confiscated assets, other than the provisions of the Criminal Procedure Code and the Rules of Internal Procedure of the PPO, which is based on the nature of the seized items (e.g., evidence, prohibited items, objects of artistic or historical value, perishable objects, etc.).

#### ***Weighting and Conclusion***

66. The confiscation of instrumentalities, including the property used, intended or allocated for use in TF, terrorist acts or terrorist organisations, has only a discretionary character and the property subject to confiscation is limited to "items" and does not include intangible assets. The confiscation of the laundered property is not provided expressly. There is no comprehensive mechanism to preserve and manage seized or confiscated assets. **R.4 is rated Largely Compliant.**

#### ***Recommendation 5 - Terrorist financing offence***

67. In the 4th round evaluation report, Poland was rated 'PC' for the former Special Recommendation II. The evaluation team had concluded that funding terrorist organisations or an individual terrorist is not fully criminalised, so is the terrorist financing committed abroad. It had been pointed that there were purposive supplementary elements for some of the acts constituting offences in the treaties annexed of the Convention. Since then, the Polish authorities initiated and approved a National antiterrorist program for 2015-2019, a strategic document aiming, among the others, to improve the anti TF provisions. As a result, an amendment of the Penal Code (PC) was introduced in March 2017, broadening the existing autonomous offence of financing of terrorism (Article 165a of the PC).

#### ***Criterion 5.1 - (Mostly met)***

68. Terrorism financing continues to be criminalised by Art. 165a (Crimes against public safety) in combination with Article 115 (20) of the PC, which defines a crime of a terrorist character. Art. 165 (a) criminalised the act of "accumulating, transferring or offering" goods with the intent of financing a crime of a terrorist character, or a crime provided by a series of Art. of the CC, corresponding to the treaties listed in the annex to

the TF Convention. However, the criminal conduct provided for in one of the treaties included in the annex<sup>80</sup> and by the instruments amending the Treaty offences<sup>81</sup> is not encompassed by the terrorist acts under the CC. Therefore, TF offence does not fully capture all of the offences in the treaties listed in the Annex to TF Convention as required by its Art. 2(1) (a). The requirements of Art. 2 (1)(b) of the Convention are covered by the reference to Art. 115 (20) of the PC. However, Art. 165a §1 does not provide expressly for all the elements of Art. 2(1) of the TF Convention, since the indirect provision or collection of funds, and the intention/knowledge that the funds are to be used “in full or in part” are not explicitly covered by the TF offence.

***Criterion 5.2 – (Partly met)***

69. The Polish PC (Art. 165a § 2) criminalises the act of making funds or other assets available to groups or associations having the purpose, or persons intending to commit a terrorist act. In the absence of a definition for the terms “terrorist organisation” and “individual terrorist”, Art. 165a §2 is making reference to some characteristics aiming to describe those: (i) “an organized criminal group or association intending to commit” a terrorist act, (ii) “a person participating in such a group or association intending to commit” a terrorist act; and (iii) “a person who intends to commit” a terrorist act. However, the described elements are not fully in line with those defining the terms “terrorist organisation” and “terrorist” under the FATF Glossary. On the other hand, the “intention” element (as described under IO9) is understood by the academia, practitioners and judiciary to be strictly connected to a specific terrorist act for the recognition of the TF<sup>82</sup>. All these are indicative on the need for more clarity (via legislative amendments or guidelines) regarding the coverage of TF for “any purpose”. The mere collection of funds without having made the funds available to terrorist organisations or individual terrorists for any purpose is not covered. The shortcomings related to the indirect funding and the partial use of the funds as described under R5.1 apply.

***Criterion 5.2 bis – (Mostly met)***

70. Art.165a §3 criminalises the covering of costs, without a statutory duty to do so, associated with satisfying the needs or carrying out financial obligations of a group, association or persons intending to commit a terrorist act. This could include the travel costs. Art.165§3 criminalises the financing of a terrorist act, including that covered by Art. 259a of the CC, consisting in crossing the border with the purpose of committing in another state’s territory a crime of a terrorist character or participating in a terrorist training (Art. 255a of the CC). Art. 255a §2 covers only the “receiving” of a training (engaging in), and not the “provision” of a training, as required by the standard. Additionally, it provides for the purposive element of “committing a crime of a terrorist character” before engaging in a training that “may make the commission of such crime possible”. Thus, the financing of travel of individuals for the purpose of providing terrorist training is not covered, while the financing of travel for the purpose of receiving a terrorist training is covered only when linked to the purpose of committing a terrorist act.

***Criterion 5.3 – (Mostly met)***

71. The funds or assets covered by the TF offence include assets of every kind, i.e. legal

---

<sup>80</sup> 1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf.

<sup>81</sup> 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, 2005 Protocol to the Convention for Suppression of Unlawful Acts against the Safety of Maritime Navigation, Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (New Civil Aviation Convention).

<sup>82</sup> Also, the case example invoked by the authorities to demonstrate that no such connection needs to be proved refers to the “collecting and transferring” of funds, which is not covered by Art. 165a §2 (but rather by Art. 165a §1), for the purpose of financing terrorist offences to be committed by members of a terrorist organization.

tenders, financial instruments, securities, foreign exchange, property rights or other movable or immovable property. Nevertheless, Art. 165a PC does not distinguish between legitimate or illegitimate sources..

**Criterion 5.4 – (Mostly met)**

72. Art.165a PC does not specifically require that the funds or other assets were actually used to carry out or attempt a terrorist act or be linked to a specific terrorist act. However, the restrictive interpretation of the “intention” element adopted in jurisprudence and followed by practitioners, as discussed under C.5.2 above, requires a strict connection to a specific terrorist act, which does not allow for a full compliance with c.5.4.b.

**Criterion 5.5 – (Met)**

73. The present AT upholds the conclusions of the previous round evaluators that in the Polish jurisprudence, criminal intent can generally be inferred from objective factual circumstances according to the principle of criminal proceedings (principle of free evaluation of evidence), based on principles in the Code of Criminal Procedure (Article 2 §2 and 92).

**Criterion 5.6 – (Mostly Met)**

74. Overall, the penalty (imprisonment from 2 to 12 years) in relation to natural persons is considered proportionate and dissuasive. The maximum limit of the possible imprisonment was increased by the 2017 amendment (from 8 years to 12) and has to be welcome as a positive step. However, the penalty for acts under Art. 165a § 3 is limited up to three years, thus not meeting the requirement of proportionality and dissuasiveness. The principles of the imposition of the penalties are established by Art. 53 (1) and (2) of the CC and include *inter alia*: the level of social consequences of the act committed, the preventive and educational objectives which the penalty has to attain with regard to the sentenced person, the motivation and the manner of conduct of the perpetrator, the type and dimension of any adverse consequences of the offence, the characteristics and personal conditions of the perpetrator, his efforts to redress the damage or to compensate the public perception of justice in another form, etc. Also, the court may impose a fine in addition to the penalty of deprivation of liberty if the perpetrator has committed the act in order to gain material benefit or when he has gained such benefit (Art. 33(2) of the CC).

**Criterion 5.7 – (Partly Met)**

75. A collective entity may be held liable in case of commission a terrorist financing offence by a natural person according to the *Act of 28 October 2002 on the liability of collective entities for criminal acts*. The civil or administrative or individual criminal liability of the perpetrator is not excluded (art.6 Act of 28 October 2002). The liability of an entity is secondary to the criminal liability of an individual acting on its behalf. There is no possibility to hold liable an entity, if the natural person (referred to in Art. 3 of the law) cannot be identified or takes flight, even in the presence of clear evidence indicating the culpability of the legal person

76. A fine ranging from PLN 1 000 to PLN 5 000 000 (approx. €225 to €1 125 000), forfeiture of property and different bans may be applied to a legal person. The dissolution of the collective entity is not available as a sanction. Overall, the narrowing factors in the law limit the scope of corporate criminal liability and the limitations concerning the sanctions are detrimental to the dissuasiveness<sup>83</sup>.

---

<sup>83</sup> These limitations were also perceived as *potential legal barriers which could impede the investigation and prosecution of legal persons and could preclude the imposition of effective and dissuasive sanctions*, by the conclusions of the 2007 report of

### ***Criterion 5.8 – (Met)***

77. The criminal liability for a wide range of ancillary criminal activity remains as reflected in the 4<sup>th</sup> MER (§232 – 233) and fully satisfies the criterion. The attempt to commit, participation in as aiding and abetting, facilitating and counselling the commission of an act are criminalised by the provision of Chapter II of the Penal Code. Article 18 of the General Part of the PC addressed liability for organising or directing other persons in a common way. In addition, a special provision (Art. 258 PC) covers organising or directing others to commit a crime of a terrorist nature. Contribution to the commission or attempting a crime of financing terrorism meets the criteria as it is actually aiding crime activity regulated in Article 18 § 3 of the General Part of the Penal Code.

### ***Criterion 5.9 – (Met)***

78. The assessors confirm the finding of the 4<sup>th</sup> MER (§232) that the “all crime approach” makes TF offences predicate offences for money laundering.

### ***Criterion 5.10 – (Met)***

79. In the absence of any specific limitation, the language of Art. 165a of the CC is sufficiently broad to establish jurisdiction for the TF activity in cases that involves a foreign state element, i.e. different country from the one in which the terrorist or terrorist organisation is located, or the terrorist act occurred or will occur.

### ***Weighting and Conclusion***

80. Since the 4<sup>th</sup> evaluation, the autonomous offence of terrorist financing in the Penal Code (section 165a) has been upgraded. Some shortcomings remain to be covered. Not all acts which constitute an offence within the scope of and as defined in the treaties listed in the annex to the TF Convention are covered by the TF offence. Art. 165a does not cover expressly the indirect funding and the partial use of the funds/ assets and does not distinguish between legitimate or illegitimate source of the funds or other assets. The TF offence does not cover the collection of funds/ assets for terrorist organizations and individual terrorists for any purpose, in which context the terminology used to define “terrorist organisation” and “terrorist” is not fully in line with the FATF Glossary. Furthermore, the restrictive interpretation of the “intention” element by the practitioners and by the judiciary requires that such offences must always be linked to a concrete terrorist act. The financing of travel of individuals for the purpose of providing terrorist training and for receiving a terrorist training without the link to the purpose of committing a terrorist act is not covered. The penalty for acts provided by Art.165a §3 does not have a proportionate and dissuasive character and the scope of criminal liability is limited by the requirement of a prior natural person’s criminal liability. **R.5 is rated Partially Compliant.**

---

the OECD WG on bribery in international business transactions report (para. 157), <https://www.oecd.org/daf/anti-bribery/anti-briberyconvention/38030514.pdf>

## ***Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing***

81. Poland was rated PC for SR. III in the previous round MER. The following deficiencies have been identified: definition of funds did not cover funds controlled by a designated person or persons acting on their behalf or at their direction; absence of a clear legal mechanism which covers designations in Poland with respect to EU internals or other named persons proposed by other countries that were not included on the EU clearinghouse list; no publicly known and clearly defined procedure for de-listing of suspected terrorists listed by Poland; unclear legal basis for monitoring of compliance with some aspects of the AML/CFT Act dealing with terrorist financing issues.

82. As an EU member state, Poland is applying EU legal instruments which implement UNSCRs: Reg. 881/2002 (UNSCR 1267/1989), Reg. 753/2011 (UNSCR 1988) and Reg. 2580/2001 and Common Position 2001/931/CFSP (UNSCR 1373). The mentioned instruments are supplemented at the national level by the application of the provisions of Chapter 10 of the AML/CFT Act, which complements the EU Regulations and overcome the delays still existing in the EU transposition system.

### ***Criterion 6.1 – (Mostly met)***

83. (a) Based on Art. 123 of the AML/CFT Act, the GIFI may request, through the MFA, international organisations (which would include the 1267/1989 and 1988 Committees) to apply restrictive measures to persons and entities.

84. (b) The categories of subjects and the criteria for designations are regulated both at the EU level (Decision 1693/2016/CFSP) and in national legislation (AML/CFT Act). The criteria for designation are in line with the UNSCR. The national mechanism provides that the Financial Security Committee is responsible for identifying targets for designation (the proposal to list a person or entity may be submitted by any member of the Financial Security Committee - representative of the Minister of Justice, Public Prosecutor, Head of Internal Security Agency, GIFI etc. – Art. 20 of the AML/CFT Act) based on a set of criteria (Art. 121), review the designations and make proposals for de-listing if need be (Art. 124).

85. (c) The evidentiary standard of proof of “*justified suspicions*” when evaluating a proposal for designation is stated within the provisions of Art. 120-121 of AML/CFT Act. This can be considered as equivalent to “*reasonable grounds*” as required by the standard. The existence of a criminal proceeding is not a requirement when proposing designations.

86. (d) There is no legal requirement obligating to apply specific standard forms. The Polish authorities maintain that the application of the procedure and standard forms would stem in practice from the UN guidelines and recommendations. Still, this sub-criterion cannot be considered as fully met.

87. (e) Art. 120 (3) of the AML Law provides for the elements to be included in the proposal for designation (*i.a.*, indication of a person or entity against which the decision is to be issued, the justification as well as information and documents confirming the circumstances), which is in line with the requirements of 6.1(e). However, there is no provision specifying whether Poland’s status as a designated state may be made known.

### ***Criterion 6.2 – (Mostly met)***

88. (a) See 6.1 (a)

89. (b) See 6.1 (b)

90. (c) At the Financial Security Committee’s recommendation, the GIFI is responsible

for examining and deciding upon a request of designation pursuant to UNSCR 1373, including from a foreign jurisdiction (Art. 121-122 of AML/CFT Act). There is no requirement that a prompt determination shall be made. To this, the Polish authorities argue that the swift reaction is indirectly underpinned by some provisions of the Regulation of Works of FSC, stipulating that the convening of the FSC meeting requires only the notification of the FSC Chairman sent to its members, the meeting may be delivered to FSC members by means of electronic communication, the possibility to immediately convene FSC meeting in urgent cases. Nonetheless, from a technical point of view, this sub-criterion cannot be considered as fully met.

91. (d) See 6.1 (c)

92. (e) The same type of information needs to be provided to support the designation (see 6.1.(e)).

### ***Criterion 6.3 - (Met)***

93. (a) At the European level, all EU member states are required to provide each other with the widest possible range of police and judicial assistance on TFS matters, inform each other of any actions taken, cooperate and supply information to the relevant UNSC bodies (Art.8 Reg.881/2002; Art.8 Reg.2580/2001; Art.4 CP 2001/931/CFSP). At the national level, the GIFI has the main responsibility of collecting and soliciting information. ISA and the Public Prosecutor's Office are also competent to collect and solicit information to identify persons and entities that meet the criteria for designation.

94. (b) For asset freezing at the EU level, the Court of Justice of the EU makes an exception to the general rule that notice must be given before the decision is taken in order not to compromise the effectiveness of the first freezing order. National legislation also provides exceptions regarding the first instance proceedings concerning the issuance of the decisions regarding listing (Article 61 (4) of the *Act of 14 June 1960 - Code of Administrative Procedure*).

### ***Criterion 6.4 - (Mostly met)***

95. The obligated institutions shall apply specific restrictive measures (freeze assets and refrain from making them available without prior notification of persons – Art. 119 (1)), against persons and entities indicated in the lists announced by the GIFI pursuant to the Resolution of the United Nations Security Council, issued under Chapter VII of the United Nations Charter. The obligation enters into force at the moment of the publication by GIFI. The sanctions lists are published on the GIFI's website immediately after the decision of the United Nations Security Council (Article 118 (2) of the AML/CFT Act), and the lists announced pursuant to the UNSCRs are automatically updated based on changes on the website of UN Committees.

96. Nevertheless, the wording of the legal text mentions “in particular”, the lists referred to in paragraph 3 of Resolution 2253 (2015) of the United Nations Security Council or in paragraph 1 of Resolution 1988 (2011) of the United Nations Security Council. The authorities explained that those were the Resolutions in force at the time of the adoption of the AML/CFT Law with no consequence on the newer Resolutions. Although clearly a technicality, the AT cannot consider this criterion as fully met.

97. The implementation of sanctions stemming from resolution 1373 takes place without delay as at the national level, the decision of the GIFI concerning listing is enforceable with immediate effect (Article 120 (7) of the AML/CFT Act).

### **Criterion 6.5 – (Mostly Met)**

98. (a) According to Article 119 (1) of the AML/CFT Act, the obligated institutions shall freeze assets without prior notification of listed persons or entities. Any information held, associated with the freezing of assets or refraining from making them available shall be provided to the GIFI immediately, in any case not later than within two business days following the day of performing freezing of assets or refraining from making them available. Therefore, the freezing needs to be done “immediately” since it is an action preceding the obligation to inform the GIFI. According to Article 118 (2), after the lists are announced by the GIFI, they shall be published immediately. Under UNSCRs 1373, the obligation to freeze funds and other assets applies immediately to all EU member states and without prior notice. Nevertheless, for the rest of the natural and legal persons that are not reporting entities, the EU mechanism will apply, including the respective delays.

99. (b) The existing EU legal framework (Regulation 881/2002, Regulation 753/2011, and Regulation 2580/2001), as well as the AML/CFT Act (Art. 117 (1, 2) regulates the freezing of all assets owned, held or controlled directly or indirectly by listed persons and entities as well as proceeds derived from such assets. This would include assets owned in any form, including jointly.

100. (c) Under the EU framework Regulations 881/2002 (Article 2 (2)), 753/2011 (Article 3 (2)), 2580/2001 (Article 2 (1(b))) prohibit making funds and other assets available, directly or indirectly, to, or for the benefit of, designated persons and entities. Regarding the domestic sanctions regime, according to Article 117 (2)(2) of the AML/CFT Act, the specific restrictive measures involve refraining from making assets available, directly or indirectly, to listed persons and entities or to their benefit, this also referring to persons and entities owned or controlled, directly or indirectly, by persons or entities suspected of being involved in a terrorist act; and persons and entities acting on behalf of, or at the direction of, such persons or entities.

101. (d) Designations made according to EU regulations are published in the Official Journal of the EU (publicly available on the EURLEX website) and on the website of the European External Action Service (users may subscribe to an automatic alert notification). Based on Art. 118 (2) of the AML/CFT Act, GIFI is obliged to immediately publish the updates of the lists pursuant to UNSCRs after the lists are announced by the GIFI.

102. (e) Art. 119 (2) of the AML/CFT Act requires the obligated institutions to provide to the GIFI immediately any information associated with the TFS, in any case no later than two business days following the freezing of assets or refraining from making them available.

103. (f) EU framework ensures the protection of bona fide third parties, based on the provisions of the Reg. 881/2002 (art. 6), Reg. 753/2011 (art. 7), Reg. 2580/2001 (Art. 4).

### **Criterion 6.6 – (Met)**

104. (a) EU legal framework regulates the procedures to submit de-listing requests to the Office of the Ombudsperson of the UN Security Council (Al-Qaida and ISIL designations) and the Focal Point for de-listing (Taliban designations). In line with *‘Update of the EU Best Practices for the effective implementation of restrictive measures’*, petitioners can submit de-listing requests also through the Focal Point established by UNSCR 1730(2006) to receive such requests. Petitioners whose names are inscribed on the Al-Qaida Sanctions List can submit their de-listing requests through the Office of the Ombudsperson (paragraph 23 Item Note 8519/18). At national level, the FSC is responsible for proposing on listings and de-listings, and any of the members of the Committee can raise any related issue within the Committee. The GIFI is responsible for

examining and deciding upon any such request. According to Art. 122 of AML/CFT Act, a request can be submitted through the minister competent for foreign affairs by entities referred to in Article 12(1)(9) of AML/CFT Act.

105. (b) At the EU level, it is mandatory to review the list of targeted persons (entities) at regular intervals and at least once every six months to ensure that there are grounds for keeping them on the list. At the domestic level, the Financial Security Committee shall assess the circumstances justifying further need to apply the specific restrictive measures against persons or entities entered into the domestic sanctions list on a semi-annual basis (Article 124 of the AML/CFT Act).

106. (c) According to EU legislation, designated persons and entities may challenge the EU act imposing relevant sanctions by instituting proceedings (according to Article 263 (4) and Article 275 (2) TFEU) before the EU Court of Justice, regardless of whether the designation was initiated by the EU on its own motion, or pursuant to UN sanctions. At the domestic level, Article 120 (9) of the AML/CFT Act guarantees that decisions of the GIFI concerning the listing may be appealed against to the minister competent for public finance within 14 days following the day of submission of the notification of a party on the decision.

107. (d, e) The designated persons and entities are notified of their designation and the right to request a review of the designation, according to Art. 120 (5) and (8) of the AML/CFT Act. At the EU level, there are procedures that provide for de-listing, unfreezing funds and reviewing designation decisions by the EU Council. Interested parties may submit their requests directly to the above-mentioned EU and UN institutions (EC Regulation 753/2011, Art.11; EC Regulation 881/2002, Art.7a and 7e).

108. f) Article 119 (3) AML/CFT Act provides that in case the GIFI receives information on the application of restrictive measures against a person or an entity that are not specified in the lists, it shall issue the decision on the unfreezing of assets or on making them available. The EU Best Practices for the effective implementation of restrictive measures procedures constitute publicly known procedures for persons inadvertently affected by a freezing mechanism.

109. g) Mechanisms for communicating de-listings are the same as in the case of designations. The procedure provided in Art. 118 (2) applies to all obligations related to application of financial sanctions. See criterion 6.5(d).

#### ***Criterion 6.7 – (Met)***

110. Both the EU and domestic level, there are mechanisms for authorising access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses, or for extraordinary expenses. Article 127 (1) of the AML/CFT Act provides that unless contrary to the objective of counteracting terrorism and financing of terrorism, upon request, the GIFI shall issue the permit to use assets for basic expenses and payment of certain types of fees as provided by UNSCR 1452.

#### ***Weighting and Conclusion***

111. Most of the requirements of Recommendation 6 are Met. Minor deficiencies remain in relation to: the legal requirement to apply specific standard forms on designation; absence of clear provision specifying whether Poland's status as a designated state may be made known; absence of requirements on a "*prompt designation*" in case of designations made according to 1373; delays in the implementation of the EU mechanism in case of natural and legal persons other than REs. **R.6 is rated Largely Compliant.**

## ***Recommendation 7 – Targeted financial sanctions related to proliferation***

112. These requirements were added to the FATF Recommendations in 2012 and were therefore not previously assessed. As an EU Member State, Poland implements UNSCRs through the EU legal framework.

### ***Criterion 7.1 – (Mostly met)***

113. At the EU level, UNSCR 1718 and successor Resolutions on the Democratic People's Republic of Korea (DPRK) is transposed into the EU legal framework (the current legislative framework is based on Council Decision (CFSP) 2016/849 and Regulation (EU) 2017/1509)). UNSCR 2231 on Iran is transposed into the EU Legal framework through EC Regulation 267/2012 as amended by EC Regulations 2015/1861 and 1862. EU regulations and the UNSCRs are directly applicable in Poland. Delays related to the transposition of DPRK designations can still occur.

### ***Criterion 7.2 – (Mostly met)***

114. The Minister of Foreign Affairs (the Legal and Treaty Department) is the competent authority for coordination of implementation of international provisions regarding targeted financial sanctions. (<https://www.gov.pl/web/diplomacy/international-sanctions>). In line with Article 105(3)(4) of the AML/CFT Act, the GIFI shall make available the information in his/her possession on a written and justified request of the Minister of Foreign Affairs – in the scope of the statutory competence of the MFA in connection with the application of specific restrictive measures.

115. (a) In its Art. 34, EU Regulation 1509/2017 and Regulation 267/2012 provide that all funds and economic resources belonging to, owned, held or controlled by the persons, entities and bodies listed in relevant annexes (XIII, XV, XVI and XVII) should be frozen. This obligation is triggered as soon as the regulation is approved and the designation published in the Official Journal of the European Union. With respect to the moment of entry into force of the UNSCRs, the obligation to freeze takes place after a prior confirmation at the EU level.

116. (b) The relevant EU legislation covers the requirement to freeze all types of funds or other assets as targeted by the FATF Methodology. Annexes (XIII, XV, XVI and XVII) to Regulation 1509/2017 cover persons and entities designated by the Sanctions Committee or the UNSC as well as additional persons and entities autonomously indicated by the EU. Also, EU Regulation 267/2012 lays down the obligation to freeze all funds and economic resources belonging to, owned, held or controlled by the persons, entities and bodies listed in Annex XIII and Annex XIV to the Regulation. Annex XIII to Regulation 267/2012 includes the natural and legal persons, entities and bodies designated by the UN Security Council in accordance with paragraph 6(c) of Annex B to UNSCR 2231 (2015).

117. (c) According to existing EU regulations (267/2012, 1509/2017) is prohibited from making available, directly or indirectly, funds or economic resources to designated persons or entities or for their benefit, unless otherwise authorised or notified in compliance with the relevant UNSCRs.

118. (d) All EU regulations and sanctions lists are published in the Official Journal of the EU available through the internet. Relevant information regarding the international sanctions regime is also publicly available on the website of the Ministry of Finance and Ministry of Foreign Affairs, providing information about UN and EU regimes, as well as sanctions of third countries. No specific Guidance is provided.

119. (e) According to EU regulations (267/2012, 1509/2017), all natural and legal persons, entities and bodies are required to supply immediately any information which would facilitate compliance with the regulations, such as accounts and amounts frozen, to the competent authorities of the Member States. There is no domestic provision to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

120. (f) The rights of bona fide third parts are protected by the EU legal framework (267/2012, 1509/2017) according to which actions by natural or legal persons, entities or bodies shall not give rise to liability of any kind on their part, if they did not know, and had no reasonable cause to suspect, that their actions would infringe the measures set out in this regulation.

**Criterion 7.3 – (Not met)**

121. Under the EU Regulations 267/2012 (Art. 47) and 2017/1509 (Art. 55), EU Member States must take all necessary measures to implement EU regulations, which would include adopting measures to monitor compliance with the sanctions regime by FIs and DNFBPs.

122. According to the GIFI's *Control procedure of 16 January 2019*, the controllers shall examine the way the obligated institution fulfils the AML/CFT duties, including the application of customer due diligence measures and provisions of Article 43 of the AML/CFT Act, which in turn makes specific reference to the transactions with a state in relation to which the UN or the EU made the decision on imposing sanctions or specific restrictive measures. Any obligated institution which fails to fulfil its obligations provided by Art. 33-43 of the AML/CFT Act shall be subject to administrative penalty. Nevertheless, the controls and the sanctions are limited to the application of the enhanced CDD measures (Art 43) and do not extend to the application of freezing requirements.

123. Part of UKNF activities during the inspection process includes control of compliance with requirements regarding suspension of transactions, blocking accounts, freezing and refraining from making assets available. There is no specific PF UNSCRs provision in the AM/CFT Act or elsewhere.

**Criterion 7.4 – (Mostly Met)**

124. Article 47 of the EU Regulation 1509/2017 provides that where the Security Council or the Sanctions Committee lists a natural or legal person, entity or body, the Council shall include such natural or legal person, entity or body in Annex XIII and XIV. Where the United Nations decides to de-list a natural or legal person, entity or body, or to amend the identifying data of a listed natural or legal person, entity or body, the Council shall amend Annexes XIII and XIV accordingly. In accordance with Article 47a of the EU Regulation 1509/2017, the Annexes are reviewed at regular intervals and at least every 12 months and include the grounds for the listing of persons, entities and bodies concerned. However, besides the procedures available at EU level, there is no mechanism developed at domestic level. Since the criterion requires that “*in the view of the country*”, the listed persons do not or no longer meet the criteria for designation, the EU Regulations cannot be considered as sufficient for the criterion to be fully met.

125. (a) As stated in ‘update of the EU Best Practices for the effective implementation of restrictive measures’ (paragraphs 18-20 in document 8519/18), individual requests for de-listing should be processed, as soon as they arrive, in accordance with the applicable legal instrument and “EU Best Practices for the effective implementation of restrictive measures”. The General Secretariat of the Council acts as a mailbox for de-listing requests, and petitioners can submit de-listing requests also through the Focal Point established by

UNSCR 1730(2006) to receive such requests (paragraph 23 in document 8519/18).

126. (b) Publicly known procedures are available for obtaining assistance in verifying whether persons or entities are inadvertently affected by a freezing mechanism having the same or similar name as designated persons or entities (*i.e.* a false positive), mainly provided within the “Update of the EU Best Practices for the effective implementation of restrictive measures”.

127. (c) At the EU level, there are specific provisions for authorising access to funds or other assets, where the competent authorities of Member States have determined that the exemption conditions set out in UNSCRs 1718 and 1737 are met, and in accordance with the procedures set out in those resolutions (Regulation 1509/2017, Regulation 267/2012).

128. All EU regulations and sanctions lists are published in the Official Journal of the European Union and are available online. Relevant information regarding international sanctions regimes is publicly available on the website of the Ministry of Finance, providing information about UN and EU regimes, as well as sanctions of third countries. In this context, the procedures set out in C.6.5 (d) are equally applicable to any changes to EU listings, which will be given effect by a Council Regulation or a Council/Commission Implementing Regulation.

#### ***Criterion 7.5 – (Met)***

129. (a) Relevant EU framework (Article 34 of the Regulation 1509/2017, Article 29 (1) of the Regulation 267/2012) do not prevent financial or credit institutions in the Union from crediting frozen accounts where they receive funds transferred by third parties to the account of a listed natural or legal person, entity or body, provided that any additions to such accounts will also be frozen. The financial or credit institution shall notify the competent authorities about such transactions without delay.

130. (b) Regulation 267/2012 authorises the payment of sums due under a contract entered into prior to the designation of such person or entity if the payment does not contribute to an activity prohibited by the Regulation, and after notice is given to the UN Sanctions Committee.

#### ***Weighting and Conclusion***

131. Most of the essential criteria are met or mostly met. Moderate shortcomings remain in relation to delays in the implementation of TFS on PF and in relation to the monitoring mechanism: although obligatory through the EU Regulations, the implementation of the PF TFS is not enforceable by means of domestic supervision, and countermeasures cannot be applied in case of failures in the implementation of the TFS. **R.7 is rated Partially Compliant.**

#### ***Recommendation 8 – Non-profit organisations***

132. Poland was rated PC with former SR.VIII. The main deficiencies were: limited review of the risks in the NPO sector; steps taken to enhance financial transparency and reporting structures do not amount to effective implementation of the essential criteria VIII.2 and VIII.3; lack of effective and proportionate oversight of the NPO sector.

#### ***Criterion 8.1 – (Partly met)***

133. (a) According to the NRA, the subset of organisations, which fall within the FATF definition include all foundations and associations. They could be obliged entities under

the conditions provided by the art. 2 of the AML/CFT Act. Both are classified as NGOs<sup>84</sup> and, as such, have the possibility to apply for the status of a public benefit organisation or benefit from subsidies from public administration. Nevertheless, the categories of NPOs identified are very general, and there is no particular risk assessment to identify the features and types of NPOs that, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse.

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

135. (c) There was no review of the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for terrorism financing support in order to be able to take proportionate and effective actions to address the risks identified.

136. (d) The reassessment of the sector’s potential vulnerabilities to terrorist activities is to be conducted at least on a biannual basis or whenever necessary in the context of the NRA. At EU level, the regular review of new information and assessment of the sector is executed through the SNRA, which, based on Article 6(1) of the Directive 2015/849, shall be updated every two years, or more frequently if appropriate. So far, information on threats and vulnerabilities related to the non-profit sector has been included both in the 2017 and 2019 assessments. However, in practice, no reassessment has been carried out since the sector has not been subject to an initial assessment.

### ***Criterion 8.2 – (Partly met)***

137. (a) There are some provisions to promote accountability, integrity and public confidence contained in the legal acts governing the NPOs<sup>85</sup>. Art. 10(5) of the Law on Associations provides that the “authorities” of the association, the procedure for their election, the method of electing supplementary authority members and their “competences” should be written in the association statute. Associations must have a management board and an internal control authority. Nevertheless, there is no referral to any integrity requirements applicable to the administration and management of the associations. Turning to foundations, the “sponsor” shall determine its statute, its name, address, assets, purposes, principles, forms and scope of activity, composition and organisational structure of governing board, and the procedure for appointing members of that body, as well as the responsibilities and powers of that body and its members. As in the case of associations, no integrity requirements are applicable to the administration and management. There are no policies to promote accountability, integrity, and public confidence in the administration and management of NPOs. The establishment of bodies such as the National Institute of Freedom, the Public Benefit Committee, Council of Public Benefit Work might be considered as steps to promote accountability, integrity and public trust in the NPO sector, as they have prerogatives indirectly related to accountability, integrity and public confidence such as “*creating mechanisms for the provision of information on standards of public benefit organisations and on identified cases of breaches*”

---

<sup>84</sup> Pursuant to Article 3(2) of the *Act of 24 April 2003 on public benefit activity and volunteering*.

<sup>85</sup> Act of 7 April 1989 - Associations Law, the Act of 6 April 1984 on Foundations and the AML/CFT Act.

*of these standards*". Nevertheless, the mere establishment of such advisory and coordination bodies but cannot be considered as fully meeting the requirements of 8.2.

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

139. (c) In 2020, the GIFI organised workshops dedicated to methods of strengthening co-operation between non-profit organisations, the banking sector and other competent bodies in the AML/CFT area. However, this does not amount to developing and refining best practices to address terrorist financing risk and vulnerabilities and thus protect them from terrorist financing abuse as required by 8.2(c).

140. (d) The introduction of associations and foundations performing cash payments equal to or exceeding the equivalent of €10 000 (regardless of whether the payment is performed as a single operation or as several operations which seem linked to each other) to the catalogue of obliged entities gives an impulse to conduct non-cash transactions through financial institutions. Several activities promoting cashless transactions in Poland have been carried out by public administration and private entities, participants of the market of payment services, commercial banks and cooperative banks. The projects concerned the NPO sector, among others.

### ***Criterion 8.3 – (Mostly Met)***

141. The existing legal framework, in particular the AML/CFT Act, provides a mechanism for risk-based supervision and monitoring of the NPO sector, including from the perspective of potential TF abuse. However, since the NRA is deficient in identifying the features and types of NPOs which by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse, the implementation of a risk-based approach is difficult to be applied in practice, and hence, this EC cannot be considered as being fully met.

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

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

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

established and includes financial accountability.

***Criterion 8.4 – (Mostly Met)***

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

146. The AML/CFT control over the activity of associations and foundations is exercised by the GIFI, with the involvement of other competent authorities if need be. The control shall be performed based on annual control plans of GIFI, UCS, Ministries, voivodes and governors of districts. However, the deficiencies concerning the NPO sector risk assessment, this EC cannot be considered as fully met.

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

***Criterion 8.5 – (Mostly met)***

148. (a) General provisions regarding information sharing are specified in the Regulation of the Chairman of the Public Benefit Committee on the exchange of information concerning public benefit organisations of 25 October 2018. This mainly concerns the Minister of Justice, the Director of NIF, the minister competent for public finance in relation to public benefit organisations. More specific and complex mechanisms of co-operation between the competent authorities seem to be lacking.

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

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

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

coordination, the ISA collects, processes and analyses different types of information which are i.a linked to the NPOs activities.

#### ***Criterion 8.6 – (Met)***

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

#### *Weighting and Conclusion*

153. Moderate shortcomings remain in respect of: the assessment of features and types of NPOs which, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse, with a negative impact on the risk-based supervision; no review of the adequacy of measures, related to the subset of the NPO sector that may be abused for terrorism financing; limited involvement of the NPO sector in any activity to develop and refine best practices to address FT risks; no specific and complex mechanisms of co-operation between the competent authorities. **R.8 is rated Partly Compliant.**

#### ***Recommendation 9 – Financial institution secrecy laws***

#### ***Criterion 9.1 – (Met)***

154. The following items are assessed in order to determine whether the confidentiality provisions in the Polish legal regime have an impact on the application of the FATF Recommendations, in particular, the pursue of CDD obligations:

##### **(a) *Access to information by competent authorities***

155. According to article 96(1) of the AML/CFT Act, any restrictions concerning the disclosure of classified information or data do not apply when disclosing information to the GIFI in the manner and scope provided by the Law.

156. The article provides an exception concerning the provisions on the protection of classified information, which prevail when compared with the aforementioned article of the AML/CFT Act. However, it should be noted that it is applicable to the exchange of information with the GIFI in general terms (both from OIs and other authorities), and the application of this article will not impede the submission of the information to the GIFI, although the measures on the protection of classified information will have to be applied.

157. According to articles 104(2)(7)-(7a) and 106(1)(3) of the Banking Act, the UKNF can freely exchange information protected by the banking secrecy laws for AML/CFT purposes. In particular, it is stated that “*a bank shall be obliged to disclose information that is subject of banking secrecy exclusively at the request of the UKNF, (...) employees of the UKNF, (...) and persons authorised by resolution of the UKNF, to the extent defined in the respective authorisation.*” The last part of the article referring to “authorised persons” mainly include cases of employers of the Office of the Commission (UKNF) on the basis of specific task contracts, contracts of mandate or other contracts of similar nature as established in Article 16 of the UKNF Act.

158. Similarly, the financial institutions that are part of the capital markets sector (including both the trading in financial instruments and investment firms), as well as the payment institutions, are also obliged to promptly prepare and deliver all the copies of documents and other information and explanations that are requested by the UKNF, so that it can exercise effective supervision. This obligation is provided by article 88 of the Act on the trading in financial instruments and Article 225(2) of the Act on investment funds, as well as Article 102 of the Act on payment services. None of these provisions, however, make reference to secrecy or confidentiality laws and their relation to them in terms of hierarchy.

159. In relation to the cooperative savings and credit union sector, article 9(f)(1) of the Act of 5 November 2009 on Cooperative Savings and Credit Unions, the duty to keep professional secrecy will not be breached when transferring information covered by professional secrecy to the KNF or the NACSU, at their request.

160. The insurance sector is explicitly not bound to preserve secrecy on the information furnished upon request by *“the supervisory authority”*, according to article 35 of the Act on insurance and reinsurance activities.

161. FIs are allowed to disclose information protected by banking secrecy laws to the authorities relevant in terms of AML/CFT, including the GIFI (as established by Article 76 of the AML/CFT Act), the UKNF and the NACSCU. It should be noted that the submission of information to the authorities must be complied with whenever it is requested. In the case of the UKNF the information request must be integrated within the scope of its supervisory framework and functions (in general terms, not just banking supervision) but is not bound to a particular inspection or supervisory activity. Furthermore, all these provisions reiterate that the submission of information is to be understood within the framework of the supervisory activity of those authorities.

162. The analysis above demonstrates that the competent authorities have access to information held by FIs.

(b) *Sharing of information between competent authorities*

163. The AML/CFT Act provides cases when the GIFI can exchange information with national authorities. The GIFI is obliged to make available the information in his/her possession on a written and justified request of the authorities listed in article 105 of the AML/CFT Act, with the exception of the cases when might negatively affect the analysis related to ML/TF suspicious or exposing a natural or legal person to disproportionate damage.

164. Regarding the UKNF, information, including classified, may be exchanged with the NBP and the Bank and Insurance Guarantee Funds to the extent necessary for the performance of their statutorily defined responsibilities, according to Article 17 of the Act of Financial Market Supervision.

165. As for the NBP, the results of their inspections are systematically shared with the GIFI, pursuant to Article 131(5)(3) of the AML/CFT Act, which establishes a specific period of 14 days since the completion of the control or the issuance (when applicable) of recommendations to share the results. However, it is unclear whether the provision limits itself to controls to currency exchangers. NBP also provides information upon request to law enforcement authorities.

166. Finally, the NACSU, within the scope of the AML/CFT regime, provides to the GIFI and KNF a yearly inspection plan, as well the results of the onsite inspections and other relevant information, according to Articles 63 to 70 of the CSCUs Act and Article 131 of the AML/CFT Act. The flow of information is bilateral, as the UKNF also informs NACSCU about

the recommendations made to CSCUs (according to Article 69.10 of the CSCUs Act) and the GIFI provides information to NACSCU regarding areas and sectors particularly exposed to ML/TF risks (according to Article 132.2).

(c) *Sharing of information between FIs*

167. The sharing of information between FIs include:

- those cases where the application of CDD measures is delegated to third parties, according to article 47 of the AML/CFT Act.
- Between the FIs referred to in Article 54(2)(1) and 54(2)(2) and their branches and subsidiaries included in the group or persons from third equivalent countries who perform their professional activities within the same legal person or a structure that has a common owner, management board or compliance control with the AML/CFT provisions.
- Between the FIs referred to in Article 54(2)(4) and their corresponding institutions established in a third equivalent country.

168. In the last two cases, the FIs are not obliged to keep confidentially, thus allowing for the exchange of information, unless the GIFI explicitly tells otherwise, as stated by article 54(3).

***Weighting and Conclusion***

169. In general terms, the Polish legal regime allows for access to information of the main competent authorities that deal with FIs, thus ensuring that the application of the FATF Recommendation is not hampered. **R.9 is rated Compliant.**

***Recommendation 10 – Customer due diligence***

170. In the 2013 MER, Poland was rated partially compliant with former R.5. The assessment identified technical deficiencies related to the lack of requirement to identify the beneficial owner, to verify the authorisation of any person who acts on behalf of a legal person, to use reliable and independent sources for the verification and to establish the source of funds when conducting ongoing due diligence on the business relationship. The availability of exemptions from CDD in some cases of simplified CDD and deficiencies in CDD requirements regarding wire transfers were also noted in the analysis.

***Criterion 10.1 – (Mostly Met)***

171. Although there is no specific legal provision prohibiting FIs from keeping anonymous accounts or accounts in obviously fictitious names, FIs are obliged to pursue CDD measures, including customer identification, whenever establishing a new business relationship, thus ensuring no anonymous bank accounts can be kept.

***Criterion 10.2 – (Mostly Met)***

172. Article 35(1)(1) of the AML/CFT Act establishes the obligation for all reporting entities to conduct CDD measures whenever establishing a business relationship.

173. The obligation to conduct CDD measures on occasional transactions above the applicable threshold, including situations where the transaction is carried out through operations that appear to be linked, is set in article 35(1)(2a). The article establishes a threshold of €15 000.

174. According to Article 35(1)(2b), CDD must also be pursued when performing occasional transactions that constitute a transfer of funds, where the amount exceeds €1

000. This constitutes a deficiency, as R.16 requires wire transfers amounting to €1 000 also to be subjected to CDD. However, it is not specified if the obligation applies to both domestic and cross-border transactions.

175. CDD must be applied in all cases where there is suspicion of money laundering or financing of terrorism, according to Article 35(1)(5) of the AML/CFT Act.

176. Article 35(1)(6) sets up the requirement for obligated institutions to conduct CDD measures whenever there are doubts regarding the authenticity or the completeness of customer identification data obtained up to that point.

***Criterion 10.3 – (Met)***

177. Article 34(1)(1) sets the identification of a customer and verification of its identity as one of the CDD measures that obligated institutions must perform. Customer is defined in Article 2(10), where it is specified that includes both natural and legal persons, as well as organisational units without legal personality.

178. Article 37 provides that the verification of the identity must be determined based on a document that confirms the identity of a natural person, a document containing valid data from the extract of the relevant register (it is understood that it is applicable to legal persons) or other documents, data or information that also originate from a reliable and independent source.

***Criterion 10.4 – (Met)***

179. Article 36(3) sets the requirements to identify a person authorised to act on behalf of the customer (which are the same ones as for the customer who is a natural person, established in article 36(1)(1)). Furthermore, article 34(2) establishes that obligated institutions must not only identify and verify the identity of the person acting on behalf of the customer but also verify that the person is authorised to do so.

***Criterion 10.5 – (Met)***

180. The obligations for reporting entities to identify the beneficial owner and take measures to verify its identity are set in Article 34(1)(2) of the AML/CFT Act, which requires that the identification and verification of identity must be carried out based on documents, data or information gathered from reliable and independent sources.

181. Article 36(2) establishes the documents required to identify the beneficial owner, which matches those used to identify customers that are natural persons.

***Criterion 10.6 – (Met)***

182. Article 34(1)(3) requires obligated institutions to assess the business relationship and, as such, obtain information concerning its objective and intended nature.

***Criterion 10.7 – (Mostly met)***

183. Article 34(1)(4)(a) and(b) establish the obligation to analyse transactions carried out throughout the course of the business relationship in order to ensure that they are coherent with the knowledge the obligated institution has on the customer, the type and scope of its activity and its ML/TF risk. The obligation to examine the origin of the funds available to the customer is there included too.

184. Article 34(4) (c) requires obligated institutions to ensure that any documents, data or information concerning the business relationship with the customer are updated on an ongoing basis. However, the requirement to review existing records to ensure they remain relevant and the enhanced focus that needs to be put on categories of higher risk customers are not included in this provision.

***Criterion 10.8 – (Mostly Met)***

185. The requirement to define the ownership and control structure of customers that are legal persons or organisational units without legal personality is established by Article 34(1)(2)(b) of the AML/CFT Act. However, being able to define which is the ownership structure of a customer does not necessarily amount to understanding it, nor the nature of its business, therefore the criterion is not fully met.

***Criterion 10.9 – (Partly met)***

186. Article 36(1)(2)(a) and (b) establish that, in order to identify a customer that is a legal person or arrangement, the obligated institution must determine its name and organisational (or legal) form. Letter d of the same article establishes the obligation to obtain the TIN and/or evidence of registration in the commercial register. The extract of the National Court Register includes notes on submission of annual financial statements, references of submission of audit reports, mentions of the submission of the report on conducted activities or references to the submission of the report on necessary payments to the public administration, all of the elements which can prove the existence of the legal person or arrangement.

187. Article 36(1)(2) requires identification of the representatives of the legal person or arrangement, as set in letter e) but does not require to identify the persons having senior management positions, nor the powers that regulate the legal person or arrangement.

188. The obligation to determine the address of the registered office or the address of pursuing the activity when identifying the customer is established by Article 36(1)(2)(c).

***Criterion 10.10 – (Met)***

189. Article 36(1)(2) sets the requirements to identify the beneficial owner, which match those to identify a customer that is a natural person (except for the identification of the economic activity set in Article 36(1)(1)(f)).

190. The definition of beneficial ownership contained in Article 2(2)(1) states, in letter a), that the natural person that has a controlling ownership interest in a legal person would be the stakeholder or shareholder holding the ownership title of more than 25% of the total number of stakes or shares of such legal person.

191. Article 2(2)(1)(a) also determines other cases in which a person can have a controlling interest of a legal person besides the ownership of more than 25% of its shares/stocks. In particular, assumptions of control through other means in this article include holding more than 25% of the total number of votes in the governing body of the natural person, exercising control over a legal person or persons who hold the ownership of more than 25% of the stocks/shares of the legal person's governing body or the exercise of control through powers defined in the Accounting Act, amongst others.

192. The consideration of beneficial owner to the natural person holding a senior management position is also established by Article 2(2)(1)(a), in the events of documented lack of possibility to determine the identity, or doubts regarding the identity, of the natural persons defined in the other assumptions of the article, already explained in this criterion, as long as there are no ML/TF suspicions.

***Criterion 10.11 – (Mostly met)***

193. The obligation to identify and verify the identity of the beneficial owner is established in Article 34(1)(2), and Article 36 defines the requirements to do so; in particular, section 2 addresses the organisational units without legal personality (legal

arrangements). The definition of beneficial owner in Article 2(2)(1)(a) explicitly mentions the figures that must be considered beneficial owners of the trust and, as a result, must be identified as part of the CDD measures.

194. These include the founder (settlor), the trustee, the supervisor (protector), the beneficiary and any other (natural) persons exercising control over the trust. The definition does not explicitly include the possibility of beneficiaries designated by characteristics or class, nor the assumption for which a person can be considered to have effective control over the trust.

195. Unlike trusts, the definition of beneficial owner set in Article 2(2)(1)(a) does not directly address other types of legal arrangements (or organisational units without legal personality, as referred to in the AML/CFT Act). Although the general definition of beneficial ownership is any natural persons(s) who exercise directly or indirectly control over a customer, the fact that legal arrangements are not directly covered does not allow other figures akin to the settlor, the protector, the trustees or the beneficiary (if applicable for that particular type of arrangement) to be included and, therefore, subject to obligation of identification.

***Criterion 10.12 - (Met)***

196. According to Article 40(1) of the AML/CFT Act, the insurance companies shall apply the CDD measures referred in Article 34(1)(1) (identification and verification of the identity of the customer) to the beneficiaries of the insurance agreement as well. Article 36(1)(a) and(2)(a) require, for the identification, to determine the name of the natural or legal person.

197. As the stated Article 40(1) establishes, the CDD measures to beneficiaries of life insurance policies must be undertaken immediately upon determining the beneficiaries of the insurance agreement, which can be upon the payment of the benefit of the agreement, at the latest.

***Criterion 10.13 - (Partly met)***

198. The AML/CFT Act contains the obligation (Article 46(3)) to determine whether the beneficiaries or their beneficial owners are PEPs (at the time of the payment of the benefit at the latest) or, when a higher level of ML/TF risk is identified (irrespective of whether the beneficiary is a legal person or arrangement), adopt enhanced measures limited to an in-depth analysis of the business relationship and to inform senior management before proceeding to the payout (Article 46(4)). Therefore, the consideration of the beneficiary of the insurance agreement as a risk factor when determining the application of enhanced due diligence is not covered, nor the obligation to identify and verify the identity of the beneficial owner of the beneficiary when the beneficiary is a legal person or arrangement that poses a higher risk.

***Criterion 10.14 - (Met)***

199. Article 35(1)-(4) provides that CDD measures must be conducted when establishing a business relationship or performing an occasional transaction. While the AML/CFT legal framework does allow for completing the verification of the identity of the customer or the beneficial owner during the establishment of the business relationship (Article 39(2)) or constitute a bank, securities or omnibus account before concluding the CDD process (but not operate through those accounts, as set by Article 39(2)), it does not allow for deferments in the application of CDD after the establishment of the business relationship.

200. a) In the cases established in Article 39(2) (that is, when the verification can be

concluded during the establishment of the business relationship), the verification shall take place as soon as possible after the commencement of the business relationship.

201. b) Article 39(2) can only be applied when the deferment of the verification is necessary to ensure the adequate conduct of the economic activity.

202. c) Similarly, the postponement in the identification and verification of the identity of the customer envisaged by Article 39(2) can only take place when the risk of money laundering and terrorist financing is low.

***Criterion 10.15 - (Met)***

203. As stated in criterion 10.14, there are no possibilities to utilise a business relationship prior to verification of the identity of the customer. The cases in which the verification can be concluded while establishing the business relationship are covered as well in c10.14 and are only applicable where it is determined that the ML/TF risk is low. Regarding the settlement of bank, securities and omnibus accounts that Article 39(3) allows, the risk management measure established in the same article consists in not allowing any transaction to be conducted through those accounts until the verification of the identity can be concluded.

***Criterion 10.16 - (Met)***

204. Article 35(2) of the AML/CFT Act establishes the obligation to also apply CDD measures in relation to customers with whom obligated institutions already maintain a business relationship, taking into consideration the identified risk of money laundering and terrorist financing and, in particular, in those situations when a change in the formerly determined nature of the circumstances of the business relationship occurs.

***Criterion 10.17 - (Met)***

205. Article 43(1) states that obligated institutions shall apply EDD in cases of higher risk of money laundering or terrorist financing (section 2 of the same article determines certain circumstances that, in particular, entail a higher risk of ML/TF), as well as in the cases of article 44 (persons originating or established in high-risk third countries) and 46 (PEPs).

***Criterion 10.18 - (Met)***

206. Obligated institutions can apply SDD where they have determined there is a low risk of ML/TF in accordance with Article 42 of the AML/CFT Act. Article 42(2) determines a series of assumptions that would constitute low ML/TF risk scenarios, and, therefore, where SDD could be applied, based on the annexes of the EU AMLD (such as certain types of electronic money or investment funds as stated in article 42(2)(5)). On top of that, OIs themselves need to assess and justify the low-risk scenario in order to be able to apply SDD. Furthermore, it is explicitly stated in Article 42(3) that SDD cannot be applied when there is suspicion of ML/TF (Article 35(1)(5)) or there are doubts regarding the authenticity or completeness of the CDD identification data obtained up to that point (Article 35(1)(6)).

***Criterion 10.19 - (Met)***

207. a) According to Article 41(1) of the AML/CFT Act, the obligated institution shall not establish a business relationship (open an account), perform an occasional transaction, conduct transactions through an account and terminate a business relationship when it is unable to apply any of the CDD measures defined in Article 34(1).

208. b) As stated in Article 41(2), the obligated institution, when unable to apply any of the CDD measures, shall also, according to Article 41(2), assess whether a notification of

this fact should be made to the GIFI, pursuant to Article 74 (reporting of circumstances suspicious to entail ML/TF) or 86 (reporting of suspicious transactions being related to ML/TF).

#### **Criterion 10.20 – (Not met)**

209. There is no specific provision in the AML/CFT Act that permits obliged institutions not to pursue CDD processes in the case they reasonably believe this will tip off the customer.

#### **Weighting and Conclusion**

210. The AML/CFT legal framework of Poland largely complies with the CDD requirements. Certain shortcomings exist, such as the non-explicit prohibition of anonymous or fictitious accounts in c.10.1, no CDD obligations for some low-value occasional transactions, the absence of a requirement to obtain proof of existence of customers that are legal persons in c.10.9 or non-consideration of other legal arrangements besides trusts in c.10.11, amongst other minor shortcomings related to the full implementation of 10.13 and 10.20. **R.10 is rated Largely Compliant.**

#### **Recommendation 11 – Record-keeping**

211. In the 2013 MER, Poland was rated largely compliant with former R.10. The assessment identified technical deficiencies related to the limited ability for authorities to ask obliged institutions to keep records beyond five years and the absence of the requirement to retain business correspondence.

#### **Criterion 11.1 – (Met)**

212. According to Article 49(1) of the AML/CFT Act, *“the obliged institutions shall keep the following documents (...): evidence confirming conducted transactions and transaction records comprising original documents or copies of documents required to identify the transaction”*. The period of five years that is mentioned in this article is calculated from the first day of the year in which the business relationship with a given customer is terminated, or the occasional transaction is conducted, thus complying with the minimum requirement of this criterion of “at least five years”. Furthermore, article 49(3) of the same law allows for the extension of this period for up to five additional years if the GIFI requires so for AML/CFT purposes.

#### **Criterion 11.2 – (Partly Met)**

213. As stated in the previous criterion, article 49 of the AML/CFT Act establishes the types of documentation and records that obliged entities must keep and the period during which they must be maintained. Section 1 of Art. 49 of the AML/CFT Act makes explicit reference to *“copies of documents and information obtained as a result of the application of customer due diligence measures”*. It should be noted that, according to article 34, CDD measures encompass the identification and verification of the identity of the customer and the beneficial owner, the assessment of the objective and intended nature of the business relationship and the ongoing monitoring of the relationship, including the analysis of transactions. As also explained above, the period of retention specified in Article 49 (1) is compliant with the minimum required by this Recommendation.

214. The scope of the analyses of 34(3) covers both documentation of CDD measures and ongoing analysis of transactions (understood as separate from the ongoing monitoring of the business relationship, which also includes analysis of transactions, of Article 34(1)(4), within the scope of CDD). As a result, only records obtained through CDD

and evidence of transactions would be covered by an appropriate record-keeping period according to this criterion, as this is the scope of Article 49(1), not covering analyses undertaken of any kind.

215. Section 2 of Article 49 makes direct reference to “*the results of the analyses referred to in Article 34(3) over a period of 5 years, as of the first day of the year following their conducting*”. Article 34(3) refers to both the documentation of CDD measures applied, as well as the results of the ongoing analysis of transactions. Article 49(2) is not in line with the criterion, nor with section 1 of the same Article, as it states the period of 5 years to start counting from the day that particular analysis was conducted and not from the day of termination of the business relationship or occasional transaction. Although the scope of the analyses of 34(3) is broader than the ongoing monitoring within the scope of CDD, such analyses must also be kept during the period required by this criterion. Furthermore, these provisions could lead to documentation of CDD measures applied and analysis related to the ongoing monitoring of transactions not being kept the required minimum amount of time.

#### ***Criterion 11.3 – (Mostly met)***

216. As stated in c.11.1, Article 49(1)(2) of the AML/CFT act requires to keep “*evidence confirming conducted transactions and transactions records comprising original documents or copies of documents required to identify the transaction*”. However, there is no specific provision requiring that this evidence and transaction records subject to record-keeping requirements have to be sufficient to permit reconstruction of individual transactions.

#### ***Criterion 11.4 – (Met)***

217. Article 76 of the AML/CFT Act states that, at the request of the GIFI, the obligated institutions have to “*immediately*” submit or make available any information or documents held, including those referring to customers, transactions, type and value of assets and place of storage, the application of all the CDD measures referred in Article 34 and the IP addresses from which the obligated institution has connected to its IT system, therefore complying with this criterion.

218. The submission of information to other competent authorities such as the KNF, NBP and NACSU is analysed under the scope of Recommendation 9.

### ***Weighting and Conclusion***

219. The AML/CFT Act covers the main criteria of Recommendation 11, however there are some concerns mainly regarding the defined periods for the keeping of analyses within the framework of the CDD, as well as the requirement of transaction records to be sufficient to reconstruct their traceability not being fully enforceable. **R.11 is rated Largely Compliant.**

### ***Recommendation 12 – Politically exposed persons***

220. In the 2013 MER, Poland was rated largely compliant with former R.6. The assessment identified technical deficiencies related to the definition of PEP, which did not cover all PEP categories specified in FATF standards; lack of requirement to apply enhanced CDD if the beneficial owner is a PEP, to conduct enhanced ongoing monitoring on the entire business relationship and to obtain senior management approval to continue such relationship with a PEP.

#### ***Criterion 12.1 – (Mostly Met)***

221. a) The definition of PEP available in Article 2(2)(11) of the AML/CFT Act is aligned

with the FATF Glossary.

222. The application of risk management systems to identify whether a customer or a beneficial owner is a PEP is articulated through Art. 46(1), which states that obligated institutions need to implement procedures based on risk assessments in order to determine whether a customer or a beneficial owner is a PEP

223. b) Article 46(2) of the AML/CFT Act establishes the measures that need to be adopted by all obligated institutions regarding business relationships with PEPs. Such measures include obtaining the permission of the senior management to establish or continue a business relationship with a politically exposed person.

224. c) Article 46(2) establishes the obligation to “*apply adequate measures in order to establish the source of the customer’s wealth and sources of assets available to the client under the business relationship or the occasional transaction.*” The “assets” in the legal provision are to be understood as the funds concerned in the business relationship. However, the obligation only refers to the *customer* but not the beneficial owner.

225. d) Article 46(2) states that obliged entities shall “*intensify the application of the customer due diligence measures referred to in Article 34(1)(4)*” when establishing business relationships with PEPs. Article 34 (1)(4) is related to the ongoing monitoring of the business relationship and, as such, “intensify” should be read as “enhance”.

#### ***Criterion 12.2 – (Mostly Met)***

226. a) The definition of PEP contained in Article 2(2)(11) does not make any difference between domestic or foreign PEPs, thus including them both. Therefore, the applicable measures do not make a difference between typologies of PEPs either and are equally applicable to all persons regardless of their field of activity (national or foreign).

227. As a result, the measure contained in Article 46(1) of the AML/CFT Act explained in criterion 12.1.a) is equally applicable to a domestic PEP.

228. b) The measures described in that Article 46(2) of the AML/CFT are equally applicable to domestic PEPs, regardless of a higher risk being detected or not. However, the minor shortcoming identified in criterion 12.1.c) would also apply here.

#### ***Criterion 12.3 – (Mostly Met)***

229. Article 46(6) of the AML/CFT Act established that the measures defined in the very same article that are applicable to the business relationships with PEPs should also apply to family members of politically exposed persons and other persons known as close co-workers of the PEP. While the extent of “family members” is not defined in the law, “co-workers” are defined in Article 2(2)(12). However, the scope of the definition of co-workers is narrower than the FATF definition of close associates, since it only covers beneficial owners of legal persons or arrangements alongside a PEP or being close to a PEP, and beneficial owners of legal persons or arrangements established for the personal gain of a PEP.

#### ***Criterion 12.4 – (Mostly Met)***

230. According to Article 46(3) of the AML/CFT Act, obligated institutions that take part in insurance agreements (as defined in Article 2(1)(8) of the same law) shall undertake adequate measures in order to determine whether the beneficiaries of the agreement or their beneficial owners are truly PEPs.

231. Article 46(4) established that should a higher level of money laundering or terrorist financing risk be identified, prior to the payment of the benefit or transfer of rights, the obligated institutions shall perform in-depth analysis of the business

relationship with the customer and inform the senior management of their intention to pay this benefit.

232. The obligated institutions that need to apply the described measures are the ones defined in Article 2(1)(8) (insurance companies, including domestic ones, main branches of foreign ones), as they are the only financial institutions that are allowed to intermediate with insurance policies/agreements. However, the measures described in Article 46(4) do not include a direct reference to consider making a suspicious transaction report.

### ***Weighting and Conclusion***

233. Poland's legal framework is mostly in line with the requirements set in Recommendation 12, while only existing some minor shortcomings in criteria 12.1.c) and 12.2.b) (lack of obligation to identify the source of funds and wealth of beneficial owners who are PEPs), 12.3 (the definition of close associates is narrower than that of the FATF) and 12.4 (there is not a direct reference in the AML/CFT Act to consider making a SAR whenever a PEP is a beneficiary of a life insurance policy and high ML/TF risks are identified). As a result, **R.12 is rated Largely Compliant**.

### ***Recommendation 13 – Correspondent banking***

234. In the 4<sup>th</sup> round MER, Poland was rated LC with the previous R.7. The requirements concerning cross-border banking relationships were limited to respondent institutions located in a state not imposing equivalent AML/CFT obligations. There was no requirement to establish the reputation of the respondent and to determine whether it has been subject to an ML/TF investigation or regulatory action, nor to ascertain that the AML/CFT measures implemented by a respondent institution were adequate and effective.

235. Article 45 of the AML/CFT Act addresses correspondent relationships with institutions in third countries. The provisions do not apply to correspondent relationships with institutions in EU Member States. The Article covers any correspondent relationship, not only banking relationships.

#### ***Criterion 13.1 – (Mostly met)***

236. a) Article 45(1)(1) specifies that obligated institutions must acquire information concerning the respondent in order to understand the operations it carries out. Article 45(1)(2) adds to this by requiring institutions to determine, based on commonly held information, the reliability of the respondent and the quality of supervision of it. This latter provision might implicitly cover whether the respondent has been subject to ML/TF investigation or regulatory action but would still leave some room for not actively identifying and assessing the implications of such action, and there would be merit in extending the language of the legislation so that it expressly addresses investigation and regulatory action.

237. b) Article 45(1)(3) requires obligated institutions to evaluate the respondent's procedures for AML/CFT, which would include controls.

238. c) Article 45(1)(4) specifies that obligated institutions must acquire the approval of senior management before establishing correspondent relations.

239. d) Article 45(1)(5) requires obligated institutions to determine and document the scope of responsibility of each of the obligated institutions and the respondent. The concept of determination does not fully embrace the concept of understanding used in the criterion.

### ***Criterion 13.2 – (Met)***

240. a) Article 45(1)(6) of the AML/CFT Act specifies that obligated institutions must ascertain that the respondent has applied CDD measures, including identification and verification of the identity of customers, in relation to customers having direct access to accounts held with the obligated institution.

241. b) The same article requires obligated institutions to ensure that the respondent will make information concerning the CDD measures applied available to the obligated institution on request.

### ***Criterion 13.3 – (Partly met)***

242. Article 45(2)(1) of the AML/CFT Act specifies that obligated institutions shall not establish nor maintain correspondent relationships with a FI that is not part of a group, which does not have a registered office (which can also be translated as “headquarters”) and which is not actually managed and governed in the territory of the jurisdiction of the law in which it is established (a shell bank). There is a gap between this language and the FATF definition of shell bank, which refers to effective consolidated supervision and meaningful mind and management. The Article also requires obligated institutions not to establish nor maintain correspondent relationships with FIs that are known to conclude contracts for operating accounts with a shell bank; this is a different test to that of the criterion which indicates that FIs must satisfy themselves that respondents do not permit their accounts to be used by shell banks.

### ***Weighting and Conclusion***

243. Poland fully meets the requirements of 13.2. Moderate shortcomings remain as there is no express requirement to assess whether the respondent has been subject to ML/TF investigation or regulatory actions, the concept of understanding the AML/CFT responsibilities is not fully covered, and there is a gap between the language of the AML/CFT Law and the FATF definition of shell bank. Poland is rated **Partially Compliant with R.13**.

### ***Recommendation 14 – Money or value transfer services***

244. In the 4<sup>th</sup> round MER, Poland was rated LC with former SR.VI. The assessment identified technical deficiencies in the AML/CFT Law relating to preventive measures, particularly on CDD, which applied to MVT operators.

245. There is no general definition of value transfer under the Polish law, hence there is no explicit prohibition in the law for providing such services. However, the UKNF maintains that all identified types of value transfer are subject to 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. Given the above, the UKNF did not identify any values or value transfer services providers except from areas which are regulated and subject to supervision. In case an institution offering its services without relevant license is identified, this institution is immediately added to the list of public warnings of the UKNF and information on this institution is submitted to the law enforcement authorities.

### ***Criterion 14.1 – (Met)***

246. Article 60 of the Act on Payment Services specifies that the provision of payment services as a domestic payment institution requires licensing by the UKNF. A license may only be granted to legal persons with their headquarters in Poland. A few exceptions apply, but those are in line with the registration requirements:

- (i) In accordance with the principle of the EU single passport, a business authorised in another EU member state may perform payment services in Poland as cross-border activity or through a branch or an agent without separate authorisation in Poland provided that such activity falls within the scope of the authorisation issued by a competent supervisory authority in a home member state. The UKNF maintains the list of all EEA entities providing payment services in Poland, in accordance with the principle of the EU single passport, which is publicly available on its website.
- (ii) Payment services conducted by a small payment institution (Art. 117(g) and Art. 119 of the Act) or money service offices do not require to be authorised but can be undertaken after entry into the register of small payment institutions or money service offices kept by UKNF.
- (iii) Payment services and activities are covered by a series of exclusions in Art 6, particularly limited network exclusion and payment transactions by means of telecom or information technology devices (Arts. 6.11 and 6.12 of the Act). Only 13 entities are covered by this exclusion. Telecommunication companies are subject to entry in a specific Register of Telecommunication companies, kept by the Office of Electronic Communications.

***Criterion 14.2 – (Mostly met)***

247. Criminal sanctions are applicable to individuals and legal persons undertaking business without authorisation. Article 150 of the Payment Services Act specifies that a fine of up to 5 million PLN (€1.1 million) and up to two years' imprisonment can be imposed. The penalties also apply to a person acting on behalf of another person (including an entity that does not have legal personality). In addition, Article 151 specifies that any person who, without permission from the authorised service provider, concludes a payment service contract is liable to a fine of up to 3 million PLN (€0.66 million) and up to two years' imprisonment. Penalties imposed by the court can be published on the Common Courts Judgments Portal available on the website of the Ministry of Justice. These sanctions are proportionate and dissuasive.

248. At the administrative level, (i) According to Art. 6b of the UKNF Act, the UKNF must disclose to the public the notification of the suspicion of committing an offence specified in Art. 151 of the Payment Services Act; (ii) According to Art. 105 of the Act on Payment Services (Act of 19 August 2011), the UKNF may impose a financial penalty on the payment service provider that pursues its business in breach of the law or endanger the interest of users or electronic money holders; in connection with a failure to fulfil its obligations under Art. 20a, Art. 32b – 32d, Art. 59ia-59ie, Art. 59ig, Art. 59ih and Art. 59ij-59is of the Act on Payment Services; and (iii) the UKNF may disclose to the public information on the application of an administrative sanction to the provider in connection with the violation of the provisions of the Act on the provision of payment services unless the disclosure of such information could threaten the stability of the financial market or disproportionately harm the legal interest of the interested parties (Article 15d of the Payment Services Act).

249. There are no formal procedures to be applied to identify persons carrying out MTS without authorisation. Nevertheless, such cases have been found by UKNF and public warnings issued online in relation to those persons, which proves that action had been taken for their identification.

250. No penalties are available for those MTS that do not require authorisation but only need registration (see 14.1).

#### ***Criterion 14.3 – (Met)***

251. According to Article 2(1)(3) of the AML/CFT Act, MTS are reporting entities and, therefore, subject to GIFI's supervision (see c.16.16). In addition, those MTS that are supervised by UKNF are monitored for AML/CFT compliance in the course of the prudential supervisory actions.

#### ***Criterion 14.4 – (Mostly met)***

252. Article 85 of the Act on Payment Services specifies that the service provider must notify the UKNF in writing of its intention to provide payment services through agents, together with an application to enter the agent(s) on a register maintained by the UKNF. The MTS shall also immediately notify the UKNF about changes concerning the use of services of agents (Art. 87(a) of the Act on Payment Services).

253. The notification shall include, *i.a.*, the name and surname of the agent and the seat and address or the place of residence as well as the main place of business of the agent.

254. The payment institution shall notify the UKNF on intention to provide services within the framework of EU cross-border activity. It is not clear if cross border activities are allowed outside of the EU and, if so, what is their status.

255. Supervisory sanctions for failure to comply with Articles 85 are provided under the Art. 105 or Art. 69 of the Act on Payment Services.

#### ***Criterion 14.5 – (Mostly met)***

256. The notification made by the MTS to the UKNF shall include the description of the control mechanisms placed on its agents in order to prevent money laundering and terrorism financing (Art. 85(2)(3) of the Act on PS). Nevertheless, since there is no explicit requirement for MTS providers to include agents in their AML/CFT programmes, this criterion cannot be considered as fully met.

#### ***Weighting and Conclusion***

257. The authorities have advised there are no value transfer service providers in Poland. MTS providers are required to be licensed by the UKNF. A few exceptions apply in relation to EEA entities providing payment services in Poland, in accordance with the principle of the EU single passport, small payment institutions and some telecommunication companies; however, they are in line with the registration requirements. Although there are no formal procedures to be applied to identify persons carrying out MTS without license/registration, such cases have been found by UKNF and public warnings issued online in relation to those persons. The sanctions available are dissuasive and proportionate, although they only apply to MTS requiring licensing and not to those requiring registration. There is a requirement for MTS providers to maintain a current list of their agents, although it is not clear if this applies to cross-border activities outside of the EU. Although there is no explicit requirement for MTS providers to include agents in their AML/CFT programmes and monitor them for compliance, the notification made by the MTS to the UKNF shall include the description of the control mechanisms placed on its agents in order to prevent money laundering and terrorism financing. Therefore, **R.14 is rated Largely Compliant.**

#### ***Recommendation 15 – New technologies***

258. 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.

***Criterion 15.1 – (Partly met)***

259. There is no specific provision in the AML/CFT Act that requires reporting entities to identify and assess the AML/TF risks that may arise specifically due to the development of new products and new business practices and the use of new or developing technologies for both new and pre-existing products. Notwithstanding this fact, Article 33(3)(4) requires OEs 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.

***Criterion 15.2 – (Not met)***

260. Similar to c.15.1, there is no provision requiring obligated institutions to undertake a risk assessment prior to the launch or use of new products, practices and technologies and to take the appropriate measures to manage and mitigate the risks.

***Criterion 15.3 – (Partly Met)***

261. Poland has considered virtual currencies in the annexes of their most recent version of the NRA, where several money laundering and terrorist financing risks scenarios are analysed. The main conclusions are that decentralised cryptocurrencies/virtual assets constitute a high threat of money laundering, while centralised ones create a medium-level threat of money laundering, and the main vulnerabilities identified are the limited information available to the 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.

262. Entities pursuing economic activities involving providing services related to virtual currencies are obligated institutions of the AML/CFT Act, according to Article (2)(1)(12). However, the scope of VASPs covered in this article does not fully match the FATF definition, as the activities of participation in the provision of financial services related to an issuer's offer and/or sale of a virtual asset are not covered. Notwithstanding the above, the VASPs that do fall within the definition of the AML/CFT Act are obligated institutions, and therefore subject to all the provisions of the Act as any other type of obligated institution would be. 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.

***Criterion 15.4 – (Not Met)***

263. There is no licensing regime or registration regime for VASPs, although a framework is being worked on, and it is expected to be enforceable during the course of 2021.

264. The legal framework for VASPs registration that is being worked on (articles 129m-129wa) will include provisions to ensure that any person providing virtual asset services have not been convicted or, in the case of legal persons, this obligation would be applicable to partners entrusted with management functions.

***Criterion 15.5 – (Not Met)***

265. The AML/CFT legal framework in force at the time of the onsite did not include the possibility to impose penalties on companies or organisational units without personality providing virtual assets services without the requisite license or registration, which are obligations that were not in force yet. Notwithstanding this fact, and as any other business operating in Poland, obtaining an entry in the business register of companies or trusts is mandatory and non-compliance is punishable under Article 601 of the Code of Petty Offences.

***Criterion 15.6 – (Partly Met)***

266. 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)).

267. As stated above, VASPs are subject to the controls implemented by the GIFI to ensure compliance with AML/CFT requirements. In particular, 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. However, as there are no requirements for registration, the possible penalties of withdrawal, restriction or suspension of a license cannot be applied.

***Criterion 15.7 – (Partly Met)***

268. Although the AML/CFT Act establishes a provision for which the GIFI must make knowledge and inform about ML/TF-related issues in a public information bulletin on the website of the Ministry of Finance, no specific feedback or guideline has been provided, in terms of AML/CFT, aimed specifically to the VASPs sector and the particular risks they may face, although some measures to raise awareness in relation to the risks associated with VA and VASPs have been taken, such as providing a summary in Polish of the FATF *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* report.

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

***Criterion 15.8 – (Met)***

270. 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.

271. 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.

***Criterion 15.9 – (Not Met)***

272. At its current state, the AML/CFT Act only obliges to implement the CDD measures contained primarily in Article 34 to occasional transactions equivalent to or exceeding €15 000 or to wire transfers exceeding €1 000, therefore any transaction conducted by a

VASP that does not fall under any of those categories, would not be subject to CDD requirements.

273. Compliance with R.16 in Poland mainly stems from the direct application of Regulation (EU) 2015/847 due to its condition as an EU member. Since the Regulation does not cover VASPs, this part of the criterion is not met.

***Criterion 15.10 – (Mostly Met)***

274. VASPs, as reporting entities under the AML/CFT Act, must implement the restrictive measures and freezing mechanisms defined in Article 119 of the Act to the entities described in Article 118(1), which include the list announced by the GIFI pursuant to the relevant United Nations Security Council Resolutions. However, the concerns related to the timeliness in the implementation of the UNSCRs by obligated institutions expressed in R.7 are also applicable to VASPs.

***Criterion 15.11 – (Mostly Met)***

275. According to Article 12(1) of the AML/CFT Act, the GIFI, as both FIU 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.

276. 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.

277. As stated in the analysis of Recommendations 37 to 40, judicial authorities are able to provide mutual legal assistance, thus including cases in which VASPs could be involved. However, some minor shortcomings regarding the timely prioritisation and execution of requests and the lack of a sound case management system impact their MLA capabilities.

278. Similarly, regarding other competent authorities (UKNF, as supervisor), the shortcomings identified in R.40 (in particular c.12 to 16) would also be applicable regarding VASP information.

***Weighting and Conclusion***

279. Poland has not in place specific requirements, so that obligated institutions have 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 and their risks have been considered within the NRA, there is no obligation for them to officially register, the requirements of wire transfers of R.16 are not applicable to them, and the scope of the definition of virtual asset-related activities contained in the AML/CFT Act is not fully in line with that of the FATF. **R.15 is rated Partially Compliant.**

***Recommendation 16 – Wire transfers***

280. In 2013 MER, Poland was rated compliant with former FATF SR.VII due to direct applicability of the relevant requirements at the EU level as set out in the Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006.

***Criterion 16.1 – (Met)***

281. First of all, it should be noted that EU Regulation 2015/847, on the information accompanying transfers of funds, is automatically enforceable in Poland as an EU member.

282. Article 4(1) of Regulation 2015/847 requires that PSPs (which are also obligated institutions within the Polish AML/CFT legal framework) must ensure that transfers of funds are accompanied by complete information on the payer (originator of the transfer), including its name, payment account number, address, official personal document number, customer identification number or date and place of birth.

283. On similar terms, Article 4(2) of the Regulation, PSPs must also ensure that the transfer of funds is accompanied by information of the payee (beneficiary), in particular, the name of the payee and its payment account number, or if not made from or to a payment account, a unique transaction identifier (Article 4(3)).

***Criterion 16.2 – (Met)***

284. Regulation (EU) 2015/847 considers cross-border wire transfers as those where the payer or the payee is situated outside the area of the European Union; therefore, the same consideration applies in Poland, which is consistent with the FATF standards.

285. In the case of batch transfers, article 6(1) of the Regulation states that it is not necessary to attach the complete information to each individual wire transfer, provide that the batch file contains that information (thus including the originator and beneficiary information), that it has been verified and that the individual transfers carry the account number of the payer or a unique identifies (therefore ensuring traceability).

***Criterion 16.3 – (Met)***

286. According to Article 6(2) of the Regulation 2015/847, for wire transfers where the PSP of the payee is established outside the EU, transfers of funds not exceeding €1 000 shall also be accompanied by, at least, the names of the payer and the payee and the payment account numbers of the payer and the payee or the unique transaction identifier.

***Criterion 16.4 – (Met)***

287. Article 6(2) of the Regulation (EU) 2015/847 also established that the PSP of the payer does not need to verify the information of the payer unless it has received the funds to be transferred in cash or in anonymous electronic money or has reasonable grounds for suspecting ML or TF.

***Criterion 16.5 – (Met)***

288. Domestic transfers in Poland would also include those where all the PSPs involved in the payment chain are established within the EU. In the cases of domestic transfers, Article 5 of the Regulation (EU) 2015/847 establishes that those transfers of funds shall be required to be accompanied by, at least, the payment account number of both the payer and the payee or the unique transaction identifier. According to Article 5(2) of the Regulation, the PSP of the payer must provide to the PSP of the payee, whenever it requests it, complete information on the payer within three working days since receiving the request.

289. Additionally, Article 14 of the Regulation sets the obligation for PSPs, in general, to respond fully and without delay to the enquiries from the authorities responsible for preventing ML/TF.

***Criterion 16.6 – (Met)***

290. The requirements of c.16.6 are met (see c.16.5).

***Criterion 16.7 – (Met)***

291. Article 16 of the Regulation (EU) 2015/847 establishes that the information on the payer and the payee shall be retained by the PSPs of the payer and the payee for a period

of five years. Additionally, the Regulation also allows Member States to extend the period of retention for another five years, after conducting a comprehensive assessment on the need and proportionality of such extended, justified for AML/CFT purposes.

292. The periods of record-keeping are not only compliant with c.16.7 but are also in line with the periods established in the Polish AML/CFT Act regarding the retention of the information obtained in the framework of application of CDD measures.

***Criterion 16.8 – (Met)***

293. According to Article 4(6) of the EU Regulation 2015/847, the PSP of the payer shall not execute any transfer of funds before ensuring full compliance with Article 4 (where the obligations regarding the information of the payer and the payee that must accompany the transfers of funds are defined).

294. Furthermore, the AML/CFT Act defines specific administrative penalties, in Article 148, to those obligated institutions that fail to fulfil the obligations to ensure that the transfer of funds is accompanied by the information on the payer or the payee or to implement effective procedures to detect the absence of information on the payer or the payee.

***Criterion 16.9 – (Met)***

295. Article 10 of Regulation 2015/847 states that intermediary PSPs shall ensure that all information received on the payer accompanying the transfers of funds is retained with the transfer.

***Criterion 16.10 – (Not applicable)***

296. The current European legal framework on the information accompanying transfers of funds (Regulation 2015/847) no longer allows for exceptions in the implementation of its requirements due to technical limitations, unlike it did the previous Regulation 1781/2006. Therefore, this criterion is not applicable in Poland as an EU member.

***Criterion 16.11 – (Met)***

297. Article 11 of Regulation 2015/847 establishes that intermediary PSPs shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to transfer the funds have been filled in using characters or inputs admissible in accordance with the conventions of that system. The PSPs must also implement effective procedures, including, where appropriate, ex-post or real-time monitoring, in order to detect whether the information on the payer or the payee is missing.

***Criterion 16.12 – (Met)***

298. The requirements of this criterion are met by Article 12 of Regulation 2015/847, where the intermediary PSP must establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking the appropriate follow-up actions.

***Criterion 16.13– (Met)***

299. Article 7 of the Regulation (EU) 2015/847 sets the requirement for the PSPs of the payee (beneficiary FIs) to implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to transfer the funds have been filled in using characters or inputs admissible in accordance with the conventions of that system, as well as to implement

effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the information on the payer on the payee is missing, for domestic transfers (inside the EU) and cross-border transfers, both individual and batch file transfers.

***Criterion 16.14 – (Met)***

300. The obligation for the PSP of the payee to verify the accuracy of the information on the payee on the basis of documents, data or information obtained from reliable and independent sources before crediting the payee's payment account or making the funds available to the payee, is set in Article 7(3) of the Regulation 2015/847. The obligation is applicable for wire transfers exceeding €1 000.

301. As stated in c.16.7, Article 16 of the Regulation that the information on the payer and the payee shall be retained by the PSPs of the payer and the payee for a period of five years (extendable).

***Criterion 16.15 – (Met)***

302. The criterion is met on the basis of the application of Article 8 of the Regulation (EU) 2015/847, where the PSP of the payee (beneficiary) must implement effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up actions.

***Criterion 16.16 – (Mostly met)***

303. MVTS are reporting entities according to Article 2(1)(3) of the AML/CFT Act. However, since the wire transfers obligations in Poland stem from the implementation of the EU Regulation 2015/847, it is unclear whether an MVTS that is subject to the Polish AML/CFT obligations would be required to implement wire transfer controls when providing services outside Poland and the EU, either directly or through agents.

***Criterion 16.17– (Mostly met)***

304. a) MVTS, as reporting entities (see c.16.16), must comply with the obligation set in Article 74 of the AML/CFT Act to report to the GIFI any circumstances that may indicate the suspicion of committing a crime of ML or TF (an SAR). Article 74(3)(2), in particular, determines that when submitting a communication to the GIFI, not only the information related to the customer of the entity must be considered and reported, but also any available data related to the natural persons, legal persons or organisational units involved in the transaction, amongst other types of data and information listed in Article 74(3), such as the value of the assets involved, the numbers of the accounts, etc.

305. b) The obligation to submit an SAR to the FIU of the country affected by the suspicious wire transfer would have to arise from the AML/CFT legal framework of such country and not the Polish Act.

***Criterion 16.18 – (Mostly met)***

306. FIs that conduct wire transfers, as reporting entities under the AML/CFT Act, must implement the restrictive measures and freezing mechanisms defined in Article 119 of the Act to the entities described in Article 118(1), which include the list announced by the GIFI pursuant to the relevant United Nations Security Council Resolutions.

307. Furthermore, as being established in a country that is an EU member, FIs are also subject to the EU requirements that give effect to UNSCRs 1267 and 1373 and subsequent resolutions.

308. However, the concerns related to the need for a legally binding act at an EU level for UNSCRs to be applicable, the timeliness in the entry into force and implementation of the UNSCRs by obligated institutions and the immediateness of freezing funds expressed in R.6 and R.7 are also applicable here.

### *Weighting and Conclusion*

309. Poland meets most of the criteria for R.16 as a result of the immediate application in the country of the EU Regulation 2015/847 and mostly meets c.16.16, c.16.17 and c.16.18. **R.16 is rated Largely Compliant.**

### *Recommendation 17 – Reliance on third parties*

310. In the 4<sup>th</sup> round MER, Poland was rated PC with former R.9. The assessment identified technical deficiencies related to the requirement to immediately obtain from a third party the necessary information concerning certain elements of the CDD process; the requirement to obtain upon request, without delay, from third parties, the CDD documentation; the absence of clear requirements to ensure that the third party is regulated and supervised and has measures in place to comply with the CDD requirements; and the absence of measures to determine whether the country in which the third party is based adequately applies the FATF Recommendations.

#### *Criterion 17.1 – (Partly met)*

311. Under Article 47(1) of the AML/CFT Act, obligated institutions can use the services of another entity while applying the measures articulated at Articles 34(1) to (3) (identification and verification of customers and beneficial owners of legal persons, definition of the ownership and control structure, assessment of the business relationship and, if applicable, obtaining information on its objective and intended nature). The information at Articles 34(1) to (3) must be obtainable by the obligated institution upon request and immediately in order to use the services of another entity.

312. By virtue of Article 47(3), there is a requirement for the entity relied on to be an obligated institution or a membership organisation or federation associated with such entity, which seems to be wider than the FATF concept of a FI or DNFBP. Similarly, where the entity relied upon is outside Poland, then reliance may be placed on persons applying provisions equivalent to those in place in the EU which are supervised for compliance with those requirements in line with EU provisions. This may extend beyond FIs and DNFBPs. The requirements to obtain immediately the necessary information do not explicitly cover the purpose and intended nature of the business relationship being understood.

313. Article 47(2) adds that the use of third-party services shall not discharge the obligated institution from its liability for the application of customer due diligence measures.

314. (a) Article 47(1) provides that the obligated institution must obtain the information specified in Articles 34(1) to (3). See above for the difference between the Articles and the necessary information specified in sub-criterion (a).

315. (b) Article 47(1) specifies that the obligated institution must require the entity on whom reliance is placed to immediately provide the required information and documents related to applied CDD measures, including copies of documents which consist of identification and verification of the customer and beneficial owners. However, there is no provision in the AML/CFT Act clearly requiring obliged institutions to take steps to satisfy themselves that data and other relevant information relating to the understanding of the nature of the business will be made available by the third party without delay.

Accordingly, and in the light of the aforementioned deficiency related to the absence of a requirement for the CDD to derive from reliable, independent source material, the obliged institutions will not be in a position to determine whether the third party relied upon can or will provide the required information and documents when called upon to do so.

316. (c) Article 47(3) specifies that the relied-on person must meet the relevant EU AML/CFT provisions in connection with the application of CDD measures and record retention, as well as supervision by competent authorities corresponding to those of EU requirements. This is consistent with sub-criterion (c).

***Criterion 17.2 – (Met)***

317. Under Article 47(4), the obligated institution cannot appoint a third party established in a high-risk country unless the third party is a branch or majority-owned subsidiary of the obligated institution or a branch or majority-owned subsidiary of an entity established in any Member State where the branch/subsidiary is subject to the EU AML/CFT directive framework. A high-risk third country means a country identified, on the basis of information originating from reliable sources, including FATF MERs, as not having in place an effective ML/TF system, or having significant gaps in its system, in particular, a third country identified by the European Commission in the Delegated Act adopted pursuant to Article 9 of Directive 2015/849.

***Criterion 17.3 – (Mostly met)***

318. a) Article 47(5) of the AML/CFT Act specifies that the relied-on entity must be included within a group that applies CDD measures, record keeping and internal procedures at the group level. Article 47(5) stipulates that obligated institutions applying (all) CDD measures may acknowledge that the obligation of application of CDD measures indicated in criterion 17.1 is satisfied if these measures were applied by an entity belonging to the same group.

319. b) Article 47(5) includes a requirement for supervision at the group level of implementation of CDD measures, record keeping and internal procedures by a competent authority of a Member State or a third country under the rules and in a manner corresponding with EU AML/CFT requirements.

320. c) There is no explicit reference to higher country risk being adequately mitigated by the group's AML/CFT authority. This gap is largely mitigated by the provisions articulated in c.17.2 and general coverage of the group-wide procedures mentioned at sub-criterion (a).

***Weighting and Conclusion***

321. The requirements to obtain immediately the necessary information do not explicitly cover the purpose and intended nature of the business relationship being understood. There is no provision in the AML/CFT Act clearly requiring obliged institutions to take steps to satisfy themselves that data and other relevant information relating to the understanding of the nature of the business will be made available by the third party without delay. Accordingly, the obliged institution will not be able to determine whether the third party relied upon can or will provide the required information and documents when called upon to do so. Also, there is no clear reference that any higher country risk is adequately mitigated by the group's AML/CFT policies.  
**R.17 is rated Partially Compliant.**

***Recommendation 18 – Internal controls and foreign branches and subsidiaries***

322. In the 4<sup>th</sup> round MER, Poland was rated LC with former R.15 and R.22. The

assessment identified technical deficiencies related to the lack of provision concerning timely access to CDD and other relevant information; the absence of the obligation to introduce screening procedures to ensure high standards when hiring employees; and the lack of requirement for certain FIs to have internal audit function. There were also no requirements for foreign branches and subsidiaries to apply the higher standard and inform the home country supervisor to apply AML/CFT measures which are at least equivalent to those in force in Poland.

***Criterion 18.1 – (Partly met)***

323. Obligated institutions are required by Article 50(1) of the AML/CFT Act to have an internal procedure for AML/CFT. Article 50(2) adds that this procedure should take into account the nature, type and extent of activity conducted and define rules of procedure considered to be analogous to controls. These rules must cover internal control and oversight of compliance as well as the rules of conduct defined in the internal procedure. In addition, this Article provides that obligated institutions must implement a procedure of reporting of actual or potential infringements of the Act by persons acting for the institution. These provisions do not explicitly cover internal policies.

324. a) Article 6 of the Act specifies that obligated institutions shall appoint a member of senior management to be responsible for the performance of obligations under the Act. Article 7 adds that where there is a management board or other governing body, one of them must be appointed as responsible for implementation of the Act. Also, Article 8 specifies that an employee of management position should be appointed for ensuring AML/CFT compliance. Under Article 9, sole practitioners are responsible for performing the functions specified in Articles 6 and 8.

325. In addition, provisions in the Banking Law complement these general requirements. Article 9 requires banks to have risk management and internal control systems, with some features of the latter being provided by Article 9(c). The UKNF has also issued Principles of Corporate Governance for Supervised Institutions. While the Principles are not enforceable and do not explicitly refer to AML/CFT, paragraph 45 stipulates that a supervised institution should have an adequate, effective and efficient internal control system. The UKNF has also issued “Recommendation H Concerning the Internal Control System of Banks” under the Banking Law and the Act on Financial Market Supervision. While Recommendation H constitutes guidance and does not expressly refer to AML/CFT, it recommends the establishment of an internal control system based on the “three lines of defence” model and extends to the application and effectiveness of the risk management system.

326. b) There are some legal provisions relevant to the screening of employees in the Act of 12 April 2018 “On the principles of obtaining information on the criminal record of applicants for employment and persons employed in entities in the financial sector”. Financial sector employees, as defined in Article 2 of the Act, are able to examine the criminal record of employees and applicants for employment where (i) the employment relates to the property of the institution or third parties or (ii) where the position allows access to legally protected information or (iii) positions related to a decision-making process connected with a high risk of loss of property or other significant damage to the institution or a third party. It is not clear how these legal provisions may be applied through AML/CFT programmes to generally ensure high standards in line with c.18.1. An exemption is laid down in Article 1(5) of the Act, pursuant to which the provisions of the Act shall not apply to applicants for employment and persons employed in entities of the financial sector for which the requirement of criminal record is laid down in the provisions of the laws referred to in Article 3(1). It is not clear how these exemptions permit FIs to

ensure high standards in line with c.18.1.

327. c) Articles 50(1) and (2) require obligated institutions to have internal rules relating to the dissemination of knowledge among employees on the scope of the AML/CFT requirements. In addition, Article 52(1) specifies that obligated institutions must ensure the participation of employees fulfilling obligations under the Act associated with AML/CFT in training programmes related to the performance of their functions. Article 50(2) adds that training programmes must take into account the nature, type and scope and activity of the institution and ensure up-to-date knowledge of the scope of implementation of the institution's obligations.

328. d) The AML/CFT Act does not contain provisions on an independent audit function. Article 9c of the Banking Law, while not expressly referring to AML/CFT, requires an internal control system to include an internal audit sub-unit to examine and assess the adequacy and effectiveness of the internal control and risk management systems in an independent and objective manner. This Article is supported by the Principles of Corporate Governance for Supervised Institutions and Recommendation H Concerning the Internal Control System of Banks, which specify that internal audit functions should be independent. Apart from the banks, the other obliged entities have no provisions related to an independent audit function to test the system.

#### ***Criterion 18.2 – (Partly met)***

329. Article 51(1) of the AML/CFT Act specifies that obligated institutions must introduce a group AML/CFT procedure for branches and majority-owned subsidiaries established in third countries. This requirement, however, does not extend to branches and subsidiaries in EU member states. The contents of the procedure do not expressly or implicitly include the measures set out in c.18.1.

330. (a) Article 51(2) of the Act provides that the procedure must define rules for the exchange of information and the protection of information provided for AML/CFT purposes within the group. Article 54(2)(1) of the Act permits obligated institutions and their branches and subsidiaries to exchange information when applying the rules of procedure in the group procedure. Potentially, rules might not necessarily cover both policies and procedures, and while the generality of AML/CFT is covered, there is no explicit reference to CDD or risk management.

331. (b) Articles 51(2) and 54(2)(1) of the Act are also relevant to compliance with this criterion. While the generality of AML/CFT is covered, there is no explicit reference to the specific matters in the criterion, and so it is not clear the extent to which compliance, audit and risk functions will receive or disseminate information.

332. (c) Article 51(1) specifies that a group procedure must be put in place in relation to branches and subsidiaries in third countries; Article 51(2) refers to rules being put in place under the third country group procedure in relation to the exchange and protection of information; and Article 51(3) addresses situations where the requirements in a third country are less strict than those in the AML/CFT Act (including in relation to data protection). However, while these provisions circle the requirements of the sub-criterion, there is no explicit reference to imposing adequate safeguards on confidentiality, use of information and tipping off.

#### ***Criterion 18.3 – (Mostly met)***

333. There are provisions in place in relation to group entities in third countries (see the opening paragraph of c.18.2). Article 51(3) specifies that if the AML/CFT requirements in the third country are less restrictive than those in the AML/CFT Act, obligated institutions must require application of the provisions of the Act to the extent permitted

by regulations in the third country. Article 51(4) provides for the situation where a host country does not allow proper implementation of AML/CFT measures consistent with Polish requirements. In this case, financial groups are required to ensure the application of additional measures by branches and subsidiaries to manage the ML/TF risks. The additional measures to be applied in relation to third countries are regulated at the EU level<sup>86</sup>. In such circumstances, there is a requirement to inform the home supervisors (the GIFI and the authorities referred to in Article 130(2)). However, this does not apply to branches and subsidiaries located in EEA member states.

### ***Weighting and Conclusion***

334. Controls put in place by FIs do not explicitly cover internal policies. It is not clear to what extent AML/CFT programmes address screening procedures for hiring employees, nor to what extent there is a statutory basis for such screening. Apart from the banks, the other financial institutions have no provisions related to an independent audit function to test the system. The content of group-wide AML/CFT programmes is not specified, nor do they apply to branches and subsidiaries in EEA Member States. There is no explicit requirement for such programmes to impose adequate safeguards on confidentiality, use of information and tipping off. Financial institutions are required to ensure the application of AML/CFT measures consistent with the Polish legislation in relation to group entities in third countries where the AML/CFT requirements are less strict. Where a third country does not permit the proper implementation of AML/CFT requirements, there are additional measures at the EU level which can be applied by the country. However, this does not apply to branches and subsidiaries located in EEA member states. Together, these are considered to be moderate shortcomings, and therefore **R.18 is rated Partially Compliant**.

### ***Recommendation 19 – Higher-risk countries***

335. In the 4<sup>th</sup> round MER, Poland was rated as PC with former R.21. The assessment identified technical deficiencies related to the lack of requirement to give special attention to business relationships with persons from or in countries that do not or insufficiently apply the FATF Recommendations; there is also an absence of the requirement to make written findings available to assist auditors and to apply appropriate countermeasures.

#### ***Criterion 19.1 – (Mostly met)***

336. Article 43(1) of the AML/CFT Act requires obligated institutions to apply EDD in cases they consider having higher ML/TF risk and in some specified circumstances. These circumstances include those in Article 44(1), which requires EDD to be applied to customers originating from or established in a high-risk jurisdiction outside the EU (i.e. a third country). A high-risk third country is defined in Article 2(2)(13) as a country identified on the basis of information originating from reliable sources, including evaluation reports by the FATF and affiliates, as countries not having an effective AML/CFT system, as listed by the Regulation (EU) 2016/1674. Thus, the requirement to apply EDD measures is limited to the high-risk jurisdictions outside the EU/EEA area.

337. The EDD obligation does not apply in relation to branches or majority-owned subsidiaries, wherever located, of obligated institutions in Poland or to branches or

---

<sup>86</sup> [Commission Delegated Regulation \(EU\) 2019/758 of 31 January 2019 supplementing Directive \(EU\) 2015/849 with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries \(Text with EEA relevance.\)](#)

majority-owned subsidiaries, wherever located, of any entity established within the EU where such entity is subject to the EU directive framework (see Article 44(2)).

338. There is a gap in meeting the criterion with regard to the exceptions permitted in relation to EU Member States and branches/subsidiaries of EU entities. This gap is reduced to some extent by a combination of Article 43(1) and other provisions in the Act as set out below.

339. Article 43(2) provides that a range of circumstances may substantiate increased ML/TF risk. These include association of the business relationship or occasional transaction with a high-risk third country; or a state defined by a reliable source as having an elevated risk of: corruption or other criminal activity, support for or commission of acts of terrorism, or association with terrorist organisations; or a state in relation to which the UN or EU has imposed sanctions or restrictive measures.

340. Under Article 44(3), the scope of CDD measures to be undertaken must include the risk assessment of the business relationship/occasional transaction required by Article 33(2) (i.e. EDD might or might not be undertaken dependant on the obligated institution's risk assessment). Article 33(3) requires geographic risk to be taken into account when undertaking the risk assessment. More generally, Article 27 requires an obligated institution's "whole of business" risk assessment to take account of geographic risk.

#### ***Criterion 19.2 – (Not met)***

341. Polish legislation does not provide for countermeasures when this is called for by the FATF or independently, except for the requirement of EDD measures in the circumstances set out in c.19.1.

#### ***Criterion 19.3 – (Met)***

342. After each FATF plenary, the GIFI publishes via its website the two updated FATF lists of jurisdictions subject to a call for action and jurisdictions under increased monitoring. In addition, the EU's list of high-risk third countries is accessible via a link on GIFI's website.

### ***Weighting and Conclusion***

343. There are moderate shortcomings under Recommendation 19. Poland has measures in place to ensure that FIs are advised on concerns about weaknesses in the AML/CFT systems of other countries. EDD obligation does not apply in relation to branches or majority-owned subsidiaries, and there is a gap regarding the exceptions permitted in relation to EU Member States and branches/subsidiaries of EU entities. There are no specific provisions in the AML/CFT on countermeasures other than EDD, which are subject to specific limitations. **R. 19 is rated Partially Compliant.**

### ***Recommendation 20 – Reporting of suspicious transaction***

344. Poland was rated PC in the MER of 2013 for the former Recommendation 13 and Special Recommendation IV. The deficiencies pertained to the scope of reporting requirements (linked to transactions without extending to funds). The assessment team also highlighted deficiencies in the criminalisation of ML and FT, limiting the reporting obligations. Attempted transactions were not covered.

#### ***Criterion 20.1 – (Partly Met)***

345. According to Article 74 of the AML/CFT Act, the obligated institution shall notify the GIFI of any circumstances which may indicate the suspicion of committing the crime of ML or TF. The notification shall be submitted immediately, but no later than two

business days following the day of confirming the suspicion by the obligated institution.

346. Another reporting requirement is defined under Article 86 of the AML/CFT Act, which is a separate procedure as it implies the suspension of transactions. Under that article, the obligated institution shall immediately notify the GIFI, with the use of electronic communication means, of any case of acquiring justified suspicion that the specific transaction or assets may be associated with ML or TF.

347. The GIFI shall immediately confirm the receipt of the SAR containing, in particular, the date and the time of accepting the notification. The obligated institution shall carry out the indicated transaction for no longer than 24 hours, counting from the moment of the confirmation of the receipt of the notification or any other transactions charging the account on which reported assets have been collected.

348. The GIFI thus has 24 hours to make a first assessment of the SAR. In case of the transaction or assets can be associated with ML or TF, the GIFI shall within those 24 hours provide the obligated institution with a request to suspend the transaction or block the account for no more than 96 hours from the date and time indicated in the confirmation of receipt of the SAR. In such a case, the GIFI has to notify the competent prosecutor on suspicion of committed crime of ML or TF.

349. According to Article 90 of the AML/CFT Act, the obligated institution shall immediately notify the GIFI, with the use of electronic communication means, of performing the transaction referred to in Article 86(1) in the event if the submission of the notification prior to the performance of the transaction was impossible. In the notification, the obligated institution shall justify the reasons for its failure to submit the notification in advance and provide information available to it confirming the acquired suspicion referred to in Article 86(1).

350. Another reporting regime is provided under Article 89 of the AML/CFT Act for the obligated entities (excluding banks and similar establishments), which provides for the obligation to report to the competent public prosecutor suspicions unrelated to ML, TF or fiscal crimes.

351. Nevertheless, the evaluation team has a number of concerns on the overall SAR regime as defined under Recommendation 20. First of all, neither of the relevant articles extends the reporting requirement to the cases when there are suspicions or reasonable grounds to suspect that funds are the proceeds of criminal activity. Moreover, the shortcomings in relation to Article 165a of the CC with regard to the criminalisation of TF restrict the scope of the TF reporting requirement (see further details in the analysis for c.5.1). Concerns that the lack of clarity/ distinction between these two (or even three) modes of the reporting regime might create confusion have also been expressed in the previous round MER.

#### ***Criterion 20.2 – (Met)***

352. Article 74 extends to attempted transactions as it refers to circumstances, which may indicate the suspicion of ML or TF. As for Article 86, it relates to attempted transactions.

353. The obligation to report covers all ML/TF suspicion transactions, regardless of the amount of the transaction.

#### ***Weighting and Conclusion***

354. The AML/CFT Act is partly in line with the substantive requirements under Criterion 20.1, as one of the mechanisms to file SARs casts doubts on the fulfilment of the

obligation to do so “promptly” in line with the FATF Recommendations. The reporting requirements do not extend to the cases when there are reasonable grounds to suspect that funds are the proceeds of criminal activity. Shortcomings in relation to the criminalisation of TF restrict the scope of the TF reporting requirement. There are also concerns over the lack of clarity/ distinction between the two (or even three) modes of the reporting regime. Criterion 20.2 is met. **R20 is rated Partially Compliant.**

### *Recommendation 21 – Tipping-off and confidentiality*

355. In 2013 MER, Poland was rated largely compliant with former R.14. The assessment identified minor technical deficiencies related to some unclarity regarding civil and criminal liability and coverage of the related information by the tipping-off provision.

#### ***Criterion 21.1 – (Mostly met)***

356. According to Article 91 of the AML/CFT Act, obligated institutions will not incur disciplinary, civil, criminal or any other liability when submitting SARs to the FIU, complying with GIFI’s demand to suspend a transaction under the conditions of Article 87 of the same law or notifying suspicions of criminal activities other than ML/TF to the prosecutor’s office in application of Article 89.

357. However, the article does not explicitly address if directors, officers or employees of the obligated institution are equally exempted from liability as the legal person is according to the aforementioned legal provisions.

#### ***Criterion 21.2 – (Partly met)***

358. Article 54, in particular 54(1), states that obligated institutions, their employees and other persons acting on their behalf shall keep confidentiality of the fact of submitting to the GIFI the information defined in chapters 7 and 8 of the AML/CFT Act. Chapter 8 of the Act includes Article 86, which defines the obligation to submit SARs to the FIU by all reporting entities.

359. However, the very same article 86, in its para 12, states that the obligated institutions can inform a customer, on their request, about the submission of information to the GIFI related to a transaction they performed or ordered to perform, as well as accounts they are the holders or owners of, due to suspicions they might be linked to ML or TF. It is explicitly stated that, in this event, article 54, which grants confidentiality, would not be applicable.

360. This is further reinforced in Article 54(2)(3) as well, as it allows certain obligated institutions to inform their customers about the scope of information provided to the GIFI so that such customer ceases or does not undertake the activity contrary to the AML/CFT Act.

361. Therefore, there are several legal provisions that allow disclosure of SAR-related information to customers, thus not fully complying with the criterion.

### *Weighting and Conclusion*

362. While Poland has measures in place in order to avoid tipping off and ensure confidentiality, in particular relating to the submission of SARs, certain legal provisions allow reporting entities to communicate such facts to their customers in order to deter them from engaging in the reported attempted transaction or to justify the end of the business relationship. **R.21 is rated Largely Compliant.**

## *Recommendation 22 – DNFBPs: Customer due diligence*

363. Poland was rated partially compliant in the MER of 2013 for the former Recommendation 12. The assessment identified technical deficiencies – in addition to those vis-à-vis former R.5, R.6, R.8, R.9, R.10 and R.11 – related to uneven application or absence of application of relevant AML/CFT requirements by the CSPs, legal professionals and notaries.

### ***Criterion 22.1 (Mostly met)***

364. Casinos (as well as any other entity pursuing activities in the scope of games of chance, betting, card games and games on gaming machines) are obligated institutions pursuant to Article 2(1)(20) of the AML/CFT Act and, as such, are subject to the implementation of the CDD measures of Article 34.

365. When determining the scenarios in which CDD must be performed, according to article 35(1)(4), casinos must apply due diligence measures to customers betting a stake and collecting prizes with a value equivalent to €2 000 or higher, irrespective of whether the transaction is conducted as a single operation or as several operations which seem to be linked, therefore complying with the threshold required in this criterion.

366. According to Article 2(1)(18), real estate agents are obligated institutions and, therefore, must apply CDD measures whenever they intermediate in real estate trading.

367. All “entrepreneurs” that accept or make cash payments exceeding the equivalent of €10 000, regardless of whether the payment is performed as a single operation or several operations which seem to be linked, are obligated institutions. Therefore, the DPMS are included in the definition and the minimum threshold for which they should apply CDD is compliant with the one required for this criterion.

368. Lawyers and other independent legal professionals (such as attorneys, legal advisers or foreign lawyers) are obligated institutions and must apply CDD in the conditions stipulated by R22(1)(d).

369. Notaries are subject to the same CDD requirements, according to Article 2(1)(13), in particular within the scope of activities performed in the form of a notarial deed. These activities do not include the managing of client money, securities, other assets, banks, savings or securities accounts, as notaries are not entitled to perform them, according to the Law on Notaries.

370. Tax advisers are subject to CDD requirements (in the same terms specified as for the lawyers, as well as in relation to tax advisory services). The statutory auditors must perform CDD for all their services (Article 2(1)(15) of the AML/CFT Law). Article 2(1)(17) also covers natural persons as legal entities “pursuing activities in the scope of providing bookkeeping services”. Such services are limited to those defined in Article 76a par.1 of the Accounting Act and do not include any of the activities that the FATF attributes to accountants in order for them to have AML/CFT obligations.

371. TCSPs are not directly covered by the AML/CFT framework. Instead, article 2(1)(16) of the AML/CFT Act considers obligated institutions any entrepreneur that provides TCSP-like services<sup>87</sup>.

---

<sup>87</sup> Establishment of legal persons or organisational units without legal personality, fulfilling the function (or enabling another person to do so) of a member of the management board of a legal person or organisational unit without legal personality, providing a registered office, address of establishment or correspondence to a legal persons/organisational unit, acting or enabling another person to act as a trustee or act or enable another person to act as a person exercising its

372. As a result, these types of persons or entities are subject to perform CDD when engaging in any of the mentioned activities. The cases in which the entrepreneur would be acting (or arranging for someone else to act as) as a director, secretary or partner of a company/partnership/legal person, acting as the equivalent position of a trustee in other types of legal arrangements or acting or arranging for someone else to act as nominee shareholders would not be explicitly covered.

373. However, such cases are not provided for in Polish legislation.

***Criterion 22.2 – (Partly met)***

374. All DNFBPs defined under criterion 22.1 are obligated institutions and, therefore, are subject to the record-keeping obligations set primarily in Article 49 of the AML/CFT Act already analysed under Recommendation 11. As such, shortcomings identified under c.11.2 and 11.3 are also applicable to DNFBPs, as well as the shortcomings in the DNFBPs scope described in c.22.1.

***Criterion 22.3 – (Mostly met)***

375. All DNFBPs defined under criterion 22.1 are obligated institutions and, therefore, are subject to the PEP obligations set primarily in Article 46 of the AML/CFT Act already analysed under Recommendation 12. As such, the minor shortcomings identified under c.12.1, 12.2 and 12.4 are also applicable to DNFBPs, as well as the shortcomings in the DNFBPs scope described in c.22.1.

***Criterion 22.4 – (Partly Met)***

377. There is no provision in the AML/CFT Act that requires reporting entities to identify and assess the AML/TF risks that may arise specifically due to the development of new products and new business practices (although Article 33(3)(4) requires OEs to identify and assess the ML/TF risks associated to, among others, their types of products, services and means of distribution), and the use of new or developing technologies for both new and pre-existing products, undertaking a risk assessment prior to the launch or use of such products, practices and technologies and taking appropriate measures to manage and mitigate the risks. Additionally, the problems in the definition of the DNFBPs scope as obligated institutions also have an impact here.

***Criterion 22.5 – (Mostly Met)***

378. Article 47 of the AML/CFT Act, which is also applicable to DNFBPs, allows the use of third-party entities services while applying the customer due diligence measures. However, all shortcomings identified in R.17 are equally applicable to the reliance on third parties from DNFBPs.

*Weighting and Conclusion*

379. The Polish AML/CFT legal framework presents some shortcomings when defining the scope of the requirements related to TCSPs. Furthermore, the deficiencies identified in R11, 12, 15 and 17 have a cascading effect here, in particular the absence of any requirements related to the assessment of risks and implementation of mitigation measures related to new technologies. **R.22 is rated Partially Compliant.**

***Recommendation 23 – DNFBPs: Other measures***

380. In 2013 MER, Poland was rated partially compliant with former FATF R.16. The

---

rights from shares/stocks from an entity non-listed to a regulated market or not subject to information disclosure requirements from the EU or equivalent international standards.

assessment identified technical deficiencies – in addition to those vis-à-vis former R.13 and R.21 – related to the mentioned above uneven application or absence of application of relevant AML/CFT requirements by the CSPs and notaries.

***Criterion 23.1 – (Mostly Met)***

381. The obligations to report suspicious circumstances or transactions to the GIFI set up in Articles 74 and 86 of the AML/CFT Act are also applicable to DNFBPs, as described in c.22.1.

***Criterion 23.2 – (Mostly Met)***

382. The obligation to define internal procedures on AML/CFT is established by Article 50 of the AML/CFT Act and is also applicable to the scope of DNFBPs considered obligated institutions according to article 2 of the same Law.

383. Article 50(2) specifies the contents of the internal AML/CFT procedures. However, the requirements of c.18.1 do not seem to be specifically covered.

384. The implementation of group-wide programmes on AML/CFT, as required by c.18.2, is regulated under Article 51. Although this article covers the fact that the “group procedures” must address the policies for sharing information required for the purposes of compliance with the AML/CFT provisions as well as the protection of such information, it is unclear whether the provision of customer, account and transaction information (including the analysis performed on unusual ones) would also be covered, as required by c.18.2.b.

385. Regarding the obligation to ensure that foreign branches and subsidiaries apply AML/CFT measures consistent with the home country, Article 50(3) establishes that, if the AML/CFT requirements of the third country are less restrictive than those of Poland, obligated institutions shall require the implementation of the provisions of the Polish AML/CFT Act by their branches and subsidiaries established in the third country, to the extent permitted by the regulations of such country.

386. However, the shortcomings identified under c.18.2 and c.18.3 are also applicable to DNFBPs.

***Criterion 23.3 – (Mostly Met)***

387. All DNFBPs, as obligated institutions, must comply with Article 44 of the AML/CFT Act, which demands the application of EDD to customers originating from or established in a high-risk third country.

388. According to Article 2(2)(13), the definition of high-risk third country includes any country identified to not have in place effective systems for counteracting money laundering or terrorist financing or have significant gaps in those systems, on the basis of reliable sources such as mutual evaluation reports from the FATF and affiliated organisations or third countries identified by the EU. Therefore, the GIFI publishes the FATF lists of jurisdictions subject to a call for action and jurisdictions under increased monitoring and the EU’s list of high-risk third countries on its website.

389. However, the shortcomings identified under c.19.1 and c.19.2 are also applicable to DNFBPs.

***Criterion 23.4 – (Mostly Met)***

390. DNFBPs must comply, as obligated institutions, with the tipping off and confidentiality requirements primarily set in Article 54 of the AML/CFT Act and described under R.21. The shortcomings there identified are applicable to DNFBPs.

### ***Weighting and Conclusion***

391. Poland meets the requirements of c.23.1 (besides the shortcomings in the scope of DNFBPs explained in c.22.1), however, the deficiencies of R.18, 19 and 21 have a cascading effect in **R.23, which is rated Largely Compliant.**

### ***Recommendation 24 – Transparency and beneficial ownership of legal persons***

392. In the 4th round MER, Poland was rated PC on R33. The identified deficiencies were that Polish law did not require adequate transparency concerning beneficial ownership and control of legal persons, access to information on beneficial ownership and control of legal persons was not always timely, and there were no real measures in place to guard against abuse of bearer shares of private companies.

#### *General*

393. Pursuant to Article 33 of the Civil Code, legal persons are the State Treasury and organisational units, which are accorded legal personality by specific regulations. Legal persons comprise, and the provisions in the Code on legal persons apply to: (a) commercial companies (which have a wide meaning – see 24.1) and (b) other types of persons and organisational units with no legal personality but which conduct economic activity and which are granted legal capacity under the Code. Legal persons are subject to registration in the Register of Entrepreneurs, which is a part of the NCR. The types of legal persons are as follows:

1. limited liability companies,
2. joint-stock companies,
3. limited partnerships,
4. professional partnerships,
5. limited joint-stock partnerships;
6. cooperatives operating on the basis of the Law on Cooperatives;
7. associations, regional units of associations having legal personality as well as unions of associations operating on the basis of the Act on Associations;
8. foundations operating on the basis of the Act on Foundations;

394. Cooperatives, associations and foundations conducting economic activity are registered by virtue of Article 50 of the NCR Act.

### ***Criterion 24.1 – (Met)***

395. The different types, basic features and processes for creation of legal persons that can be formed under Polish law are specified in the legal instruments referred to in the general section above.

396. For example, the provisions on creating commercial companies, the most commonly formed legal persons, are stipulated under the Commercial Companies Code, namely Articles 25 and 25<sup>1</sup> (registered partnerships); Articles 91, 93 and 94 (professional partnerships); Articles 105, 109 and 110 (limited partnerships); Articles 130, 133 and 134 (limited joint-stock partnerships); Articles 157, 163, 166 and 168 (limited liability companies); and Articles 304, 306, 318 and 320 (joint-stock companies). These provisions include identification and description of the different types, forms and basic features.

397. There are common elements in the procedure for establishing commercial companies under the Code, such as the obligation to have a statute, filing the statutory documents of the company with the NCR and entering the details of the company in the NCR. A company acquires legal personality on the date of entry in the NCR. Information

on the types, forms, and basic features of legal persons and the manner of their creation (including application forms for entry in the NCR) are available online on websites of Polish authorities (e.g. the information and services website for entrepreneurs (Biznes.gov.pl) and the website of the Republic of Poland (www.gov.pl – National Court Register).

398. The provisions for establishing other types of legal persons (cooperatives, associations and foundations) are stipulated in other legislation, as listed above. The procedure for formation encompasses preparing and signing statutory documents as well as filing those documents with the NCR, which results in the legal person acquiring legal personality (Art. 37(1) of the Civil Code). Information on their creation is also available online at the two websites mentioned above.

399. Beneficial ownership information must be filed with the CRBO in order to form some types of commercial companies. The process is set out under Article 55 of the AML/CFT Act. The legal persons required to file information are: registered partnerships, limited partnerships, limited joint-stock partnerships, limited liability companies, simple joint-stock companies, joint-stock companies (excluding joint-stock companies which are public companies, i.e. companies which are listed on a regulated market or trading on the alternative trading market of Poland).

400. The legal provisions relevant to the criteria described below address the obtaining and recording of basic and beneficial ownership information.

401. All information described above is publicly available.

#### ***Criterion 24.2 – (Partly met)***

402. Poland has assessed elements of the ML/TF risks associated with legal persons created in Poland. The NRA report conducted by Poland includes some general descriptions of risks associated with legal persons, which are included, for example, in the subsections ‘Creation and operation of business entities’ and ‘The Vulnerability of the economy’. The most serious risk of abuse of legal persons, VAT fraud facilitated by so-called “fictitious companies” and “straw men” is also described in the report, along with (to a lesser degree) other types of misuse. In addition, quite substantial information relevant to risk and assessment of it has been captured in the analysis of operational cases by the authorities, statistics and individual and combined outcomes. Understanding of risk is greater than articulated in the NRA report. The authorities agree with the assessment that the most serious risk of abuse is fictitious companies; the materiality of this risk has led to a national initiative to address it. Also, see IO.5.

#### ***Criterion 24.3 – (Met)***

403. Information about the company name, proof of incorporation, legal form and status, address, basic regulating powers and directors of legal persons must be registered in the NCR. The same provisions also apply to cooperatives, associations and foundations. Associations and foundations (Art. 49(1) and 50 of the NCR Act) are obliged to provide accurate basic information (Art. 52-53a). The information to be disclosed and registered in the register is set out under the provisions of Articles 34-35, 38-41, 43-44, 49 and 52-53a of the NCR Act. Under Article 8 of the Act, this information is publicly accessible.

#### ***Criterion 24.4 – (Mostly met)***

404. Articles 9 and 12 of the NCR Act; 84, 89, 103, 126, 288 and 476 of the Commercial Companies Code; 32 of the Tax Ordinance Act; 74 of the Accounting Act address the elements in c.24.3.

405. Under Article 188 and, for joint-stock companies, Article 328 of the Commercial

Companies Code, the management boards of commercial companies are required to maintain a register of shares setting out the name and address of shareholders, the amount of payments made for shares and any transfers of shares to another party, and voting rights. There is no explicit requirement as to where the management board should keep the information or to notify the location to the NCR; the most obvious location on practical grounds (including, for LLCs, right of access to the register of shareholders by shareholders and the management board and right of access by any person in some circumstances) is the registered office of the company and this is the experience of the MoJ and NCR. The authorities also note that the information is held at the NCR.

***Criterion 24.5 - (Met)***

406. With regard to information provided to the NCR, under Articles 22 and 47 of the NCR Act, legal persons are obliged to provide changes to the basic information specified in c.24.3 to the NCR within 7 days of the change (unless provided otherwise by legislative provision). This provision has been used rarely, and its purpose is to cater for difficult and exceptional situations in which a longer time frame than seven days is necessary. For example, in Article 319 of the Commercial Companies Code, the purchase of all shares by one shareholder should be reported to the NCR within three weeks from the date on which the company's management board found out that all the company's shares were acquired by the sole shareholder.

407. Cooperatives, associations and foundations (Art. 49(1) and 50 of the NCR Act) are obliged to provide accurate basic information (Art. 52-53a) as well as any changes thereto.

408. Under Article 24 of the NCR Act, failure by a legal person to submit required documents to the NCR is subject to a summons by the Court (also referred to as coercive proceedings) to file documents within seven days under pain of a fine provided for by the Civil Procedure Code. Where documents have been provided, Article 24 provides for the removal or correction by the Court of information on the NCR that is not in line with documents that are on the registration files. This applies if it is necessary for legal certainty and the issue is significant. For example: (a) Article 24(6) of the NCR Act might justify the removal of individuals who are listed in the NCR as members of the management board from the NCR but are no longer members, as these individuals are representatives of the company and failure to remove them, due to the principle of completeness of the NCR, could potentially lead to significant problems with security of trading; (b) false data on partners in a partnership will be relevant to the security of trading of the partnership as the partners are liable for the commitments of the partnership and disclosure of persons who are no longer partners goes against this security; (c) on the same grounds of security of trading, the correction of an incorrect address if the Court becomes aware that the address in the register is not correct.

409. Criminal penalties apply if information held by legal persons is not updated and accurate. In addition, the requirement to provide the NCR with updated information means that legal persons will be subject to the sanctions framework of the NCR Courts if information in the NCR is not accurate and updated on a timely basis; legal persons must therefore keep their own records accurate and up-to-date to meet the NCR requirements.

***Criterion 24.6 - (Mostly met)***

410. Poland has a multi-faceted approach to ensuring that adequate, accurate and current BO information is available.

411. First, the network of provisions described below mean that almost all legal persons (noting that there have been examples where bank accounts have been surrendered by criminal elements) have a bank account at any one point in time (with

banks being subject to the AML/CFT obligations described in R.10). Legal persons need to have a bank account for commercial and transactional purposes. In addition, the following legal provisions require legal persons to have bank accounts in specified circumstances:

a) According to Article 19 of the Entrepreneurs Act, entrepreneurs (legal persons as well as individuals) are required to have a bank account whenever the other party to a transaction is also an entrepreneur or the value of a transaction exceeds PLN 15,000 (around €3,280).

b) Joint-stock companies and joint-stock limited partnerships are required to have a bank account in an EU member state for payment of share capital; the experience of the NCR team is that these payments have been made by accounts kept in Polish banks.

c) Settlements between the KAS and legal persons (both from the KAS to legal persons and legal persons to the KAS) in respect of tax obligations (payments and returns of due amounts of public law liabilities) are carried out via bank accounts. Moreover, pursuant to the Entrepreneurs' Law, making or receiving payments related to the business activity performed takes place via the entrepreneur's bank account in each case when the party to the transaction from which the payment results is another entrepreneur and a single transaction value, regardless of the number of payments resulting therefrom exceeds PLN 15,000 (around €3,280) or its equivalent. Failure to comply with this obligation has an effect that is similar to a fiscal sanction as the failure makes it impossible to recognise expenses as a tax-deductible cost.

d) Although it is not a legal requirement to pay the fees payable in relation to the NCR via a bank account, an official of the Court registering the largest number of legal persons advised the AT that the vast majority (over 90%) of court fees are paid to the bank account of the competent court. A large proportion of the remaining 10% of court fees are paid by special court fee stamps; since 1 July 2018, these stamps have only been provided in electronic form and must be purchased via a bank account. Due to the need to ensure access by disadvantaged customers to their rights in court, it is possible to pay the fees at the cash desk by cash in the court; this involves full identification of the party making the payment and is generally not sued for payments in relation to legal persons.

412. Second, there is use of notaries and lawyers (also subject to the AML/CFT obligations described in R.22) by a significant number of legal persons.

413. A significant number of legal persons are therefore subject to CDD by more than one obligated institution.

414. Third, since 2018, the NCH has been an important part of the beneficial ownership framework. Established as part of the infrastructure of the Polish banking sector, operating pursuant to Art. 67 of the Banking Law, the main area of operation of the NCH, is electronic settlement and payment services but is now an important part of the beneficial ownership framework. As part of its activities, since 2018, the NCH has maintained a register of bank accounts used, inter alia, by the KAS, courts and judicial authorities. This register includes beneficial ownership information provided by banks on their customers, which are legal persons (Article 92bb of the Banking Act and Section iii B of the Tax Code). The provisions relevant to beneficial ownership in the AML/CFT Act are used.

415. Fourth, Chapter 6 of the AML/CFT Act establishes a public Central Register of Beneficial Ownership (CRBO). This applies to the beneficial ownership of registered partnerships, limited partnerships, limited joint-stock partnerships, limited liability companies, simple joint-stock companies and joint-stock companies (other than joint-stock companies which are public companies (i.e. companies listed on a recognised stock

exchange or which can trade on Poland's alternative trading market). Legal persons registered on the NCR after 13 October 2019 were required to submit beneficial ownership information to the CRBO within seven days following the day of entry in the NCR. For legal persons on the NCR prior to that date, BO information was required to be provided by 13 July 2020. At the time of the visit to Poland by the AT, the CRBO held data on more than 366 000 legal persons. The beneficial provisions in the AML/CFT Act are applicable to entry on the CRBO.

416. In building the CRBO, it was decided to develop the registry in two phases, with associations, foundations and cooperatives being obliged to report information on their beneficial owners to the CRBO in the second phase. The legal framework governing the structure and operation of these entities and the obligation to disclose information about natural persons related to them to the NCR (with control being held individually with, for example, a minimum number of seven founders required for an association and 10 for a cooperative) means that, in practice, information about their beneficial owners was and is seen by Poland as being publicly available in that register. These legal persons have less ML risk than LLCs. There are provisions on associations, foundations and cooperatives, bringing their beneficial ownership within the scope of the CRBO from the end of October 2021. Notwithstanding the multi-faceted approach to beneficial ownership by Poland and the success of the authorities in dealing with fictitious companies, the two-stage approach in relation to the CRBO means that it is possible for beneficial ownership information not to be complete for all associations, foundations and cooperatives within the totality of the system.

417. The definition of beneficial owner at Article 2(2)(1) of the AML/CFT Act applies to obligated institutions and for the purposes of entry in the NCH and the CRBO. The definition is supported by guidance in the form of frequently asked questions issued by the CRBO (and by the UKNF's onsite inspection methodology). There is an exemption for companies whose securities are traded on a regulated market. The definition contains one potential area of uncertainty which is that the senior managing official is not considered to be the beneficial owner where there is suspicion of ML/TF. As the FATF's standards indicate that the senior managing official is considered to be the beneficial owner if no natural persons exercising rights through ownership or other means of control have been identified (i.e. irrespective of suspicion), the AT considers that the definition creates potential uncertainty as to who should be considered to be the beneficial owner where there is suspicion of ML/TF. Poland considers that: it has gone beyond the FATF standards; the overarching legal requirement is to identify the beneficial owner, and this is clear; the text in the definition referenced by the AT focuses attention in practice on the need to identify beneficial owners exercising control "through other means"; there is understanding of the importance of considering the exercise of control through other means; the text in the definition referenced by the AT has not caused uncertainty in practice, and overall understanding of the need to establish the exercise of control through other means is demonstrated by the experience of the authorities and the pattern of data in the CRBO (beneficial ownership being categorised as the exercise of control through other means for a tangible number of legal persons). The CRBO guidance is silent in relation to suspicion (although legal persons are reporting their own data to the registry).

418. Fifth, substantial beneficial ownership information is held and used by the authorities, particularly the KAS, as a result of an analytical and investigation activity. Other authorities also obtain, hold and use beneficial ownership information as a result of their AML/CFT activities. This information enables checking of data between FIs, the NCH and the CRBO in the context both of providing input to registry officials and the authorities' own needs. The KAS, in particular, has had significant success in addressing

the risks of fictitious companies and, therefore, in addressing use of strawmen.

419. Sixth, as indicated in IO.5, the wide range of registers in addition to the NCR and the CRBO registers and the NCH database has a positive effect on checking beneficial owner information on the CRBO register and NCH database.

***Criterion 24.7 – (Mostly met)***

420. Banks, notaries and lawyers are subject to the CDD requirements specified in c.10.7 and c.22.1 to monitor customer relationships and keep information up-to-date.

421. There are also requirements data at the NCH, and therefore beneficial ownership information, to be kept accurate and up-to-date, with changes to information being required to be notified to the NCH within three business days of the change (Article 92bd of the Act of 29 August 1997).

422. With regard to the CRBO, Article 60 of the AML/CFT Act specifies that any changes to the information provided to the CRBO must be submitted within seven days of the change.

423. The CRBO does not yet cover cooperatives, foundations and associations (although their legislation will be brought within the CRBO framework at the end of October 2021). While noting the control information of these types of persons and the information in the NCR, together with the other mechanisms for keeping beneficial ownership information up to date, there is at least a theoretical possibility that cooperatives, foundations and associations might have beneficial owners which are not captured by a requirement for up-to-date information to be held.

***Criterion 24.8 – (Mostly met)***

424. Under Article 18 of the Commercial Companies Code, all members of management (and supervisory) boards must be individuals (although not necessarily resident in Poland). Under Article 3 of the Act on Associations, members of the management board of an association must also be individuals. These provisions cover most legal persons. C.24.6 describes the mechanisms relevant to obtaining and retaining beneficial ownership information and that basic information, held by the NCR in relation to control of associations, foundations and cooperatives, is relevant to beneficial ownership.

425. With regard to the NCR, under Article 694(3)(1) of the Code on Civil Procedure, the obligation is on the legal person to provide basic information to the NCR and cooperate with the registry and any instruction to provide information. These provisions are supported by Article 29 of the Commercial Companies Code (general partnership); Article 96 of the Commercial Companies Code (professional partnership); Article 117 of the Commercial Companies Code (limited partnership); Article 137 of the Commercial Companies Code (limited joint-stock partnership); Articles 204-205 of the Commercial Companies Code (limited liability company); and Article 368(1) of the Commercial Companies Code (joint-stock company). Legal persons are also commercially liable for providing false or failing to provide information to the NCR in the Register (Article 18 of the NCR Act). There are corresponding Articles in the Act on Associations, the Act on Foundations and the Law on Cooperatives.

426. In addition to the company itself, members of the management boards are accountable for providing information to the NCR; as members of the board, they can be sanctioned for failure to provide information to, and the late provision of information to, the NCR; the MoJ and the NCR team see this as a positive benefit when initiating coercive proceedings as it generates responses. Article 18 of the Commercial Companies Code requires members of the management (and supervisory) boards to be individuals,

although there is no statutory requirement for any of them to be a Polish resident.

427. With regard to CRBO, all information provided to the registry must be submitted by an individual authorised to represent the company (Article 61 of the AML/CFT Act).

428. Banks and credit unions are responsible for filing information to the NCH.

429. There are coercive powers, subject to sanction, for information on identification of beneficial owners to be provided to the NCR, the CRBO and the NCH. Also, failure by FIs and DNFBPs to provide information when instructed to do so by supervisory authorities and GIFI as FIU is subject to penalties (see 25.8). In addition, there are penalties applicable for failure by any person to comply with and provide correct beneficial ownership information to LEAs and prosecutors.

430. There are requirements in place and sanctions applicable for failure to provide information, late provision of information or the provision of false or misleading information in response to a demand by an authority to provide information for co-operation to the fullest extent possible with the Polish authorities in determining the beneficial owner by a variety of mechanisms. Nevertheless, there could be situations where a legal person does not yet have a requirement to file information which leads to filing of beneficial ownership information at a registry with an accountable individual in Poland and where that legal person does not have a bank account.

***Criterion 24.9 – (Mostly met)***

431. While there is no requirement for legal persons themselves, administrators or liquidators to retain the relevant information, there are other measures in place with regard to record-keeping.

432. First, under Article 49 of the AML/CFT Act, obliged entities must retain all CDD information and records for five years after a transaction and five years after the end of a business relationship, albeit that the first year begins from the first day of the calendar year in which the relationship is terminated. This means that records would be maintained in Poland for between four and five years after the dissolution of a company. Second, under Article 12 of the NCR Act, information may not be deleted from the NCR unless the Act provides otherwise, meaning that information must be held permanently. Third, under Article 64 of the AML/CFT Act, information on the CRBO is required to be kept for the period necessary to perform AML/CFT tasks. This does not expressly provide for a precise period of time; the AT was advised that, pursuant to Article 101(1)(2a) of the Criminal Code, the statute of limitations for an ML offence is 15 years after its commission and therefore that the wording of Article 64 of the AML/CFT Act provides for the storage of data in the CRBO for at least this period. Fourth, the NCH is subject to the record-keeping provisions of the AML/CFT Act. The UKNF, GIFI and the KAS advised that they have an (unwritten) approach in the practice of retaining information permanently or for at least the period within which the period envisaged by Article 101(1)(2)(a) of the Criminal Code (bearing in mind the KAS also has direct access to NCH data). In practice, there is limited scope for beneficial ownership records not to be available after the dissolution of a legal person.

***Criterion 24.10 – (Met)***

433. As indicated above, both the NCR and the CRBO are public and are immediately accessible to the authorities. Competent authorities also have power to compel the provision of information by obligated institutions.

***Criterion 24.11 – (Met)***

434. With the exception of joint-stock companies, shares, warrants and other

instruments conferring ownership rights in legal persons have had to be registered. Therefore, shares and warrants could not be issued in bearer form. For joint-stock legal persons, it was possible to issue bearer shares and warrants. However, new amendments to Articles 15 and 17 of the Commercial Companies Code in 2019 specified that the ownership rights of bearer shares and warrants issued by such legal persons would expire on 1 March 2021, and the rights would be registered at latest from that point.

***Criterion 24.12 – (Mostly met)***

435. CDD provisions described in R.10 and R.22 are relevant to identifying persons acting as nominees.

436. There is no concept of nominee director in Polish law. This means that directors are fully responsible for, and cannot delegate, responsibilities that they hold under Polish law, and, by extension, any person exercising control through a director is covered by the directorship provisions.

437. Articles 180, 182, 187 and 188 of the Commercial Companies Code, amongst others, include provisions on pledges and pledgees. Pledgees are analogous to nominees. They may exercise voting rights. A pledge must be made in writing and the signatures notarised (i.e. the pledgee and the nominator (the shareholder) are subject to CDD), and the nominator must notify the company of the pledge and present proof of its existence and terms to the company. The company is therefore made aware of the pledger and pledgee. Any pledge may be made conditional on the company's consent or otherwise restricted by the company. In addition, the company must include in the register of shareholders the fact of the establishment of a pledge and the actual exercise of voting rights by the pledgee. The authorities have noted that the legislation makes it impossible for a pledgee to exercise rights without the knowledge and consent of the company. The provisions on pledges do not apply to cooperatives, associations and foundations; Poland advises there is no ownership right to which a pledge can be attached.

438. Poland has advised that any nominator using a third person as a nominee should be considered as a beneficial owner in practice. Poland has also advised that a positive proportion of legal persons that have provided beneficial ownership information to the CRBO have specified that the information falls within the category of "the exercise of control through other means" as opposed to beneficial ownership by a controlling ownership interest; both legal persons and banks are aware of and responsive to the issue of control.

***Criterion 24.13 – (Mostly met)***

439. The sanctions applicable to obligated institutions for failure to meet AML/CFT requirements are specified in R.27, R.28 and R.35.

440. There is criminal liability in relation to legal persons not keeping basic ownership information accurate and up to date.

441. Failure to provide information to the NCR may result in the initiation of coercive/enforcement proceedings under Article 24 of the NCR Act, in the course of which a fine of up to PLN 10,000 (€2 117) may be imposed on the legal person and each member of the management board. A maximum total fine of PLN 1 million (€ 217 747) can be imposed under Article 1052 of the Civil Procedure Code in relation to a case (no matter how many persons are involved in that case). There is a power in Article 1052 to increase the level of fine in relation to a case for continuing failure to provide information, provided the maximum is not breached. Article 587 of the Commercial Companies Code creates a criminal offence in relation to the provision of misleading information. The Court also has the power of strike off (Article 25a1(3) of the NCR Act). Fines and strike offs are public.

442. There are separate provisions on associations and foundations for failure to provide information. Under Article 2 onwards of the Act on Liability of Collective Entities, fines of between PLN 1,000 (€ 217) and PLN I million (€ 217 747) can be imposed.

443. A legal person that has not submitted a notification of beneficial ownership to the CRBO within a week from registration is subject to a fine of up to PLN 1 000 000 (€217 747) pursuant to Article 153(1) of the AML/CFT Act. The person submitting information to the CRBO also confirms it is correct - the criminal penalty applies to this. There is criminal liability under Article 61(4) for any person providing false information or a fine where this is done unintentionally. In addition, a person submitting information on beneficial owners, including updates, shall be commercially liable for any damage caused by the submission of false data as well as by the failure to report changes in the data within the statutory time limit (Article 68 of the AML/CFT Act).

444. See R.35 for the sanctions framework relevant to FIs and DNFBPs. This framework is not wholly dissuasive with regard to breaches by obligated institutions with regard to CDD. In addition, there are administrative and criminal sanctions available to supervisory authorities and GIFI as FIU for failure by obligated institutions to provide information, late provision of information and non-provision of information.

445. Failure by any person to fulfil an obligation to provide information or the provision of incomplete or untrue information to the KAS is subject to a financial penalty imposed by the Head of KAS of up to PLN 1,000,000 / € 217 747 (Art. 119 zzh and Art. 119 zzk of the Tax Code). This penalty also applies to failure by a bank or credit union to provide information to the NCH.

446. Criminal penalties also apply to failure by any person to provide information, late provision of information or provision of false or misleading information to LEAs and prosecutors. Under Article 233 of the Penal Code, any person who makes a false declaration to the Court is subject to potential imprisonment. In addition, Article 303 of the Penal Code establishes criminal offences for individuals and legal persons for up to three years of imprisonment for failure to document a business activity or by documenting it in an unreliable or false manner, in particular by destroying, removing, concealing, altering or falsifying documents regarding such activities.

***Criterion 24.14 – (Mostly met)***

447. Basic information on the NCR and beneficial ownership information on the CRBO is immediately accessible online to the authorities in other jurisdictions. As associations, foundations and cooperatives are not yet covered by the CRBO framework, and it cannot be certain that all beneficial ownership information for these legal persons is held on the NCR, R.37 to R.40 are relevant to these persons.

***Criterion 24.15 – (Mostly met)***

448. The authorities operate within a national initiative to address fictitious companies. They have been effective, which has entailed significant checking of data and using foreign open and confidential sources of information to help check data and facilitate operational cases. The quality of information received in response to requests is monitored by Poland within the context of the national initiative to move forward operational activity and to reduce misuse of legal persons. While formal written procedures are not in place, officers assess the information received against the information requested (bearing in mind that basic information registries are public and, in some countries, there are public registers of beneficial owners, so information needed is easily accessible by website and used by Poland). Also, see IO.5. The effectiveness of monitoring by the Moj (which acts as the central authority with regard to co-operation

with non-EU countries - see R.37) is uncertain.

### ***Weighting and Conclusion***

449. Poland has recognised the main risk of misuse of legal persons, and a national programme has been established on the basis of this recognition, including the establishment of a central register of beneficial ownership and modification of the framework for the NCH, so that information on beneficial owners of bank accounts is held centrally. All but one of the fifteen criteria of the Recommendation are met or mostly met. Overall, there are minor shortcomings, with the risk and materiality of the shortcomings generally mitigated by contextual factors. **R.24 is rated Largely Compliant.**

### ***Recommendation 25 – Transparency and beneficial ownership of legal arrangements***

450. In the 4<sup>th</sup> round MER of 2013, Poland was rated N/A on R34. This was on the basis that there was no provision in domestic law for the creation of trusts.

451. By way of risk, materiality and context, the information held by obligated institutions, the GIFI and the UKNF shows that there are few cases of establishing business relations with trusts. In addition, analysis of transactions conducted by the KAS does not reveal any such cases.

#### ***Criterion 25.1 and 2 – (Mostly met)***

452. Poland is not a signatory to the Hague Convention on Laws Applicable to Trusts and on their Recognition. There is neither a law governing trusts nor other types of legal arrangements, thus sub-criteria (a) and (b) are not applicable. With regard to sub-criterion (c), according to Article 2(1)(16) of the AML/CFT Act, any professional trustee of a trust created under foreign law (or a person enabling another person to act as a professional trustee), is considered to be an obligated institution and is therefore required to apply and to document CDD measures (Article 34(4)), and to keep the collected documents for a period of five years after the business relationship is terminated – although the period starts from the first day of the year in which the relationship is terminated, which could mean between four and five years in practice (Article 49(1)). As sub-criteria (a) and (b) are not applicable and only sub-criterion (c) is applicable, the relevant information pertains to a relationship the trustee no longer has. The same approach applies to Article 2(14) of the AML/CFT Act, which brings attorneys, legal advisers, foreign lawyers and tax advisers within the scope of being obligated institutions – and the record-keeping requirements – when they are establishing, operating or managing trusts. See c.10.7 and R.22.1 on keeping records up to date. GIFI and the UKNF have advised that banks keep records on business relationships for longer than the minimum requirement in the AML/CFT Act.

#### ***Criterion 25.3 – (Partly met)***

453. The AML/CFT Act (Art. 34) requires obliged entities to undertake steps to define the ownership structure of a customer that is a legal arrangement when entering into a business relationship or carrying out an occasional transaction, including identifying beneficial owners (defined at Art. 2 as including trustees). However, there is no legal, explicit requirement for trustees or other persons involved with legal arrangements to disclose their status to obliged entities. The Polish authorities consider that Article 34 means that a trustee will have to disclose his status. They also consider that a trustee who, while representing the interests of the trust, wishes to carry out a transaction or establish business relations with an obligated institution, will (as a person authorised to act on behalf of the trust) have to provide authorisation for such actions. The lack of a literal

provision obliging trustees to disclose their status to obligated institutions is not seen by Poland as constituting a loophole in the national legal system, due to the obligation to identify persons acting on behalf of the client of an obligated institution, and that a trustee who will not disclose its status to the obligated institution will not be able to carry out transactions or establish business relations with such an obligated institution (and also potentially cause legal difficulties vis a vis the trustee's relationship with the trust and the use of trust assets).

***Criterion 25.4 - (Met)***

454. There is nothing in Polish law or other enforceable means to prevent trustees or equivalent officers of other legal arrangements from providing information to the authorities or to obliged entities.

***Criterion 25.5 - (Met)***

455. Under Article 76(1) of the AML/CFT Act, obliged entities must make available to the GIFI upon request customer due diligence information, which in cases where the customer is a legal arrangement would include beneficial ownership information about that legal arrangement. LEAs may receive relevant information on the basis of general provisions which regulate operation thereof (the Act on the Police, the Act on the ISA, the Act on the Central Anti-Corruption Bureau, etc.), under preparatory proceedings they may receive information on the basis of provisions of the Criminal Procedure Code.

***Criterion 25.6 - (Met)***

456. Information on legal arrangements, including beneficial ownership information, may be provided by the GIFI in the course of international information exchange under Articles 110-116 of the AML/CFT Act (see under R40 for further details). This must be provided within 30 days but can be provided more quickly in urgent cases if the information is already in possession of the GIFI.

***Criterion 25.7 - (Met)***

457. Under Article 2(1)(16)(d) of the AML/CFT Act, entrepreneurs within the meaning of the Act of 6 March 2018 - Entrepreneurs' Law who act as trustees are obliged entities. They are therefore subject to the obligations under the AML/CFT Act and also to the administrative penalties for breach of those obligations at Articles 147-149 of the AML/CFT Act. These penalties include public statements, prohibition on carrying out specific actions, the removal of a licence or permit, prohibition from acting in a managerial position for up to a year, and a financial penalty (which may be up to twice the benefit received as a result of the breach, or up to €1 million where this cannot be determined). However, there are no obligations in place for trustees that are outside the scope of the 6 March 2018 - Entrepreneurs' Law or for the equivalent officers of other legal arrangements.

***Criterion 25.8 - (Mostly met)***

458. Failure to respond to requests for information by the UKNF, the provision of information after deadlines set by the UKNF and the provision of misleading information is subject to administrative and criminal penalties - Articles 141(1) and 171(4) of the Banking Act and corresponding provisions in the Payment Services Act; the Act on Trading in Financial Instruments; the Act on Investment Funds; and the Act on Insurance and Reinsurance Activities; and Article 74v of the Act on Cooperatives and Credit Unions. However, Article 74v applies to information provided to the UKNF and not the NACSCU.

459. To the extent that persons representing entities supervised by the UKNF fail to provide required information promptly, which may hinder the investigative or criminal

proceedings, they are also subject to sanctions in Articles 20a or 20b of the Act on Financial Market Supervision.

460. The KAS has power to impose administrative penalties under the Tax Code for non-provision or late provision of information or for the provision of misleading information (see c.24.3).

461. Articles 147 and 156 apply administrative penalties for failure by any obligated institution to provide information and criminal penalties for provision of false or misleading information to GIFl.

462. Failure to comply promptly with requests for information by LEAs (and prosecutors) is subject to criminal liability.

463. LEAs can obtain information that may constitute evidence in preparatory proceedings pursuant to Article 217 of the Code of Criminal Procedure, according to which items that may constitute evidence in a case should be provided at the request of the court or the prosecutor, and in urgent cases also at the request of the Police or another authorised body. This provision is relevant to any person who possesses information, and therefore applies to trustees as well as to any other person who has information on trusts. Failure to fulfil the obligation specified in Article 217 promptly may result in the imposition of a fine pursuant to Art. 285(1) in conjunction with Article 287(1) of the Code. In addition, a person who does not provide information to LEAs may be assessed as obstructing preparatory proceedings, which in accordance with Articles 239 and 303 of the Criminal Code, is punishable by imprisonment.

464. For supervisory authorities and GIFl, the provisions apply in relation to information on trustees/trusts in relation to customer relationships of obligated institutions, while the provisions with regard to LEAs and prosecutors apply to any person.

### ***Weighting and Conclusion***

465. There are few cases of establishing business relationships with trusts. Professional trustees and other obligated institutions under the AML/CFT Act (including lawyers providing legal assistance in relation to establishing, operating or managing trusts) are subject to the CDD and record-keeping requirements of the Act and to statutory obligations to provide information to the Polish authorities. There are minor shortcomings. **R. 25 is rated Largely Compliant.**

### ***Recommendation 26 – Regulation and supervision of financial institutions***

466. In the 4<sup>th</sup> 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 cooperative savings and credit unions.

#### ***Criterion 26.1 – (Mostly met)***

467. Under Article 130(1) of the AML/CFT Act, the GIFl 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 Union (NACSCU) and the UKNF over credit unions and by the KAS in relation to obligated institutions controlled by these bodies.

Value transfer providers are not covered by the framework (see R.14). The discharge of these overlapping supervisory responsibilities is coordinated by the GIFI under Article 132 of the AML/CFT Act.

***Criterion 26.2 – (Mostly met)***

468. 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.

469. Non-bank lenders have been required to register with the UKNF since 2017, although the registration process is automatic.

470. Other types of financial institutions (such as factoring businesses) and VASPs are 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). In addition, value service provision is not covered by the framework.

***Criterion 26.3 – (Partly met)***

471. 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. 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. With regard to other members of senior management, 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. 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.

472. 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 AIFs, 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. In addition, as mentioned above, non-bank lenders have been required to register with the UKNF since 2017, although the registration process is automatic. Please see c.26.2 for other types of financial institutions (such as factoring businesses) and VASPs.

473. 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 the AT has been advised that the NBP controls compliance with these Articles, 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. In addition, there is no legal requirement in relation to beneficial owners (unless they are a shareholder/partner) or where a person is an associate of a criminal. The AT has been advised 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, but it is not clear to the AT which Article provides this power.

474. 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. It is not clear to the AT how a president who fails to meet the requirements in relation to offences subsequent to appointment could be removed by the supervisor once authorisation has been given. There are no authorisation requirements for other members of the management board or members of the supervisory board, although it is not clear to the AT to what extent Articles 7 and 18 allow a de facto authorisation requirement. There are also 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.

475. 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.

***Criterion 26.4 - (Partly met)***

476.

- (a) See c26.1 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. Poland was reviewed under the FSAP programme in 2018. The AT has not received information that expressly addresses footnote 78 of the FATF methodology.
- (b) Not all non-core FIs are covered by the framework; value transfer services are not covered, although the Polish authorities have advised that no value transfer 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 and 2019. The supervisory programme for such institutions has been reduced since then. The UKNF's supervisory programme has good risk-based elements; there are recommendations in IO.5 for its development so that it is comprehensively risk-based. GIFI also has a risk rating methodology for FIs; its approach to supervisory engagement of payment institutions is less comprehensive than that of the UKNF,

not least because of a staff shortfall – also see IO.5.

**Criterion 26.5 – (Partly met)**

477. 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 coordinating role, the GIFI must make information available to other supervisors annually on areas and sectors particularly exposed to the risk of money laundering or terrorist financing. 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).

478. 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.

479. 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.

480. Looking at each supervisor in turn:

- (a) The UKNF has a risk tool (ORION) and has issued a guideline which it uses to assess the risk of each institution. Section 2 of the guideline states that risk categorisation allows for optimisation of measures by targeting them primarily at entities with higher exposure to ML/TF risk. The risk assessment itself includes assessment of risk management and (as a lesser criterion having the lowest weight) information about compliance with internal procedures as part of the scoring. It develops an annual plan to meet the GIFI's guidance based on risk. There is scope for a more sophisticated approach. In addition, the guideline does not refer to the intensity of supervision and meets sub-criteria (a) and (c) to a limited extent, although the sub-criteria form part of supervisory engagement in practice.
- (b) GIFI assesses the ML/TF risk of each FI using a methodology. The methodology meets sub-criteria (a) and (c) to a limited extent, although the sub-criteria form part of supervisory engagement in practice.
- (c) The NBP assesses the risk of each currency exchange office. It has issued a methodology which it uses to assess the risk of each office. 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. In addition, the guideline does not refer to the intensity of supervision and meets sub-criteria (a) and (c) to a limited extent, although the sub-criteria form part of supervisory engagement in practice.
- (d) The NACSCU undertakes risk assessment of each credit union, and the 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.

- (e) Further information can be found in IO.5. There is scope for the UKNF, GIFI and NBP to develop more comprehensive approaches to risk assessment and supervision.

#### ***Criterion 26.6 – (Partly met)***

481. The UKNF, GIFI 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 also reviews the risk scoring for each entity on an annual basis and as a result of trigger events. GIFI also reviews its risk ratings every six months; trigger events do not lead to a reconsideration of ratings. The NBP reviews its risk ratings annually. There is no written policy or procedure in relation to the frequency of review assessment of a FI's risk rating. The AT has not been provided with information about the NACSCU.

#### ***Weighting and Conclusion***

482. There are a few gaps in the scope of coverage of FIs of the requirements in c.26.1 and c.26.2. There are some gaps in relation to market entry requirements for preventing criminals and their associates from beneficially owning or otherwise controlling FIs. The AT has not yet received information on to what extent core principles institutions are supervised in line with core principles requirements. There are gaps at the technical level with regard to meeting the precise language of the FATF on the components of risk-based supervision, and supervision itself is not wholly risk-based. **R.26 is rated Partially Compliant.**

#### ***Recommendation 27 – Powers of supervisors***

483. In the 4<sup>th</sup> round MER of 2013, Poland was rated LC for R.29. No technical deficiencies relating to the powers of supervisors were identified. However, the gap in relation to value transfer highlighted in R.14 and R.26 is also relevant to R.27.

#### ***Criterion 27.1 – (Mostly met)***

484. Articles 130(1) of the AML/CFT Act requires GIFI to exercise control of obligated institutions' compliance with AML/CFT obligations. Under Articles 133 to 145, inspectors from the GIFI have powers to supervise, monitor or enforce compliance with AML/CFT obligations by financial institutions. Under Article 130(2), control shall also be exercised under the terms of separate provisions by the NBP under the Foreign Exchange Act in relation to currency exchange operators, the UKNF under the Act on Financial Market Supervision (Article 1(2)) in relation to obligated institutions it supervises and the NACSCU (Article 63 of the Act on Cooperative Savings and Credit Unions). In practice, these other supervisors are monitoring AML/CFT compliance. It is not clear to the AT what power the NACSU has to enforce compliance in line with this criterion (noting as well that the UKNF also has a supervisory role in relation to credit unions). Under Article 132 of the AML/CFT Act, GIFI coordinates control of FIs by means of an annual control plan.

#### ***Criterion 27.2 – (Mostly met)***

485. The power to conduct onsite inspections for AML/CFT purposes is provided for in the case of GIFI inspectors under Article 135 of the AML/CFT Act. Under Article 130(2), AML/CFT control shall also be exercised under the terms of separate provisions by the NBP under the Foreign Exchange Act in relation to currency exchange operators, the UKNF in relation to obligated institutions it supervises and the NACSCU.

486. UKNF is empowered to conduct supervisory actions under Art. 3 (1) and 4(1-7) of the Act on Financial Market Supervision; the Act refers to “inspection activities” in Art. 133(3) and 133(4).

487. With regard to the currency exchange sector, the NBP is able to conduct inspections on the basis of Articles 33 to 35 of the Foreign Exchange Law Act and Articles 45 to 59 of the Entrepreneurs’ Law, and the delegation indicated in Article 130(2) of the AML/CFT Act.

488. With regard to the credit union sector, Articles 62h (power to request information) and 63 (control of credit unions for conformity with the law) of the CSCUs Act are relevant. It is not clear to the AT how the NACSCU is able to use these provisions to conduct inspections.

***Criterion 27.3 – (Mostly met)***

489. The GIFI has power to compel the production of information relevant for monitoring compliance with AML/CFT requirements under Article 76 of the AML/CFT Act. Article 130(2) of the Act provides that control by other supervisors shall be exercised under separate provisions. This includes the application of the information gathering powers available to supervisors under sectoral legislation they administer. While the UKNF has the ability to compel production of information under the CSCUs Act, under Article 62h of the Act, the NACSCU may request information to be provided to it in order for the NACSCU to meet its tasks, but there is no penalty applicable to failure to provide information to the NACSCU.

***Criterion 27.4 – (Mostly met)***

490. Under Articles 147-150, and subject to Article 151 AML/CFT Act, FI supervisors may impose administrative penalties on obligated institutions for breach of AML/CFT obligations in Articles 147 and 148. These penalties include public statements (Article 150(1)(1)), orders to cease taking specific actions (Article 150(1)(2)), revocation of a licence, permit or registration (Article 150(1)(3)), prohibition on holding a managerial position for up to a year (Article 150(1)(4)), and financial penalties (Article 150(1)(5)). Financial penalties have two tiers, general and specific. First, the general approach is that financial penalties may be up to twice the level of the benefit generated by the breach, or up to €1 million where this cannot be determined. The second tier is that, under Article 150(5), this provision is discounted (i.e. falls away) for most FIs, in relation to which financial penalties may instead be imposed of up to €5 million (up to a maximum of 10% of turnover) for an entity. However, there is no power to suspend a licence (specified in the criterion). There is also no power to require an obligated institution to take specific actions.

491. Under Article 151, the UKNF is empowered to impose the full range of administrative penalties provided for in Article 150(1). However, by virtue of Article 151, not all of the penalties under Article 150 are available to all supervisors. The NBP can impose all sanctions specified in Article 150(1), except for the prohibition on holding a managerial position for up to a year (Article 150(1)(4)). The GIFI may only impose public statements, orders to cease taking specific actions and financial penalties (Article 150(1), (2) and (5)). It also has the power to issue public statements under Article 152 in relation to any administrative penalty issued by any supervisor. The NACSCU has no power to impose penalties on the entities it supervises.

492. Article 154 also permits the imposition of a financial penalty by the UKNF, the GIFI and the NBP of up to PLN 1 million (€220 000) for breach of Articles 6 to 8 (appointment of a compliance officer). This power by itself is not proportionate (even though the GIFI

would also seem to have power to issue a public statement under Article 152). It is not clear to the AT how this power to impose financial penalties ties in with the power in Article 150.

493. The implications of Articles 147, 148 and 154 in not covering some Articles relevant to compliance by obligated institutions with the FATF Recommendations are uncertain.

494. In addition, pursuant to Article 153(2)(1) in connection with Article 129 of the AML/CFT Act, there is a penalty available for failure by a person to provide a certificate of absence of conviction for an intentional crime or an intentional fiscal offence.

495. The coverage and range of sanctions are not comprehensively proportionate and dissuasive.

### ***Weighting and Conclusion***

496. The AML/CFT Act grants most of the supervisory authorities the powers required by this Recommendation, although, more generally, there is no power to suspend a license nor to require an obligated institution to take action. The powers of sanction are not wholly proportionate and dissuasive. Substantial weight is not attached to the NACSCU as the UKNF (and GIFI) also has supervisory authority over the same institutions as the NACSCU. **R. 27 is rated Largely Compliant.**

### ***Recommendation 28 – Regulation and supervision of DNFBPs***

497. In the 4<sup>th</sup> round MER of 2013, Poland was rated LC for R24. The technical deficiencies identified were the lack of supervision of TCSPs and certain activities of notaries were not subject to AML/CFT obligations.

498. SRBs do not have supervisory powers in the scope of AML/CFT. We can mention only the supervisory authorities in the scope of AML/CFT in relation to gambling entities, i.e. the GIFI, Customs and Tax Control Offices etc. Relevant SRBs have only powers in the scope of representation of entities and possible co-operation with the GIFI or dissemination of information in the scope of AML/CFT.

#### ***Criterion 28.1 – (Partly met)***

499. Casinos are required to be licensed by the Ministry of Finance under the Act of 19 November 2009 – Gambling Act.

500. Under Article 11 of the Act, there must be no justified reservations about AML/CFT compliance in relation to persons holding 10% or more of the shares in a company conducting the activities of a casino, the members of the management board, supervisory board or audit committee of the company and any legal representative of the company. In addition, Article 12 requires that all such persons must have an impeccable reputation, and in particular, must not have been convicted of an intentional offence or a fiscal offence within the EU. Changes of shareholders and these posts must be advised to the MoF within seven days of the change. The MoF is able to remove any shareholder and any person occupying these posts (Art. 53(1)).

501. However, (i) these requirements do not apply to the beneficial owners of companies or other entities that operate casinos (although legislation is currently in train to address this) ; (ii) the provisions do not apply to management below the level of the management or supervisory boards; (iii) there are no express measures in place to prevent the associates of criminals from involvement in the ownership or operation of casinos although the reference in Article 12 to impeccability of reputation might be of

assistance in addressing associates.

502. Casinos are obligated entities under Article 2(1)(20) of the AML/CFT Act, and their compliance is subject to the supervision of GIFI under Article 130(1) of the AML/CFT Act and the Heads of KAS under Article 130(2)(1)(e) of the AML/CFT Act and Articles 54(1)(3) to (3a) of the Act on National Revenue Administration. Under Articles 133 to 145, inspectors from the GIFI have powers to supervise and enforce compliance with AML/CFT obligations by DNFBPs.

***Criterion 28.2 – (Partly met)***

503. Other DNFBPs are obliged entities under the AML/CFT Act and are supervised as follows:

- Real estate agents –compliance with the AML/CFT Act is subject to the supervision of GIFI under Article 130(1);
- Dealers in precious metals and stones - these are entrepreneurs within the meaning of the Act of 6 March 2018 – Entrepreneurs Law and as such are defined as obliged entities under Article 2(1)(23) when they make or receive cash payments of €10 000 or more; compliance with the AML/CFT Act is subject to the supervision of the GIFI under Article 130(1);
- Notaries - defined as obliged entities under Article 2(1)(13); compliance with the AML/CFT Act is subject to the supervision of the GIFI under Article 130(1) and of the Presidents of the Appeal Courts under Article 130(2)(1)(d);
- Lawyers, other independent legal practitioners and accountants - defined as obliged entities under Article 2(1)(14), Article 2(1)(15) and Article 2(1)(17) (although accountants are captured in light of the EU framework and are not able to undertake activities which the FATF attaches to accountants); compliance with the AML/CFT Act is subject to the supervision of the GIFI under Article 130(1);
- TCSPs - entrepreneurs within the meaning of the Act of 6 March 2018 – Entrepreneurs Law (other than other obliged entities) that provide services relating to legal persons or arrangements are obliged entities under Article 2(1)(16). In addition, lawyers and tax advisors involved in the establishment, operation or management of capital companies or trusts are obliged entities under Article 2(1)(14)(e); Compliance with both Article 2(1)(16) and Article 2(1)(14)(e) is subject to the supervision of GIFI under Article 130(1);

504. Additionally, while GIFI has a lead role, control in relation to any DNFBP may be exercised by the KAS. However, there are no registration or market entry requirements, except the requirement for corporate entities to be registered at the NCR, for some DNFBPs (i.e. real estate agents, DPMS and any TCSPs) except for lawyers and notaries, and this has a negative underlying effect on the ability to exercise their powers in relation to such entities.

***Criterion 28.3 – (Partly met)***

505. See c.28.2. Under Articles 130, 133 to 145, inspectors from the GIFI have powers to supervise and enforce compliance with AML/CFT obligations by DNFBPs. The absence of registration or market entry requirements, except the requirement for corporate entities to be registered at the NCR, for some types of DNFBP has a negative underlying effect on the ability of GIFI and the KAS to exercise their powers of designation.

***Criterion 28.4 – (Partly met)***

506. (a) See R.27 for the powers of the GIFI. Explicit powers for the President of the Appeal Court in relation to notaries, which also has power to exercise control at Article 130(2), are not contained in the Act. Instead, the President performs supervision in relation to notaries and notarial bodies under the provisions of Regulation of the Minister of Justice of 30 April 1991 on the procedure of supervision of the notaries and the bodies of the professional organisation of notaries and other provisions issued pursuant to the Notary Act. There is a specific power for the MoJ to define the powers of supervision at Article 42 of the Notary Act. The powers available to the Presidents of the Appeal Courts appear to include the ability to undertake onsite inspections as a substantial number have been undertaken, but otherwise, the AT is not sighted on the powers which are available.

507. (b) Under Article 129 of the AML/CFT Act, a natural person who has been convicted of an intentional crime or an intentional fiscal offence may not be the beneficial owner, partner or shareholder of an obligated institution referred to in Article 2(1)(16) (i.e. an entrepreneur providing TCSP services) or under Article 2(1)(18) (i.e. a real estate agent). Such a person is also prohibited from conducting activities within the scope of the Act or from holding a management position with, respectively, a person providing TCSP services or real estate agency services.

508. In addition, under Article 129(2) of the AML/CFT Act, at the request of the GIFI or any supervisor with authority under Article 130(2) of the Act, beneficial owners, partners or shareholders of entrepreneurs providing TCSP services and or real estate agents must produce a certificate confirming that they have not been convicted of an intentional crime or an intentional fiscal offence. According to Article 153(2) of the AML/CFT Act, failure to comply with such a request for a natural person referred to in Article 129 is subject to a financial penalty of up to PLN 10 000 (€2 200) (which the AT does not consider to be sufficient). However, the power is passive rather than requiring routine consent or authorisation by a supervisor, and it is not clear what legal provision would allow a supervisor to remove a person who cannot or does not provide a certificate. There are also no corresponding measures in place with regard to persons actually conducting the activities within the scope of Article 2(1)(16) or Article 2(1)(18) or from holding a management position with the types of obligated institutions referred to in these Articles. There are also no measures to prevent the associates of criminals from involvement in the ownership or activities of these types of obliged entities.

509. Article 129(2) (and the issue mentioned in the paragraph above) is also applicable to market entry measures in place for other DNFBPs. However, there are powers in Article 11 of the Notary Act which require notaries to have irreproachable character. The same test applies to lawyers and advocates.

510. The AT has also been advised that certain SRBs are able to license and monitor compliance of the obligated institution with the obligations imposed on it, e.g. lawyers, tax advisers, notaries, and real estate agents. Copies of any relevant legal provisions have not been provided to the AT.

511. (c) By virtue of Article 151, the GIFI can use some of the powers of sanction available at Article 150 of the AML/CFT Act. These are: publication of information, an order to cease undertaking specific activities and financial penalties. The GIFI does not register obligated institutions, so it cannot use the sanction of revocation of a licence. Real estate agents, DPMS and any TCSPs are not required to be registered with a monitoring or supervisory body, although the NCR requirements are applicable for corporate entities. The AT considers the absence of powers to suspend registrations of those entities which are registered and to require an obligated institution to undertake specific acts to be a gap.

In addition, as mentioned above, the financial penalty attached to failure to provide a certificate in relation to criminality is not dissuasive.

512. It is not clear to the AT which of the powers in Article 150 of the Act can be used by the President of the Appeal Court in relation to notaries or whether the President has other powers of sanction which might be applicable. The President of the Appeal Court does not have the power to impose sanctions for failure to comply with AML/CFT requirements. However, pursuant to Article 150(1)(1) of the AML/CFT Act, the GIFI shall impose administrative penalties referred to in Article 150(1)(1), (2) and (5) in the scope of infringements found as a result of control referred to in Article 130(2)(1)(d). There are sanctions available in Article 51 of the Notary Act which relate to breaches of that Act.

513. Article 154 permits the imposition of a financial penalty by the GIFI, the NBP and the UKNF of up to PLN 1 million (€220 000) for breach of Articles 6 to 8 (appointment of a compliance officer). This power by itself (i.e. as the only power) is not proportionate.

514. The implications of Articles 147, 148 and 154 in not covering some Articles of the AML/CFT Act relevant to compliance by obligated institutions with the FATF Recommendations are uncertain.

#### ***Criterion 28.5 – (Partly met)***

515. 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. These legal provisions deal with the generality of ML/TF risks. DNFBPs are subject to a sectoral risk rating by GIFI but are not individually risk rated. The Appeal Courts undertake routine onsite supervision of notaries. The KAS has undertaken some onsite inspections. GIFI undertakes AML/CFT supervision of DNFBPs by undertaking ad hoc inspections on the basis of risk-based triggers. See IO.5. There are no policies and procedures additional to the provisions in the Act which address the particular language of sub-criteria.

#### ***Weighting and Conclusion***

516. There are gaps in controls in relation to preventing control of casinos by criminals. There is also absence of registration (beyond registration of corporate entities at the NCR) and requirements to prevent criminals and their associates from professional practice or control of several types of DNFBP, which negatively affects supervisory designation in practice and the ability to exercise supervisory powers. There are also gaps in relation to supervisory powers. Beyond a generic power in the AML/CFT Act, there are no risk-based policies or procedures, no individual risk rating of DNFBPs and risk-based supervision is limited. **Poland is rated Partially Compliant with R.28.**

#### ***Recommendation 29 - Financial intelligence units***

517. In the 2013 MER, Poland was rated LC with the former R.26. Deficiencies pertained to the outdated guidance on the manner of reporting and the lack of provisions to ensure that the GIFI maintains confidential any information received in the performance of his functions following the termination of his appointment.

#### ***Criterion 29.1 – (Met)***

518. Article 10 of the AML/CFT Act sets out that Competent government administration authorities in charge of counteracting money laundering and financing of terrorism,

hereinafter referred to as “financial information authorities”, as: i) the minister competent for public finance, as the supreme financial information body; ii) the GIFI.

519. According to Articles 74 and 86, the GIFI is responsible for receiving information on ML/TF suspicions (see analysis under R.20). Other tasks of GIFI are set out under Article 12 of the AML/CFT Act and include analysis and dissemination of information. According to Article 12(2) of the AML/CFT Act, the GIFI shall perform his/her duties with the assistance of an organisational unit established for this purpose within the structure of the office providing services to the minister competent for public finance.

***Criterion 29.2 – (Met)***

520. (a) In line with article 74 of the AML/CFT Act, the reporting entity shall notify the GIFI of any circumstances which may indicate the suspicion of committing the crime of ML or TF. An additional reporting requirement is set under article 86(1)-(3) of the AML/CFT Act, which provides that the obligated institution shall immediately notify the GIFI when there are justified suspicions that a specific transaction or specific assets may be associated with ML or TF.

521. (b) According to Article 72 of the AML/CFT Act, the reporting entities shall provide the GIFI with information on the following transactions: - accepted payment or executed disbursement of funds exceeding the equivalent of €15 000; - executed transfer of funds exceeding the equivalent of €15 000.

522. The obligation shall also apply to the transfer of funds initiated outside the territory of the Republic of Poland to the benefit of a recipient for whom the obligated institution acts as a payment service provider. The reporting entities shall provide the GIFI with information concerning the executed purchase and sale transaction of foreign currency with a value exceeding the equivalent of €15 000 or intermediation in performing such transaction. The notaries provide the GIFI with information concerning the above-described activities with a value exceeding the equivalent of €15 000. Pursuant to Article 85(1) of the AML/CFT Act, the Border Guard authorities and KAS authorities shall provide the GIFI with information arising from declarations of cross-border cash transportation across the EU border.

***Criterion 29.3 – (Met)***

523. The GIFI is entitled (Article 76 of the AML/CFT Act) to demand the reporting entities to submit or make available any information or documents required for the implementation of the GIFI’s tasks.

524. According to Article 82.1 of the AML/CFT Act, at the GIFI’s request, cooperating units<sup>88</sup> are within the scope of their statutory competence to provide or make available any information or documents held. The GIFI also has direct/indirect electronic access to a broad range of information and databases.

***Criterion 29.4 – (Met)***

525. a) According to Article 12(1)(1), the GIFI analyses information related to assets, in relation to which there are suspicious of association with ML or TF. The broad definition includes all the elements listed in 29.1(a), which was confirmed during the onsite visit. To assist its operational analysis, during the first stage of analysis (pre-analysis) the FIU uses the SIGIF (the Information System of the GIFI- database for identifying any links with

---

<sup>88</sup> Under Article 2(8) of the AML/CFT Act as cooperating unit is considered any government and local government authorities and other state organisational units as well as Narodowy Bank Polski (NBP), the Komisja Nadzoru Finansowego (KNF) and the Supreme Audit Office (NIK).

previous analytical cases), requests from cooperating units or foreign FIUs. The SIGIIF is used to gather the following information from reporting entities: over threshold transaction reports; SARs; additional information specifically requested by GIFI. The system also gathers cash transport declarations data from the border guard. During active analysis, the FIU makes use of its power to request additional information from obligated institutions, cooperating units, foreign FIUs, internal databases that the GIFI can access, open sources – open databases, social media, websites, news outlets etc.

526. b) According to Art. 15 of the Internal Organisational Regulation of GIFI, the Data Modelling Unit shall perform strategic analysis of information in order to identify patterns and trends related to ML/TF and identify the areas and degrees of risk related to ML/TF. The same Unit shall conduct, *i.a.* statistical analysis of information submitted to the GIFI by electronic means; statistical quality control of data submitted to the GIFI by electronic means; and prepare and test models and analytical streams for automatic analysis of threshold transactions and other information available in the GIFI databases.

#### ***Criterion 29.5 – (Met)***

527. If the justified suspicion of committing a crime of ML or TF arises from the information held by the GIFI or from the processing or analysis of such information, the General Inspector shall submit to the competent prosecutor a notification which shall include the supporting information or documents (Article 103(1) of the AML/CFT Act). In addition, the GIFI shall make available the information in his/her possession on a written and justified request from the competent authorities (including law enforcement authorities) listed under Article 105 of the AML/CFT Act.

528. An independent, dedicated and secured IT system is used for the exchange of information between the GIFI and the prosecutors' offices which is managed by the Public Prosecutor's Office. The system enables the GIFI to send notifications promptly to prosecutors, together with all attached evidence, which is particularly important in cases of the GIFI requesting blocking an account or suspending a transaction. The prosecutors use this system to send the GIFI requests for information. Communication with the prosecutors' offices can also be conducted via dedicated, secure e-mail boxes. This mode of exchange is a parallel one and is used mainly for sending notifications about the possibility of committing a crime or, in urgent cases.

529. For exchange of information between the GIFI and Internal Security Agency, a dedicated and secured IT system is used – CATEL, which is managed by the ISA.

530. In particular cases, the information is shared via classified correspondence with the "restricted" clause.

#### ***Criterion 29.6 – (Met)***

531. a) Provisions related to classified information are set by the Act of 5 August 2010 on the protection of classified information (consolidated text: Journal of Law 2019, item 742). The GIFI possess its own internal classified rules in place related to the security and confidentiality of information processed in its system. The IT system of GIFI is designed to process confidential information up to a restricted level, and it has valid accreditation from Internal Security Agency to process such information. All workstations with access to the GIFI system are located in secure zones. Access to these zones is monitored and logged. Access to data is limited to personnel employed by GIFI, all of whom have current security clearance. Data transfers to and from computers in the GIFI system are monitored, users are accountable for all transfers. All activities in the GIFI system are subject to internal security regulations. Those regulations are regularly revised.

532. b) All personnel of the Department of Financial Information must undertake a

security clearance process, which allows them access to the level of classified information required for their particular role. All security clearances are regularly reviewed and updated. Employees undertaking proceedings related to the access to secret and top-secret information, the EU or NATO clauses, shall be subject to the enhanced inspection procedure. According to domestic regulation on protection of confidential information, staff members must have valid security clearance and a certificate of attendance in a training session on regulations on protection of confidential information. The employees are given rigorous ongoing training directed at protecting personal and other sensitive information. Before receiving access to the system for the first time, each staff member must attend a lecture on procedures of safe use.

533. c) The FIU premises are separated from the rest of the Ministry of Finance building, and only the FIU employees can enter the premises by using personalised cards. Also, access to visitors is limited and registered by the secretariat of the Department of Financial Information. Physical access to facilities is limited in accordance with domestic regulations on protection of confidential information; this includes visual monitoring of access routes, 24/7 presence of security guards in the building, intrusion alarm on doors and windows, access control system with magnetic locks on doors to FIU corridors. Access to the IT system requires authentication with password. User-accessible parts of FIU's IT system are on an isolated network; copying information to removable media leaves audit trail; accessing case information, modifying case and subject information, and performing searches case subjects leaves audit traces.

534. The premises of the FIU are divided into zones with limited access. The FIU acts under the special procedures of behaving within the zones and special procedures for cases of emergency.

535. In addition to this, a special position was created as part of the Department of Financial Information dedicated to handling the separated GIFI archive. GIFI documents are collected in a separate archive dedicated to him exclusively, with limited access only by authorised employees of the Department.

***Criterion 29.7 - (Met)***

536. (a) The GIFI shall be appointed and dismissed by the Prime Minister at the request of the Minister of Finance, Development Funds and Regional Policy. After seeking the opinion of the minister - member of the Council of Ministers competent for coordination of the activity of special forces, if appointed by the Prime Minister. The authority of the GIFI to analyse, request and/or forward or disseminate specific information is set out under Article 12 of the AML/CFT Act. The Polish FIU is an administrative type located in the structure of public administration. Therefore, the employment of its staff is being regulated by the Civil Service Act, and hence, any process of recruitment or dismissal is based on the provisions of the said Act. The management of the Department of Financial Information has authorisation of the GIFI to take decisions in relation to the analysis of SARs, sending requests for additional information to obligated institutions, submission or making available of the documents to competent authorities.

537. (b) According to Article 17. 1. of the AML/CFT Act, the GIFI may conclude agreements with entities other than obligated institutions in the scope of collecting information significant for the execution of his/her duties. According to Article 116(1), in the framework of its co-operation with the competent authorities of other countries, foreign institutions and international organisations dealing with counteracting ML/TF and the European supervision authorities, the GIFI may acquire and make information available. In order to implement the co-operation, the GIFI can conclude agreements defining the procedure and the technical terms of acquiring and making information

available.

538. (c) The core functions of the GIFI are set out under the AML/CFT Act. In accordance with Article 12.2, the GIFI shall perform his/her duties with the assistance of an organisational unit established for this purpose within the structure of the office providing services to the minister competent for public finance. The Department of Financial Information is the unit created for this purpose within the Ministry of Finance. It should be highlighted that the Department has its own legal and IT staff, which provides a degree of autonomy from the services provided at ministerial level.

539. (d) The Polish FIU does not have its own budget; it is authorised as the unit placed in the structure of the Ministry of Finance to reserve the funds for its own expenditures, which are planned for the next year (for the purchase of software and hardware, maintenance of hardware, data security, training, international and internal relations and Egmont Group membership fees).

540. The FIU as such does not have its own separate structure responsible for accounting of incurred expenses; thus, they are handled by the Finance and Accounting Department of the Ministry of Finance. According to the Public Finance Act, all expenditures should be made economically and substantively justified. The expenditures should be realised in accordance with the plan, which can be adapted if need be. The bodies that control the correctness of the expenditures are and Supreme Audit Office and the internal control unit of the Ministry of Finance. The Director of the Department of Financial Information, who approves the expenditure, confirms that the expenditure was necessary and was made in accordance with legal regulations, e.g. public procurement law.

541. The staff of the FIU, which composes of civil servants, is paid from the central budget of the Ministry of Finance. In the case of funds directly dedicated to the FIU, it is not accountable for its expenditures to any other department under the Ministry of Finance.

***Criterion 29.8 – (Met)***

542. The GIFI has been a member of the Egmont Group since June 2002.

***Weighting and Conclusion***

543. All criteria are met. **R.29 is rated Compliant.**

***Recommendation 30 – Responsibilities of law enforcement and investigative authorities***

544. Poland was rated PC on the previous Recommendation 27 due to a number of effectiveness issues which included: an over focus on fiscal ML cases, low number of ML investigations in major proceeds generating cases, insufficiently proactive approach in ML investigations and insufficient utilisation of FIU information by the law enforcement authorities.

***Criterion 30.1 – (Partly Met)***

545. There are no designated LEAs in Poland with specific responsibility to investigate ML and TF offences, except for the Central Anti-Corruption Bureau (CBA), which is entrusted expressly to identify, prevent, and detect ML in connection to corruption or activities detrimental to State's economic interest and the National Revenue Administration (KAS) which has investigative powers concerning tax and customs crimes and connected ML. Within the Police, the Economic Crimes Departments, established at

the central and regional levels, are mainly dealing with ML cases. The Internal Security Agency, the responsible authority for investigating the crimes against the State's security and its constitutional order, may carry out proceedings for investigating TF offences, if they fall under the category of crimes against the security of Poland and if ordered so by the prosecution or court (Art. 5 (1)(2)(a), Art. 21(2) of the Act of 2002 on ISA and ISA; Art. 311 of the CPC). There is no authority responsible for investigating TF offences that are not targeting the Polish state's security (or better said, the ISA lacks such formal competences).

546. In principle, criminal investigations are performed by the prosecutor, who can task the law enforcement authorities to carry out investigative steps. At the Prosecutor's Office, though not specifically provided for, the supervision of ML investigations is divided between the Department for Organised Crime and Corruption (in charge of matters related to prosecuting organised crime, most grievous corruption crimes and crimes of terrorist nature) and the Department for Economic Crimes (in charge of matters related to economic, financial and fiscal offences), organised at central and regional levels.

547. In addition, the Border Guards and Military Police can also be tasked by the prosecutor with investigative measures in ML investigations too.

***Criterion 30.2 - (Met)***

548. On the order of the prosecutor, the Police, the KAS, ISA and the CBA are authorised in general to conduct investigations into ML/TF connected to their competence, including parallel financial investigations. As a rule, ML cases are initiated either where ML/TF is uncovered during the investigation of the predicate crime or where SARs lead to the detection of the suspicion of a crime.

***Criterion 30.3 - (Met)***

549. There are designated competent authorities to expeditiously identify, trace, and initiate freezing and seizing of property that is, or may become subject to confiscation or is suspected of being proceeds of crime. The Polish FIU (GIFI) has an obligation to check the suspicions involving ML/TF on the basis of information provided by the obligated institutions, cooperating authorities and foreign FIUs, and connected to a suspicion it has the power to block accounts and suspend transactions at obliged entities for a maximum of 96 hours (Art. 86 (1) (5) of the AML/CFT Act). The GIFI reports each reasonable suspicion of ML/TF to the prosecutor. The prosecutor can also order suspension or blocking.

550. As a general rule, all law enforcement authorities have the power to temporarily seize and secure property subject to future forfeiture. The formal seizure has to be ordered by the prosecutor or judge.

551. In 2008, the Asset Recovery Office (ARO) was established at the Police Headquarter. The Police, the Internal Security Agency, the Central Anti-Corruption Bureau, the Border Guard, the Military Police, the Prosecutor's Office, and the KAS are authorised to exchange information via the ARO.

***Criterion 30.4 - N/A***

552. In Poland, only the prosecutor and the above-described authorities in their law enforcement capacity are entitled to conduct financial inquiries, therefore the recommendation is non-applicable.

***Criterion 30.5 - (Met)***

553. The Central Anticorruption Bureau, as a specialised anti-corruption authority, has

the competence to investigate connected ML/TF since April 2017, also having the task to conduct connected asset tracing and recovery. Its decisions on seizure of assets are temporary, and the final decision must be made by the prosecutor or judge.

#### *Weighting and Conclusion*

554. There are no designated LEAs with specific responsibility to investigate ML and TF offences, except for the CBA and KAS, which have express investigative powers regarding ML in connection to the predicate offences under their competences. It remains unclear which authority would be responsible for investigating TF offences that are not against the state's security, as this category falls out of the competences of the ISA. **R.30 is rated Largely Compliant.**

#### *Recommendation 31 - Powers of law enforcement and investigative authorities*

Poland was not reassessed during the 4<sup>th</sup> round on former Recommendation 28 as in the 3<sup>rd</sup> round the rating was Compliant. The amendments introduced in March 2017 in criminal law strengthened the police and provided for the legal basis of inquiries to uncover criminal assets.

##### ***Criterion 31.1 - (Met)***

555. (a) The Polish Code of Criminal Procedure (Art. 15 of the CPC) provides for a general obligation for extraneous entities (both natural and legal persons and entities without legal personality) to cooperate and assist the authorities conducting a criminal procedure. Records are seen as "objects" of evidence and subject to retaining. If the objects are not released voluntarily, their seizure may be enforced (Art. 217 of the CPC). Also, the GIFI provides information and data on request or ex officio to the judicial authorities as well as to the law enforcement authorities concerning their respective competence.

556. (b) The rules governing the search of persons and premises are provided under Chapter 25 of the CPC (Art. 219 - 228 of the CPC). The search is performed based on a warrant issued by a court or the public prosecutor. In urgent cases, the warrant may be obtained "without delay" after the measure and delivered at the request of the person in question within seven days (Art. 220 of the CPC).

557. (c) The powers to take witness statements are regulated by Art. 177 - 192 of the CPC. A person summoned as a witness is obliged to appear and testify. However, this obligation can be avoided in exceptional circumstances (e.g. defence counsel, clergyman and the mediator with regard to facts learned during the proceedings/ confession, any witness who was not released from the duty of confidentiality with regard to classified information, self-incriminatory information).

558. (d) Objects, including IT data, which may serve as evidence, or be subject to seizure (for securing the property) shall be surrendered if required so by the court or the public prosecutor and, in urgent cases, by the police or other competent authority (Art. 217, 218a of the CPC). The powers are also applicable in relation to objects found in the course of a search, which might constitute evidence of other offences, are subject to confiscation or whose possession is prohibited (Art. 228 of the CPC).

##### ***Criterion 31.2 - (Mostly Met)***

559. Special investigative measures and techniques are available to use for the law enforcement agencies based on the respective laws regulating their powers. The competent regional court decides on the application of a special technique at the request of the Chief of competent LEA, approved by the Prosecutor General. In urgent cases, the

techniques can be applied after obtaining the written consent of the prosecutor.

560. (a) Undercover operations may be performed within the operational activities according to sectoral laws (e.g. Art. 19 and 19a of the Act on the Police), operational control and operational intelligence, operational control (Art. 19 and 20 of the Act on Central Anti-corruption Bureau), operational-intelligence control, controlled acquisition (Art. 27, 29 of the Internal Security Agency and Intelligence Agency Act), operational control (Art. 9f) of the Border Guard Act), operational and detective acts (Art. 118 and 119 of the Act on National Revenue Administration). In particular, some special operations such as controlled sale, takeover of objects, controlled takeover, awarding financial benefits entail direct involvement of covert agents and their interactions with members of an organised criminal group. However, the Polish legal system does not provide for the infiltration of covert agents into an organised criminal group.

561. (b, c) Intercepting communications and accessing computer systems are special operations that fall within the broader concepts of operation control, operational intelligence and intelligence control, regulated by the acts indicated under sub-criterion (a).

562. (d) Criminal police activities include secret surveillance of the manufacture, transport, storage and turnover of crime objects (Art. 19b of the Act on the Police). Controlled delivery may also be performed by ISA (Art. 30 of the Internal Security Agency and Intelligence Agency Act), by the CBA (Art. 19 of the Act on CBA), Border Guard (Art. 9f of the Border Guard Act) and by the KAS (Art. 120 of the Act on KAS).

### ***Criterion 31.3 – (Met)***

563. (a) Intelligence agencies are authorised to have access to banking information and other financial transactions (accounts, stock market, insurance, payment services, etc.). The tax authority (precisely: the Head of KAS) has access to financial information. The GIFI can request information directly from the service providers.

564. A form of central bank account register is run by the National Clearing House (NCH), where within a maximum of three days from the date of receipt of the request, the service providers are obliged to register their bank accounts free of charge. The NCH is obliged to cooperate with the law enforcement agencies and the prosecutor in a criminal investigation. The Police can have access to banking data based on a court decision. The CBA has access to the bank account register of the NCH at the request of the head of the CBA, without an obligation to obtain the approval of the court. Upon written demand of the Head of KAS or the head of a customs and tax control office, the banks and investment fund societies are obliged to provide information approximately in the same scope. Moreover, since 2018, the KAS has collected financial transaction information in an automated method from the Clearing House and may disseminate ML/TF-related data to GIFI and investigating authorities.

565. (b) Identification of assets in connection to ML/TF is done in the course of investigation. If the activities take the form of a prosecutor's order, they are notified to the parties of investigation after their completion. Other parties, including owners of the assets, are not informed of any investigative actions. Any disclosure without permission is sanctioned under Art. 241(1) of the CC.

566. In the procedures of the CBA, the court decides about the permission to identify banking data, and after 120 days, the person or entity has to be informed about the inquiry, except where this would be detrimental to the operational activity, in this case, the court may waive the obligation to notify. The Police has a wide range of potential sources to identify assets with no notification obligation about its inquiries.

### ***Criterion 31.4 – (Met)***

567. The GIFI – on a written and justified request – shall make available the information available to every authority investigating ML/TF or predicate offences.

#### ***Weighting and Conclusion***

568. The Polish law enforcement and investigative authorities possess the powers necessary to investigate ML/TF and connected predicate offences. A minor shortcoming remains in relation to the undercover agents. **R. 31 is rated Largely Compliant.**

### ***Recommendation 32 – Cash Couriers***

569. During the process of the 4th round evaluation report, the rating for FATF Special Recommendation IX equivalent to R.32 had not been considered. Therefore, the report includes the rating from the 3rd round evaluation when Poland had been rated 'LC' for Special Recommendation IX. The evaluation team had recommended the Polish authorities to perform more targeted co-operative enquiries and to demonstrate more sensitisation to terrorist financing issues.

### ***Criterion 32.1 – (Mostly met)***

570. Poland applies EU legislation (Regulation (EC) No 1889/2005 of the European Parliament and the Council of 26 October 2005 on controls of cash entering or leaving the Community, which obliges natural persons leaving or entering the EU to declare cash (including BNIs) of a value of €10 000 or more. Since June 2021, the new Regulation (EU) No 2018/1672 is applied. The new Regulation maintains the €10 000 threshold. The national legislation (Art. 18 of the Act of 27 July 2002 – Foreign Exchange Law, § 3 of the Regulation of the Minister of Finance of 20 April 2009 on general foreign exchange) sets rules for travellers (incoming and outgoing) crossing the border between Poland and non-EU Member States. to submit a cash declaration if the value of the foreign exchange values or national means of payment exceeds the total of the equivalent of €10 000. There is no mechanism to declare or disclose incoming and outgoing cross-border transportation of cash and BNI within the EU.

571. As to the cash transportation in post and freight, there is a general prohibition (Annex 2 to Decision No.1/2014/CZI of the Member of the Management Board of Poczta Polska S.A. of 2 January 2014, Annex No. 2 to Resolution No. 48/2018 of the Management Board of Poczta Polska S.A. of 20 March 2018) to use postal services (mail, parcel, shipments) for valuable items (including coins, banknotes) without a declared value. Regarding postal services in foreign trade, it is forbidden (by the same acts) to include in the mail valuable items (coins, banknotes, currency or any bearer's payable assets, travellers' checks, platinum, gold or silver, processed or not, precious stones, jewellery) without declaration of the value. Additionally, when sending a parcel with a declared value, it is mandatory to provide data on the sender and the recipient.

### ***Criterion 32.2 – (Met)***

572. Poland selected option b) of R.32.2 whereby residents and non-residents crossing the state border of Poland and of the EU are obliged to report to customs and tax authorities or Border Guard authorities imports to the country and export abroad of foreign exchange gold or foreign exchange platinum, regardless of the amount, as well as domestic or foreign means of payment, if their total value exceeds the equivalent of €10 000. The obligation to report is considered not fulfilled if the providing data is false.

***Criterion 32.3 – (N/A)***

573. Poland doesn't apply a disclosure system.

***Criterion 32.4 – (Met)***

574. The Polish authorities (Customs and Tax Control Service and the Border Guard performing customs clearance) are empowered to request and obtain further information from the travellers with regard to the origin of the cash and their intended use according to Art. 20 section 2 of the Act of 27 July 2002 - Foreign Exchange Law. That includes but is not limited to the possibilities to receive, check and certify cash declarations; to check whether the obligation to submit a declaration has been fulfilled; to carry out checks on natural persons, their luggage and means of transport; to perform cash retention; to apply sanctions in the event of failure to comply with the obligation to submit a cash declaration.

***Criterion 32.5 – (Met)***

575. In accordance with Article 106f and 106h of Act of 10 September 1999 – the Penal Fiscal Code fines for a fiscal offence are imposed on persons who, contrary to their obligation, do not report to Customs and Tax Control Service or Border Guard authorities on importation into or export of foreign currency or domestic means of payment or provide false information in the declaration and do not present to the competent authorities, on their demand, the transported cash. Pursuant to Article 48 § 1 of the Penal Code, a fine for a fiscal offence is bound to “the minimum salary”. At the moment, the sanction amounts from PLN 260 to PLN 52 000 (approx. €54 to €11 400) and the team considers them proportionate and dissuasive.

***Criterion 32.6 – (Met)***

576. The requirement is met by the established system of providing GIFI (the Polish FIU) on a regular basis (once a month) with information obtained through the declaration process by an electronic document sent via the Head of KAS or the Chief Commander of the Border Guard, which corresponds to the system described under criterion 32.6 (b) (Regulation of the Minister of Finance of 11 January 2019 concerning information on imported or exported monies, national currency and foreign exchange values). Notifications of that kind are sent through a website or interface software enabling such communication, the information being encrypted and marked by a qualifying electronic signature or electronic seal. Additionally, pursuant to Art. 83 of the AML/CFT Act, there is an obligation to immediately notify the GIFI (in hard copy or via electronic communication means) in case of suspicion of committing a crime of ML or TF.

***Criterion 32.7 – (Met)***

577. The coordination between Customs and Tax Control Service, immigration authorities and other related authorities on matters related to the implementation of Recommendation 32 appears to be adequate. The Customs and Tax Service closely cooperates with other border services, mainly with the Border Guard, with which co-operation plans with the KAS and Border Guard are signed annually. Likewise, KAS and Border Guard have common communication channels (website and two mobile applications). The Polish authorities presented examples of systematic co-operation as well between the immigration authority (the Office for Foreigners) and KAS and Border Guard.

***Criterion 32.8 – (Partly met)***

578. The current legal framework entitles the Customs and Border Guard or other authorities to stop and restrain currency and BNIs, but is limited to cases where there is knowledge about the commission of an offence. Pursuant to Art. 304 § 2 of the CCP, when

in connection with their activities, the competent authorities learn about the commission of an offence, they shall immediately notify the prosecutor or the police and take the necessary steps to prevent the loss of traces and evidence. Art. 217 of the CCP (under Chapter 25 – Seizure. Search) invoked by the Polish authorities also indicates only the ability to seize “objects” which may serve as evidence. But this does not provide for seizing them solely for the purpose of ascertaining whether there is evidence of ML or TF.

579. In case of non or false declaration, the Polish legislation does not provide for an administrative procedure for seizing the cash based on an administrative decision, pursuant to the Art. 4(4) of the Regulation (EC) 1889/2005. However, under Art. 217 of the CPC, part of the funds may be retained for securing the fine envisaged for non or false declaration until the final court decision in the proceedings. Nevertheless, according to the explanations provided by the Polish authorities, this would be the case when the traveller is a foreigner. In the case of Polish citizens, depending on the circumstances, the security for the fine is often waived. Thus, the requirement under criterion 32.8(b) is not met.

#### ***Criterion 32.9 – (Met)***

580. The general requirement for exchange of information among EU countries and with third countries is regulated by the Convention on mutual assistance and co-operation between customs administrations (Naples II) or, where applicable, Regulation (EC) No. 515/97 of 13 March 1997. Polish Customs, Tax Control Service do exchange (upon request or spontaneously) cash control information about presented cash declarations and any other information referred to R32 for international information exchange. The FIUs does provide information on filed cash declarations and any other information connected with the implementation of R32 in the course of international information exchange, in line with provisions 110-116 of the Polish AML/CFT Act. There is an IT system (ESKS Currency module) where all related documentation (covering all three categories under C.32.9) is stored indefinitely.

#### ***Criterion 32.10 – (Met)***

581. Requirements are in place to the relevant officers concerning confidentiality of all information obtained in connection with cash controls (Art. 47.3 Act on the National Revenue Administration of 16 November 2016). The information exchange is made through IT systems (CRMS, RIF, FIDE, AFIS) which includes special security measures to protect against unauthorised access.

#### ***Criterion 32.11 – (Met)***

582. Persons involved in cross-border transportation related to ML/TF or predicate offences are subject to the sanction provided under the ML offence, which is deprivation of liberty for a term of between six months and eight years (Art. 299 § 1 PC). The general rules on seizure and confiscation described under R.4 apply.

### ***Weighting and Conclusion***

583. Similarly, to other EU Member States, Poland does not have an EU-internal border declaration system for cash or BNIs. The power to stop and restrain cash appears to be limited: only when there is knowledge of the commission of an offence and only for securing the fine in case of non/ false declaration (mainly when the traveller is a non-citizen). **R.32 is rated Partially Compliant.**

### ***Recommendation 33 – Statistics***

584. 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 LEAs 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.

***Criterion 33.1 – (Partly Met)***

585. a) Art.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. Nevertheless, the SARs are not broken down on ML and TF suspicions.

586. b) Department for Organised Crime and Corruption of The Public Prosecutor's Office, 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 money laundering and terrorist financing. 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.

587. c) As per Art. 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 money laundering and terrorist financing is collected by the Department for Organised Crime and Corruption of The Public Prosecutor's Office. In fact, the statistics are kept on property frozen, seized and confiscated only on ML and TF cases, not in all proceeds generating cases. The statistics do not contain information on property actually recovered.

588. d) The Bureau of International Co-operation of the Public Prosecutor's Office and the Ministry of Justice are responsible for collecting the data on mutual legal assistance or other international requests for co-operation made and received in relation to non-EU countries. 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 SIENA channel on international organised crime in categories covered by EUROPOL's mandate, including money laundering. The authorities do not keep comprehensive statistics on MLA, both out-going and in-coming requests for all crimes and with a breakdown by jurisdiction. There are no statistics on pending, executed and refused requests, including average time of completing the requests.

***Weighting and Conclusion***

589. There are moderate shortcomings in relation to the statistics on property frozen, seized and confiscated which are available only for ML ad TF and not for all proceeds generating crimes. There is no information on recovered property. The statistics on SARs are not broken down on ML and TF suspicions. There are no comprehensive statistics on MLA, both out-going and in-coming requests for all crimes and with a breakdown by jurisdiction. There are no statistics on pending, executed and refused requests, including average time of completing the requests. **R. 33 is rated Partially Compliant.**

### **Recommendation 34 – Guidance and feedback**

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

#### **Criterion 34.1 – (Partly met)**

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

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

593. The relevant AML/CFT legal acts and the guidelines issued for the obligated institutions are supposed to be published, and the AT was provided with a list of “communications” out of which most are very technical short instructions pertaining to the way the REs are expected to fill out the threshold reports or information notes (i.a. on naming files containing the information on above threshold transactions; on adaptation of ITC systems of the obligated institutions in terms of reporting, launching of projects of harmonisation etc.). Another typology of such “communications” are GIFI's reaction to recurrent issues posed by the private sector.

594. Nevertheless, some of the “communications” do contain references to customer verifications, CDD and SAR reporting or specific situations (e.g. COVID related restrictions), although those do not amount to the requirements of the criterion “to assist financial institutions and DNFBPs in applying national AML/CFT measures, and in particular, in detecting and reporting suspicious transactions”. An AML/CFT Handbook was introduced to the AT, but the document was issued in 2009, and the assessors treat the relevance of the indicators contained therein with caution.

595. Guidance has been issued by other supervisors such as UKNF's “Position of the KNF on risk assessment of obliged institutions”, the “Statement on customer identification and customer identity verification at banks and branches of credit institutions through video ID verification” and “Recommendation H concerning the internal control system at banks” as well as NBP “Guidelines for assessing the risk of money laundering and terrorist financing resulting from the obligation the AML/CFT Act”.

596. The GIFI prepared an online on training Anti-money laundering and countering the financing of terrorism to familiarise obligated institutions, cooperating entities and other entities with the subject of anti-money laundering and anti-terrorist financing within the scope of existing regulations. The trainings available on the GIFI website.

#### **Weighting and Conclusion**

597. Moderate deficiencies remain in relation to the provision of Guidelines to assist financial institutions and DNFBPs in applying the AML/CFT measures, especially in the SAR area, as the documents provided do not include ST reporting guidance or in case of the AML/CFT Handbook, the information contained therein seems to be outdated. **R34 is rated Partially Compliant.**

### ***Recommendation 35 – Sanctions***

598. In the 4th previous MER, Poland was rated LC with R.17. There were no sanctions that could be imposed on directors and senior management. The FATF standards have been revised since then, and a new analysis has been undertaken.

599. FIs and DNFBPs - under Articles 147 and 148 of the AML/CFT Act, any FI or DNFBP that fails to comply with certain AML/CFT obligations in the AML/CFT Law is subject to administrative penalties under Article 150. In addition, Article 154 permits the imposition of a financial penalty for a breach of Articles 6 to 8. (See under c 27.4 and 28.4.)

#### ***Criterion 35.1 – (Partly met)***

600. As indicated in c.27.4 and 28.4, there are some gaps in the proportionality and dissuasiveness of the sanctions. In addition, Articles 147 and 148 do not cover many of the requirements set out in the AML/CFT Law, including some relevant to compliance with the FATF Recommendations, *e.g.* Art. 34(2), Art. 35, Art. 37, Art. 39 to 41, Art. 47 and Art. 90(2).

601. Reporting of suspicion and tipping off - under Article 147(13) of the AML/CFT Act, the administrative penalties at Article 150 apply to failure to comply with the reporting obligations at Articles 74 and 86 and under Article 147(11) the administrative penalties at Article 150 apply to the confidentiality requirement (i.e. the tipping-off prohibition) at Article 54. The authorities have not explained whether criminal sanctions can also be applied to a FI or DNFBP for failing to report. The AT has a concern that, in the absence of criminal penalties, the sanctions in relation to reporting are not fully dissuasive.

602. TFS (Recommendation 6) – under Article 149 of the AML/CFT Act, any FI or DNFBP that fails to comply with measures to implement TFS related to terrorism and terrorist financing under Article 117 of the AML/CFT Law or under EU Regulations 881/2002 and 2580/2001 is liable to an administrative penalty under Article 150. The AT has a concern that, in the absence of criminal penalties, the sanctions in relation to TFS are not fully dissuasive.

603. NPOs become obligated institutions when they accept cash with a total value of more than €10 000, regardless of whether the payment is performed as a single operation or as several operations which seem linked to each other. At that stage, they become subject to the administrative sanctions framework for obligated institutions in the AML/CFT Act.

#### ***Criterion 35.2 – (Partly met)***

604. Under Article 154 of the AML/CFT Act, financial penalties for AML/CFT breaches of up to PLN 1 million (€220 000) may be imposed on senior members of management, board members and employees with responsibility for implementing AML/CFT obligations covered by Articles 147 and 148 (see c.35.1 for the implications of this) if they were responsible for the breach or breaches. This does not constitute a proportionate and dissuasive sanctions framework. In any case, the pecuniary penalties only apply to breaches of obligations referred to in Articles 147 and 148 and do not apply to failure to comply with measures to implement TFS related to terrorism and terrorist financing, which, as explained above, are dealt with under Article 149. Therefore, no penalties apply to individuals for breach of TFS measures.

605. Under Article 156 of the AML/CFT Act, there are also criminal penalties applicable to individuals for breach of the reporting and tipping off obligations in the AML/CFT Act. Any person who fails to report suspicion to the GIFI, or who provides the GIFI with false information, conceals information from the GIFI or who discloses information to an

unauthorised person is subject to a term of imprisonment of between three months and five years (or to a fine where this is unintentional).

606. Two of the administrative penalties in Article 150 of the AML/CFT Act are applicable to individuals. However, under Article 151(1), the UKNF is the only authority that may prohibit a person from holding a managerial position for up to one year. The maximum level of fine which can be imposed in relation to an individual is PLN 20 868 500 (€4 591 070). GIFI is able to publish sanctions on individuals under Article 152 of the AML/CFT Act. The absence of a wider power to prohibit individuals and the relatively short maximum period for which individuals can be prohibited by the UKNF means that the overall range of administrative sanctions is partly proportionate and dissuasive; it is also not clear how the financial penalties in Article 150 tie in with the financial penalties in Article 154.

### ***Weighting and Conclusion***

607. As indicated in c.27.4 and 28.4, there are some gaps in the proportionality and dissuasiveness of sanctions applicable to FIs and DNFBPs. It is also noted that sanctions cannot be applied in all cases where there is a failure to comply with a requirement of the AML/CFT Act. In the absence of criminal sanctions for failing to report or comply with TFS, sanctions on FIs and DNFBPs are not fully dissuasive. Similarly, sanctions applicable to senior members of management, board members and employees with responsibility for implementing AML/CFT obligations are not proportionate or dissuasive. The absence of a wider power to prohibit individuals and the relatively short maximum period for which individuals can be prohibited by the UKNF means that the overall range of administrative sanctions is partly proportionate and dissuasive. **R.35 is rated Partially Compliant.**

### ***Recommendation 36 – International instruments***

608. Recommendation 36 covers the scope of the previous Recommendation 35 (at the time of Poland's 4<sup>th</sup> round evaluation) and was rated PC due to deficiencies connected to R3 (missing physical element of ML crime, discretionary confiscation, gaps in the confiscation regime) and R5 (gaps in criminalisation of terrorist financing).

#### ***Criterion 36.1 – (Met)***

609. Poland has signed and ratified the relevant UN conventions (Vienna Convention (1989 and 1994 respectively), Palermo Convention (2000 and 2001), Merida Convention (2003 and 2006), and the International Convention for the Suppression of the Financing of Terrorism (2001 and 2003), with no reservations.

610. In addition to the above-mentioned treaties, Poland is also a party to the Council of Europe Convention on Cybercrime (ratified in 2015 with reservations) and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceeds of Crime and on the Financing of Terrorism (ratified in 2007 with declarations) as well.

#### ***Criterion 36.2 – (Mostly Met)***

611. Poland has largely implemented into domestic legislation the provisions of the Vienna, Palermo, Merida, and TF Conventions. The level of compliance with the provisions of the Conventions, i.e. art. 6 and 10 of the Palermo Convention, Art. 3 of the Vienna Convention and art. 26 of the Merida Convention is impacted by the shortcomings described under Recommendation 3 and 4 (some shortcomings remained concerning: the requirement of a potential result, i.e. a danger to the determination of criminal origin resulting from the perpetrator's action, the physical element of transporting abroad, the concerns regarding directly obtained proceeds as property covered by ML offence, the

limited scope of the liability of legal persons and the limitation of the property subject to confiscation, i.e. *items*, compared to the requirement of the conventions, which refers to *any property*, including intangible assets). The level of implementation of the TF Convention is subject to the deficiencies identified under Recommendation 5 concerning compliance with Art. 2 of the Convention.

612. An important feature of the Polish legal system is that by virtue of the Constitution (Art. 87) ratified conventions have a binding legal effect, except if they require implementation. In the absence of the relevant information provided by the Polish authorities, it is not clear how certain non-self-executing provisions of the conventions, which require appropriate measures taken by the state party, are implemented (particularly, Art. 15 of the Vienna Convention and Art. 53 of the Merida Convention).

### ***Weighting and Conclusion***

613. Poland is party to all the relevant international conventions and has largely implemented the relevant articles of those conventions. The deficiencies indicated under R. 3, 4 and 5 apply. Certain non-self-executing provisions of the conventions (Art. 15 of the Vienna Convention and Art. 53 of the Merida Convention) do not appear to be implemented. **R. 36 is rated Largely Compliant.**

### ***Recommendation 37 - Mutual legal assistance***

614. During the 4th round evaluation, Poland has been rated as Compliant to R. 36 Mutual legal assistance and Largely Compliant for FATF Special Recommendation V together equivalent to R. 37. The evaluation team had found that the potential refusal due to lack of full dual criminality with regard to TF could be used as the basis for denying mutual legal assistance.

#### ***Criterion 37.1 – (Met)***

615. The 4<sup>th</sup> evaluation report has established that Poland can provide a wide range of mutual legal assistance and co-operation in relation to ML, associated predicate offences and TF offence. Since no changes occurred in the Polish legislation since the present AT upholds this conclusion. Poland provides legal assistance on the basis of the multilateral agreements within the capacity of the Council of Europe, i.e. the European Convention on Mutual Assistance in Criminal Matters of 20.04.1959 and the European Convention on Extradition of 13.12.1957, as well as EU conventions and bilateral agreements.

#### ***Criterion 37.2 – (Partly met)***

616. The national legal framework does not provide for a central authority for the transmission and execution of the MLA requests, the designation being made for each international instrument to which the country is party to, via notifications. As a general rule, the Department of International Co-operation and Human Rights at the Ministry of Justice executes the responsibilities of the central authority in Poland regarding the UN Conventions. When the requests relate to cases being at the stage of the court's trial, they are forwarded to the competent courts. When they concern investigative activities, the MoJ hands the MLA request over to the Bureau for International Co-operation at the Public Prosecutor's Office. In the absence of bilateral or multilateral agreements, requests are dispatched through diplomatic channels. However, the MLA requests may be dispatched directly by the judicial authorities and returned in the same way (except for requests for hearing witnesses or experts by videoconference or telephone conference, which have to be submitted via the MoJ). Such decentralized co-operation is, predominantly, within the framework of the EU co-operation or concerning urgent matters.

617. There is no clear process for the timely prioritisation and execution of MLA requests. The standard execution applies to all incoming requests. Nonetheless, according to the explanation provided by the Polish authorities, certain factors (such as objective jeopardy of losing the relevant evidence, large amount of laundered property, etc.) may impact the prioritisation of such requests.

618. The information provided does not indicate that a sound case management system is in place to monitor progress on requests. Nevertheless, based on the Order of the MoJ of 3 March 2016, on the organisation of secretariats and other administration departments in common organisational units of the prosecutor's office, all incoming MLA requests are registered.

***Criterion 37.3 - (Met)***

619. The situation remains unchanged since the previous round evaluation report. Under Polish legislation, neither restrictive nor unreasonable conditions exist with regard to mutual legal assistance.

***Criterion 37.4 - (Met)***

620. The criterion has been a subject of consideration in the 4th MER, and the conclusion should remain the same. The provisions of CCP (art. 588 and 589zj) do not provide such restrictions both for MLA and EIO.

***Criterion 37.5 - (Met)***

621. The same confidentiality requirements apply as in the case of domestic investigations. The criterion is met.

***Criterion 37.6 - (Partly met)***

622. Even though dual criminality is not a condition *per se*, it is among the reasons for denial of assistance. (Art. 588 § 3 of PCC). Thus, the legal framework does not ensure that in all cases where the request does not involve coercive actions, dual criminality will not be a condition for rendering the assistance.

***Criterion 37.7 - (Met)***

623. Article 588 § 3 of PCC provides that the assistance may be denied if there is a lack of reciprocity or dual criminality. The condition of double criminality is met if at least some of the features of the criminal conduct are the same as the equivalent in the Polish substantive criminal law. The condition of double criminality is met even when there is no crime of the same type in Polish law as in the law of the requestion country, but the act described in the request corresponds to one of the crimes provided in Polish law.<sup>89</sup>

***Criterion 37.8 - (Met)***

624. In general, all powers and investigative techniques required under R31 are available for the foreign counterparts requesting mutual legal assistance. It should be noted that the investigative actions requested by a foreign court or public prosecutor are governed by Polish law pursuant to Article 588 CCP. The request of the above authorities to apply a particular mode or form to the procedure should be honoured if this is not contrary to the legal order of the Republic of Poland.

***Weighting and Conclusion***

---

<sup>89</sup> Ruling of the Supreme Court of Poland of 16 October 2014 (reference number of the case: II KK 264/14).

625. There is no clear process for the timely prioritisation and execution of MLA requests and no indication of a sound case management system. The current legal framework does not ensure that dual criminality will not be a condition for rendering assistance in cases that do not involve coercive actions. **R. 37 is rated Largely Compliant.**

### ***Recommendation 38 – Mutual legal assistance: freezing and confiscation***

626. In the 3rd round MER<sup>90</sup>, Poland was rated largely compliant on R.38. The 4th round MER did not reassess Poland's compliance with R.38 and kept the same rating. The 3rd round evaluation team had considered the legislation as complying with the international Convention obligations and separate procedures within the European Union recognition of foreign freezing orders. However, it had been noted a reserve on effectiveness in relation to freezing, seizing, and confiscation (property and value) due to the absence of statistical data. The legislation (Code of Criminal Procedure) still provides the necessary basis for mutual legal assistance in the scope of R.38.

#### ***Criterion 38.1 – (Mostly met)***

627. The requirement of the criterion is met in respect of requests both from EU Member States or non-EU foreign countries in order to identify, freeze, seize, or confiscate property listed under sections a-e by the provisions of CCP (art. 585, 588 on mutual legal assistance and Chapter 62b to render MLA). Nevertheless, the limitation of the confiscation powers with regard to intangible property (described under R. 4) has an impact on the ability to provide assistance with respect to “any property”, as required by the standard.

#### ***Criterion 38.2 – (Met)***

628. Under Art. 45a § 1 and 2 of the CC, the assistance to request made on the basis of non-conviction based confiscation may be provided in cases when the i) harmfulness of the prohibited act to the public is negligible; ii) in the event of conditional discontinuation of the proceedings (lack of mental capacity, other circumstances excluding the punishment of the perpetrator); iii) perpetrator's death, absence due to mental illness or other serious illness; iv) non-detection or flight of the perpetrator.

#### ***Criterion 38.3 – (Mostly met)***

629. Poland authorities conduct coordination with other countries by means of formal and informal channels of co-operation. They are able to use Eurojust and other networks as Camden Asset Recovery Interagency Network (CARIN) and liaison police officers. The mechanism for managing and disposing of (when necessary) property seized has been provided by the CCP. There is no single and detailed mechanism for managing/ disposing of seized or confiscated property and no centralized authority in charge of management of such property.

#### ***Criterion 38.4 – (Met)***

630. There is an adequate mechanism of sharing confiscated property provided by CCP (Article 611fu and 611zb).

### ***Weighting and Conclusion***

---

<sup>90</sup> <https://rm.coe.int/european-committee-crime-problems-cdpc-committee-of-experts-on-the-eva/16807164e5>

631. Polish law provides a good basis for the timely and adequate rendering of assistance in the scope of international legal assistance addressing identifying, freezing, seizing, or confiscating property of criminal origin. Nevertheless, the shortcomings identified in R.4 hinder Poland's ability to provide such assistance. Namely, there is no single and detailed mechanism for managing/ disposing of seized or confiscated property, and the limitation of the confiscation powers with regard to intangible property (R. 4) which applies and impacts the ability to provide assistance with respect to "any property". **R.38 is rated Largely Compliant.**

### ***Recommendation 39 – Extradition***

632. In the 3rd round MER<sup>91</sup>, Poland was rated largely compliant on R.39. The 4th round MER did not reassess Poland's compliance with R.39 and kept the same rating. The 3rd round evaluation team had expressed doubt if the extradition requests were handled without undue delay because of the absence of statistics which did not allow determining the effectiveness in relation to extradition. Regarding the current evaluation process, it should be noted a new Ordinance of the Minister of Justice of 7 April 2016 which provides regulations for (but not only) the process of prosecutor's actions aimed at execution of the extradition request.

#### ***Criterion 39.1 – (Mostly met)***

633. Polish authorities are able to perform duties on extradition requests in relation to ML/TF without undue delay as being a party to the European Convention on Extradition and the UN International Conventions that adopt extradition as an instrument of international co-operation in criminal matters. In addition, the Polish CCP provides the full scope of powers that are necessary to the practitioners. ML and TF are both extraditable offences. No unreasonable or unduly restrictive conditions on the execution of requests exist within the Polish legislation. Nevertheless, as described under R. 37.2, there is no indication of a sound case management system in place for timely execution of extradition requests or clear process for their prioritisation.

#### ***Criterion 39.2 – (Met)***

634. Polish legislation (Article 604 para. 1 item 1 CCP) does not allow extradition of its own citizens, but since the Polish criminal law applies to any Polish citizen who has committed a crime abroad, the competent authorities are obliged to act for the purpose of prosecution of the offences set forth in the request. In this way, the requirement is met.

#### ***Criterion 39.3 – (Met)***

635. Article 604 § 1 of PCC provides that the extradition is inadmissible if the act does not contain the characteristics of a prohibited act or when the law recognises that the act does not constitute a crime. The condition of double criminality is met even when there is no crime of the same type in Polish law as in the law of the requestion country, but the act described in the request corresponds to one of the crimes provided in Polish law.<sup>92</sup>

#### ***Criterion 39.4 – (Met)***

636. In cases that fall out of the provisions of international agreements to which Poland is a party, its authorities may apply the simplified extradition mechanism which has been provided under article 603a § 2 CCP.

---

<sup>91</sup> <https://rm.coe.int/european-committee-crime-problems-cdpc-committee-of-experts-on-the-eva/16807164e5>

<sup>92</sup> Ruling of the Supreme Court of Poland of 16 October 2014 (reference number of the case: II KK 264/14).

### ***Weighting and Conclusion***

637. The Polish authorities have the necessary tools to meet the needs for international co-operation in the field of extradition proceedings, as well as to respond with appropriate prosecution when it comes to a Polish citizen. Nevertheless, the lack of a clear process for prioritisation and timely execution of the extradition requests and a sound case management system impacts the compliance with the recommendation. **R.39 is rated Largely Compliant.**

### ***Recommendation 40 – Other forms of international co-operation***

638. In the 4<sup>th</sup> round evaluation report, Poland had been rated as ‘LC’ for R.40 and SR.V, based on effectiveness issues regarding law enforcement authorities. The evaluation team recommended the Polish authorities to set out in place procedures to centrally record and monitor all international co-operation requests on matters related to ML and TF. The recommendation was not implemented.

#### ***Criterion 40.1 – (Mostly met)***

639. Competent authorities of Poland can provide both, upon request and spontaneously, a wide range of international co-operation in relation to ML, TF and predicate offences: GIFI (Art. 110-116 of the AML/CFT Act); law enforcement authorities (Police, including ARO, Internal Security Agency, Central Anticorruption Bureau, National Revenue Administration and Border Guard, Military Police and State Protection Service) (Art. 1, 4 of the Act on exchange of information with the law enforcement authorities of the Member State of the EU, third countries, EU agencies and international organisations of 2011); Additionally, special legislation regulating the activity of KAS (Art. 2(20) of the Act on National Revenue Administration), CBA (Art. 2(2) and (2a) of the Act on CBA of 2006) and ISA (Art. 8 of the Internal Security Agency and Intelligence Agency Act of 2002) provides for the legal basis for international co-operation. The mentioned authorities appear to be able to provide the co-operation in a rapid manner, except for the limitation described under c.40.2(d).

640. The NBP and UKNF do not have a legal basis for cooperating with foreign counterparts in relation to ML, TF and predicate offences (only regarding prudential matters) and mainly rely on the powers of GIFI as the main supervisory body for all reporting entities (see c.40.12).

#### ***Criterion 40.2 – (Mostly met)***

641. (a) The legal basis for co-operation of the competent authorities is described under c. 40.1 above.

642. (b) The GIFI and the LEAs, acting pursuant to the 2011 Act indicated under c. 40.1, are able to cooperate directly with the foreign counterparts and no particular impediments exist with regard to the means available for cooperating in the most efficient way. The CBA and ISA are cooperating mainly on the basis of bilateral agreements with the foreign counterparts, and any co-operation outside such framework would still require an authorisation by the Prime Minister, which does not ensure the use of the most efficient means to cooperate.

643. (c) The authorities use clear and secure gateways, such as the Egmont Secure Web, FIUNET, Interpol, Europol and SIRENE channels, EMPACT, certified channels and liaison officers for exchange of classified correspondence.

644. (d) The time limit provided for the execution of the requests received by GIFI (up

to 30 days – Art. 111(6) of the AML/CFT Act) and by the law enforcement authorities (within 14 days – Art. 15 of the Act on exchange of information with the law enforcement authorities of the Member State of the EU, third countries, EU agencies and international organisations of 2011), provides for a mechanism for the prioritisation and timely execution of the requests. When the request is made by a foreign counterpart of the law enforcement authority from an EU Member State, the reply shall be provided even more rapidly – within seven days or eight hours in urgent matters. When the co-operation is provided based on bilateral agreements, the time limit established in the agreements will apply. However, the legal requirement for a formal prior consent of the Prime Minister in the case of CBA and ISA may impact the ability of the mentioned authorities to ensure timely execution of the request in the absence of a pre-existing international agreement, especially in urgent matters. In relation to such requests, there is no clear process for their timely execution. The Acts on the CBA and ISA do not specify the term within which the response of the Prime Minister should be awaited. The general time limit provided by the Code on Administrative Procedure was invoked as applicable – up to 30 days, but there is no written procedure confirming this term or that such requests would be prioritized for their timely execution. However, the considerable number of counterparts with whom both the CBA and ISA cooperate would suggest that such instances would not occur frequently.

645. (e) The GIFI and the LEAs have in place mechanisms for safeguarding the received information (Chapter 9 of the AML/CFT Act; Art. 7.3 of the Regulation of the Council of Ministers of 2020 on how to exchange the information between a contact point and authorised entities and law enforcement authorities of the MS of the EU, third countries, EU agencies and international organisations).

***Criterion 40.3 – (Met)***

646. The new AML/CFT Act has changed the situation in a positive way compared to the 4th MER as the activity of GIFI does not require bilateral or multilateral agreements or arrangements to cooperate in exchanging information. Police, KAS and Border Guard Service also appear to be able to provide co-operation outside the framework of an international agreement. The CBA and ISA cooperate mainly based on bilateral agreements with a wide range of foreign counterparts, which obtained a prior authorisation of the Prime minister, but are also able to cooperate outside such framework, subject to Prime minister's consent. The UKNF and NBP rely on bilateral/multilateral agreements for providing assistance in relation to prudential supervision matters, a considerable part being exchanged pursuant to IOSCO and ESMA MoUs (in the case of the UKNF).

***Criterion 40.4 – (Met)***

647. According to the Polish authorities, the feedback requests are treated as any other request for information. Therefore, in terms of timelines, the analysis under 40.2 applies. Competent authorities shall inform the foreign counterpart if it is not possible to reply within the time limits set out in the law.

***Criterion 40.5 – (Mostly met)***

648. There are various circumstances in which a request for assistance may be refused, but those do not relate to fiscal matters or secrecy or confidentiality, which must be maintained by financial institutions or DNFBPs. The Act on 16 September 2011 (Art. 11) on the exchange of information with law enforcement authorities of the Member States of the European Union, third countries, European Union agencies and international organisations set out the grounds for refusal, and those in R 40.5 (a; c) are not among

them. The nature or status of the requesting counterpart authority is not relevant for international co-operation. LEAs are able to refuse requests related to tax or any other crime which does not fulfil the penalty “threshold” (punishable by imprisonment for more than a year), but this refers only to requests coming from other Member States (Art.13(2) and Art. 18f of the 2011 Act) and, therefore, not considered material to the assessment of this criterion.

649. The GIFI’s powers to exchange information are restricted by the limitation regarding the classified information (see c.4.11). Articles 110-116 of the AML/CFT Act establish a wide range of international co-operation possibilities for the FIU, regardless of whether foreign FIUs are administrative, LE or judicial FIUs.

***Criterion 40.6 – (Mostly met)***

650. Polish law (Article 12-14 of the Act mentioned in 40.5; Art. 21 of the Act of 5 August 2010 on the protection of classified information) lays down conditions to ensure that the information exchanged by competent authorities is used only for the purpose for, and by the authorities, for which the information was sought or provided. The basic act in the field of IT security of the exchanged information is the Regulation of The Prime Minister of 20 July 2011 on basic ICT security requirements (§ 6-7). Each dissemination of foreign information requires the consent of the source of information (Art. 113(2) of the AML/CFT Act, Art. 16 of the Act on exchange of information with the law enforcement authorities of the Member State of the EU, third countries, EU agencies and international organisations of 2011). Nevertheless, no safeguards are established for the dissemination/ use of information obtained by the GIFI (as a supervisor) and other financial supervisors (except the UKNF) (lack of prior consent requirement, see c. 40.16).

***Criterion 40.7 – (Mostly met)***

651. Exchanged information received from foreign authorities is protected on at least the same standards as domestic sources. The rules on data protection established by the Act on personal data protection of 10 May 2018 and the provisions of the Act on the protection of classified information of 5 August 2010 equally apply to the exchanged information.

652. The GIFI is entitled to refuse to provide information if the foreign country does not guarantee an adequate level of personal data protection (Art. 114(5) of the AML/CFT Act). KAS can also refuse to exchange tax-related information with the EU counterparts if the national law of the requesting EU members state does not ensure that the tax information is covered by the same principles as in Poland (Art. 13(7) Law on tax ordinance). With regard to non-EU countries, the legislation does not provide for such powers, and the AT was informed that the requests may be refused only when such specific provisions are included in the concluded agreements. The Act on CBA does not provide for powers to refuse providing the information when the foreign counterpart does not guarantee an adequate level of personal data protection. No information has been provided to the AT with regard to other competent authorities.

***Criterion 40.8 – (Mostly met)***

653. The powers and the investigative techniques available to the LEAs in accordance with the domestic law can be used to conduct inquiries and obtain information on behalf of foreign counterparts, based on the general framework and the available channels for international co-operation (c. 40.18). The GIFI has powers to acquire information for the purpose of its disclosure to foreign FIUs (Art. 111(4) of the AML/CFT Act). Art. 111 (1) – (3) of the AML/CFT Act provides for a general requirement that ensures that all the information and documents possessed by the GIFI shall be made available to foreign

counterparts. As a supervisor, the GIFI can acquire information on AML/CFT supervision for the purpose of its disclosure to foreign FIUs (Article 116 of the AML/CFT Law). The UKNF is able to conduct such inquiries, but only in relation to prudential supervision (Art. 141f (3a) of the Polish Banking Act; Art. 342 of the 2015 Insurance Act; Article 25(3) of the Act of 29 July 2005 on Capital Market Supervision). No information has been provided on the powers of other financial supervisors.

***Criterion 40.9 – (Met)***

654. Articles 110-116 of the AML/CFT Law establish a wide range of international co-operation possibilities for the GIFI, regardless of whether foreign FIUs are administrative, LE, judicial or other in nature.

***Criterion 40.10 – (Met)***

655. There is no legal provision that would prevent the GIFI to respond to requests to provide feedback both on the quality/content of responses and the further use of information – such as transaction suspensions, notifications to LEAs etc. This occurs in both cases when GIFI replies to requests and when GIFI receives information from another FIU.

***Criterion 40.11 – (Mostly met)***

656. Articles 111 (1) and (2) of the AML/CFT Act refer to making any data in the GIFI's possession, obtained directly or indirectly, available to Financial Intelligence Units. As set out under Article 111(4) of the AML/CFT Act in the scope of his/her powers defined in the Act, the GIFI may acquire information for the purpose of its disclosure to a foreign Financial Intelligence Unit. As explained in the analysis on c. 40.3, the provisions of the new AML/CFT Act entitles the GIFI to exchange information based on the principle of reciprocity, as the previous condition requiring the existence of bilateral/ multilateral agreements or arrangements has been removed.

657. The GIFI can refuse to provide information (article 114 AML/CFT Act) in very specific cases, for instance, when it is subject to protection in accordance with the provisions on the protection of classified information or the assistance could jeopardize the performance of tasks by the authorities or could pose a threat to the security of the state or the public order or a third country does not guarantee an adequate level of personal data protection.

658. The exemption in relation to the provisions on the protection of classified information (Article 96(1) of the AML/CFT Act) would prevail when compared with other provisions of the article. Situations in which the answering a request from a foreign counterpart requires provision of classified information are very rare and, according to the authorities, do not impact the quality or timeliness of responses. In such situations, the GIFI must undertake measures to de-classify that information to the extent it can be shared with another FIU to support the answer to the request.

***Criterion 40.12 – (Partly met)***

659. Article 116 of the AML/CFT Act provides a legal basis for the GIFI to provide and acquire supervisory information to and from foreign counterparts, excluding the classified documents and information. The UKNF and NBP have no legal basis to exchange AML/CFT information with their counterparts. Art. 10(a)(6) of the Banking Act, Articles 20 and 21 of the Act of 29 July 2005 on capital market supervision and Article 17 of the Act of 22 May 2003 on insurance and pension fund supervision provide a legal basis for the UKNF to cooperate with foreign counterparts under the rules and procedures provided by the concluded agreements with another jurisdiction, but only in relation to prudential

information. The AT has not been provided with information about the legal basis for exchange of supervisory information in respect of the other supervisory authorities identified under R.26.

***Criterion 40.13 – (Partly met)***

660. See under c.40.11 and 40.12 for the scope of information exchange by the GIFI (limited by the restrictions on classified documents and information). As explained under c.40.12, in the absence of a legal basis, the UKNF and the NBP do not exchange AML/CFT information. Concerning the exchange of prudential supervision information, the UKNF requires specific agreements to be in place, which are also limited by the range of the information to be exchanged, i.e., when it is contrary to the sovereignty, security or public interest of Poland or the other country. The authorities further explained that this category of information is exchanged on a voluntary basis, which allows them a certain degree of discretion (the decision on information sharing being constructed on a case-by-case basis and does not refer to specific legal restrictions). As indicated above, no information was provided to the AT about measures in place with regard to financial supervisors other than the GIFI and UKNF.

***Criterion 40.14 – (Partly met)***

661. (a) (b) The legal basis limitations described under c.40.12 and c40.13 apply here (ability to exchange regulatory information only in relation to prudential supervision (UKNF and NBP) and only within the framework of an agreement (UKNF).

662. (c) Only the GIFI can exchange AML/CFT information (subject to comments made under c.40.11 and 40.12 above).

***Criterion 40.15 – (Partly met)***

663. Article 116 of the AML/CFT Law provides the GIFI with a legal basis to acquire information on AML/CFT supervision for the purpose of its disclosure to foreign FIUs, excepting the classified information. No specific provisions are in place on the powers to authorise/ facilitate the ability of foreign counterparts to conduct the inquiries themselves in the country.

664. The UKNF is able to conduct such inquiries, but only in relation to prudential supervision (Art. 141f (3a) of the Polish Banking Act; Art. 342 of the 2015 Insurance Act; Article 25(3) of the Act of 29 July 2005 on Capital Market Supervision). The provisions also entitle the facilitation of the foreign counterparts to perform group supervision. No information in relation to other financial supervisors.

***Criterion 40.16 – (Not met)***

665. Art. 116 of the AML/CFT Act regulating the powers of the GIFI to cooperate with foreign financial supervisors does not establish any requirements for prior authorisation to be obtained from foreign counterparts on the dissemination of the exchanged information / use of information for supervisory/ non-supervisory purposes.

666. The UKNF, concerning the exchanged information on prudential supervision matters, is required to obtain such authorisation from the foreign counterparts (Art. 20 of the Act on Capital market supervision; Art. 10a of the Banking Act; Art. 108 and 111 of the Act on Payment Services). No information was provided to the AT on similar powers of other financial supervisors.

***Criterion 40.17 – (Met)***

667. The legal basis which enables the LEAs to exchange with foreign counterparts domestically available information is described under c. 40.1 and is relevant for the

purpose of c. 40.17.

668. ARO is the appointed central contact point for international exchange of information on assets derived from crime. The co-operation platforms include SIENA (EU member states) or CAREN (non-EU countries).

***Criterion 40.18 – (Met)***

669. The powers and the investigative techniques available in accordance with the domestic law can be used to conduct inquiries and obtain information on behalf of foreign counterparts, based on the general framework and the available channels for international co-operation (c. 40.1 and 40.2.).

***Criterion 40.19 – (Met)***

670. The power of the PPO to form joint investigation teams is provided by the Code of Criminal Procedure (Article 589b of the CCP and the following articles).

***Criterion 40.20 – (Mostly met)***

671. The GIFI has the ability to exchange information indirectly with non-counterparts. It also may conclude agreements with such authorities for defining the procedure and the technical terms of acquiring and making information available (Art. 116 of the AML/CFT Act). The UKNF cannot exchange information with non-counterparts. The CBA and the ISA have no restrictions to cooperate with non-counterparts, as the special acts regulating their activity make a general reference to foreign competent authorities and services (Art. 2 of the Act on CBA and Art. 8 of the Act on ISA). The AT has not been provided with the relevant information with regard to other competent authorities.

***Weighting and Conclusion***

672. Most of the criteria under R.40 are either met or mostly met. Some shortcomings remain to be covered. The supervisory authorities (other than the GIFI) do not have a legal basis for co-operation with foreign counterparts in the AML/CFT area (c. 40.1; 40.12-40.14). All supervisory authorities do not have powers to conduct ML/TF related inquiries on behalf of foreign counterparts and to authorise or facilitate such inquiries to be conducted by the requesting authority (c.40.15). The restrictions on disclosure of information are not applicable in relation to all supervisory authorities (c.40.16). There is no clear process for timely execution of the requests by the CBA and ISA in connection to requests coming from foreign counterparts with whom no agreement has been established. The requirement for prior agreement of the Prime minister in order to cooperate, applicable for the CBA and the ISA, does not ensure that the most efficient means to cooperate are used, especially in relation to foreign counterparts with whom no agreement has been established (c.40.2). The GIFI's powers to exchange information is restricted by the limitation regarding the classified information (c.40.5; 40.11). The ability to refuse the co-operation in cases where the requesting authority cannot protect the information effectively is provided for expressly only in relation to the GIFI and the KAS (c.40.7). Competent authorities, other than the GIFI, CBA and ISA, do not have powers to cooperate with non-counterparts (c.40.20). **R.40 is rated Largely Compliant.**

## Summary of Technical Compliance – Deficiencies

**ANNEX TABLE 1. COMPLIANCE WITH FATF RECOMMENDATIONS**

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	<b>PC</b>	<ul style="list-style-type: none"> <li>• No risk-based approach to allocating resources and implementing measures to prevent or mitigate ML/TF;</li> <li>• 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;</li> <li>• 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;</li> <li>• 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;</li> <li>• The requirement for the obligated institutions to make their ML/TF risk assessments available to professional self-regulatory bodies or associations is discretionary ;</li> <li>• There is no explicit requirement to take enhanced measures to manage and mitigate the risks where higher risks are identified.</li> </ul>
2. National co-operation and coordination	<b>LC</b>	<ul style="list-style-type: none"> <li>• No operative coordination platform;</li> <li>• No formal co-operation and coordination mechanisms to combat the financing of proliferation of WMD.</li> </ul>
3. Money laundering offences	<b>LC</b>	<ul style="list-style-type: none"> <li>• • The scope of the ML offence is limited by the requirement of a potential result i.e., a danger to the determination of criminal origin resulting from the perpetrator's action, by the physical element of transporting abroad and by the concerns regarding the coverage of directly obtained proceeds;</li> <li>• • The limitations of the corporate liability regime are detrimental to the dissuasiveness of the penalties.</li> </ul>
4. Confiscation and provisional measures	<b>LC</b>	<ul style="list-style-type: none"> <li>• The confiscation of the instrumentalities, including of the property used in, intended, or allocated for use in TF, terrorist acts or terrorist organisation has only a discretionary character;</li> <li>• The property subject to confiscation does not include intangible assets;</li> <li>• The confiscation of the laundered property is not provided for expressly;</li> <li>• No comprehensive mechanism to preserve and manage seized or confiscated assets.</li> </ul>
5. Terrorist financing offence	<b>PC</b>	<ul style="list-style-type: none"> <li>• Not all acts which constitute an offence within the scope of and as defined in the treaties listed in the annex to the TF Convention are covered by the TF offence;</li> <li>• The collection of funds/ assets for terrorist organisations and individual terrorists for any purpose is not covered;</li> <li>• The provision of funds/ assets for terrorist organisations and individual terrorists for any purpose is impacted by the terminology used to define "terrorist organisations" and "terrorist", which is not fully in line with the FATF Glossary and by the restrictive interpretation of the "intention" element by the practitioners and by the judiciary, which requires that such offences must always be linked to a concrete terrorist act;</li> <li>• The indirect funding and the partial use of funds/ assets is not expressly covered and the TF offence does not distinguish between legitimate or illegitimate source;</li> <li>• The financing of travel of individuals for the purpose of providing terrorist training and for receiving a terrorist training without the link to the purpose of committing a terrorist act is not covered;</li> </ul>

<b>Recommendations</b>	<b>Rating</b>	<b>Factor(s) underlying the rating</b>
		<ul style="list-style-type: none"> <li>• Not all acts of the TF offence have proportionate and dissuasive character and the scope of criminal liability is limited by the requirement of a prior natural person's criminal liability.</li> </ul>
6. Targeted financial sanctions related to terrorism & TF	<b>LC</b>	<ul style="list-style-type: none"> <li>• No legal requirement obligating to apply specific standard forms for listing, as adopted by the relevant committees and no provision specifying whether Poland's status as a designated state may be made known;</li> <li>• No requirement that a prompt determination shall be made of whether they are satisfied, that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373;</li> <li>• There is a delay (the EU mechanism) for the natural and legal persons which are not reporting entities in applying UNSCR1267.</li> </ul>
7. Targeted financial sanctions related to proliferation	<b>PC</b>	<ul style="list-style-type: none"> <li>• Delays related to the transposition of DPRK designations can still occur;</li> <li>• No clear guidance to financial institutions and other persons or entities on their obligations in taking action under freezing mechanisms;</li> <li>• no domestic provision to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions</li> <li>• the controls and the sanctions are limited to the application of the enhanced CDD measures (Art 43) and do not extend to the application of freezing requirements</li> <li>• no procedures to submit de-listing requests to the Security Council.</li> </ul>
8. Non-profit organisations	<b>PC</b>	<ul style="list-style-type: none"> <li>• No particular risk assessment to identify the features and types of NPOs which by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse;</li> <li>• There was no review of the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for TF;</li> <li>• No comprehensive policies to promote accountability, integrity, and public confidence in the administration and management of NPOs;</li> <li>• Educational programmes to raise and deepen awareness among the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks are absent;</li> <li>• Limited best practices identified to address terrorist financing risk and vulnerabilities and thus protect them from terrorist financing;</li> <li>• Due to the absence of a comprehensive risk assessment on the NPO sector, the implementation of a risk-based approach in supervision is difficult to be applied</li> <li>• A fully developed mechanisms of co-operation between the competent authorities that hold relevant information on NPOs is lacking.</li> </ul>
9. Financial institution secrecy laws	<b>C</b>	
10. Customer due diligence	<b>LC</b>	<ul style="list-style-type: none"> <li>• No specific legal provision prohibiting FIs from keeping anonymous accounts or accounts in obviously fictitious names;</li> <li>• No obligation to pursue CDD when performing occasional transactions that constitute a transfer of funds, where the amount is of 1000 EUR;</li> <li>• The requirement to review existing records to ensure they remain relevant and the enhanced focus that needs to be put on categories of higher risk customers are absent;</li> </ul>

<b>Recommendations</b>	<b>Rating</b>	<b>Factor(s) underlying the rating</b>
		<ul style="list-style-type: none"> <li>• The obligation to define which is the ownership structure of a customer does not amount to understanding it, or the nature of its business;</li> <li>• No requirement to identify the persons having senior management positions, nor the powers that regulate the legal person or arrangement</li> <li>• No requirement to identify the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over a trust</li> <li>• The consideration of the beneficiary of the insurance agreement as a risk factor when determining the application of EDD is not covered, nor the obligation to identify and verify the identity of the BO of the beneficiary when is a legal person or arrangement that poses a higher risk</li> <li>• There is no specific to allow obliged institutions not to pursue CDD processes in the case they reasonably believe this will tip off the customer.</li> </ul>
11. Record keeping	<b>LC</b>	<ul style="list-style-type: none"> <li>• Concerns regarding the defined periods for the keeping of analyses within the framework of the CDD;</li> <li>• No specific provision requiring that this evidence and transaction records subject to record-keeping requirements have to be sufficient to permit reconstruction of individual transactions.</li> </ul>
12. Politically exposed persons	<b>LC</b>	<ul style="list-style-type: none"> <li>• The obligation to establish the source of the customer's wealth and sources of assets is limited to the customer and doesn't extend to BO;</li> <li>• The definition of co-workers is narrower than the FATF definition of close associates;</li> <li>• A direct reference to consider making a suspicious transaction report in case of life insurance contracts is absent.</li> </ul>
13. Correspondent banking	<b>PC</b>	<ul style="list-style-type: none"> <li>• There is no express requirement to assess whether the respondent has been subject to ML/TF investigation or regulatory actions.</li> <li>• The concept of understanding the AML/CFT responsibilities is not fully covered.</li> <li>• There is a gap in the shell bank definition.</li> </ul>
14. Money or value transfer services	<b>LC</b>	<ul style="list-style-type: none"> <li>• There are no formal procedures to be applied to identify persons carrying out MTS without authorisation;</li> <li>• There are no sanctions available for those MVTS which do not require authorisation but only need registration;</li> <li>• It is not clear whether MTS providers should be required to maintain a current list of agents accessible by competent authorities in non-EU countries in which the MTS provider and its agents operate.</li> <li>• There is no explicit requirement for MTS providers to include agents in their AML/CFT programmes.</li> </ul>
15. New technologies	<b>PC</b>	<ul style="list-style-type: none"> <li>• No specific provision to identify and assess the AML/TF risks that may arise due to the development of new products and new business practices;</li> <li>• No provision requiring obliged institutions to undertake a risk assessment prior to the launch or use of new products, practices and technologies and to take the appropriate measures to manage and mitigate the risks;</li> <li>• The scope of VASPs covered in this article does not fully match the FATF definition;</li> <li>• There is no licensing regime or registration regime for VASPs;</li> <li>• The legal framework in force does not include the possibility to impose penalties on VASPs without the requisite license or registration;</li> <li>• No requirements for registration, the possible penalties of withdrawal, restriction or suspension of a license cannot be applied;</li> </ul>

<b>Recommendations</b>	<b>Rating</b>	<b>Factor(s) underlying the rating</b>
		<ul style="list-style-type: none"> <li>• No specific feedback or guideline aimed to the VASPs sector and the particular risks they may face;</li> <li>• No CDD requirements for transactions conducted by a VASP that do not fall under the occasional transactions over 15000 euro or 1 000 euro wire transfers;</li> <li>• Minor shortcomings regarding the timely prioritisation and execution of requests and the lack of a sound case management system impact supervisor's MLA capabilities;</li> <li>• The shortcomings identified in R.40 (in particular c.12 to 16) would also be applicable regarding VASP information.</li> </ul>
16. Wire transfers	<b>LC</b>	<ul style="list-style-type: none"> <li>• Unclear whether an MVTS that is subject to the Polish AML/CFT obligations would be required to implement wire transfer controls when providing services outside Poland and the EU, either directly or through agents;</li> <li>• No requirement to file an SAR in any country affected by the suspicious wire transfer.</li> </ul>
17. Reliance on third parties	<b>PC</b>	<ul style="list-style-type: none"> <li>• There is no explicit reference to the purpose and intended nature of the business relationship being understood;</li> <li>• There is no provision in the AML/CFT Act clearly requiring obliged institutions to take steps to satisfy themselves that data and other relevant information relating to the understanding of the nature of the business will be made available by the third party without delay.</li> <li>• There is no explicit reference to higher country risk being adequately mitigated by the group's AML/CFT authority.</li> </ul>
18. Internal controls and foreign branches and subsidiaries	<b>PC</b>	<ul style="list-style-type: none"> <li>• Internal policies are not explicitly covered in the controls put in place by FIs;</li> <li>• It is unclear to what extent AML/CFT programmes address screening procedures for hiring employees and whether there is a statutory basis for this;</li> <li>• Apart from the banks, the other financial institutions have no provisions related to an independent audit function to test the system;</li> <li>• The content of group-wide AML/CFT programmes is not specified (therefore unclear to which extent compliance, audit and risk functions will receive or disseminate information); nor do they apply to branches and subsidiaries in EEA Member States;</li> <li>• There is no explicit requirement for AML/CFT programmes to impose adequate safeguards on confidentiality, use of information and tipping off;</li> <li>• Where a third country does not permit the proper implementation of AML/CFT requirements, there are no additional measures to be applied for branches and subsidiaries located in EEA member states.</li> </ul>
19. Higher-risk countries	<b>PC</b>	<ul style="list-style-type: none"> <li>• EDD obligation does not apply in relation to branches or majority owned subsidiaries and there is a gap regarding the exceptions permitted in relation to EU Member States and branches/subsidiaries of EU entities;</li> <li>• There is a gap with regard to the exceptions permitted in relation to EU Member States and branches/subsidiaries of EU entities;</li> <li>• Polish legislation does not provide for countermeasures other than EDD, which is subject to specific limitations, when this is called for by the FATF or independently.</li> </ul>
20. Reporting of suspicious transaction	<b>PC</b>	<ul style="list-style-type: none"> <li>• The reporting requirements do not extend to the cases when there are reasonable grounds to suspect that funds are the proceeds of a criminal activity;</li> <li>• Shortcomings in relation to the criminalisation of TF restrict the scope of the TF reporting requirement;</li> <li>• There are concerns over the lack of clarity/ distinction between the modes of the reporting regime.</li> </ul>

<b>Recommendations</b>	<b>Rating</b>	<b>Factor(s) underlying the rating</b>
21. Tipping-off and confidentiality	<b>LC</b>	<ul style="list-style-type: none"> <li>• No provision regarding the liability exemptions for if directors, officers or employees of the obligated institution;</li> <li>• Certain legal provisions allow reporting entities to communicate that an SAR or related information is being filed with the FIU to their customers.</li> </ul>
22. DNFBBs: Customer due diligence	<b>PC</b>	<ul style="list-style-type: none"> <li>• The deficiencies identified in R11, 12, 15 and 17 have impact the implementation of R22, in particular the absence of any requirements related to the assessment of risks and implementation of mitigation measures related to new technologies;</li> <li>• Shortcomings when defining the scope of the requirements related to TCSPs.</li> </ul>
23. DNFBBs: Other measures	<b>LC</b>	<ul style="list-style-type: none"> <li>• The deficiencies of R.18, 19 and 21 impact the implementation of R23.</li> </ul>
24. Transparency and beneficial ownership of legal persons	<b>LC</b>	<ul style="list-style-type: none"> <li>• The ML/TF risks associated with legal persons created in Poland were not fully assessed.</li> <li>• There is no explicit requirement as to where the management board should keep the information or to notify the location to the National Court Register.</li> <li>• It is possible for beneficial ownership information not to be complete for all associations, foundations and cooperatives within the totality of the system.</li> <li>• The definition of beneficial owner has one potential area of uncertainty in relation to the senior managing official, which is not considered to be the beneficial owner where there is suspicion of ML/TF.</li> <li>• There is no requirement for legal persons themselves, administrators or liquidators to retain the relevant information.</li> </ul>
25. Transparency and beneficial ownership of legal arrangements	<b>LC</b>	<ul style="list-style-type: none"> <li>• There is no legal, explicit, requirement for trustees or other persons involved with legal arrangements to disclose their status to obliged entities.</li> </ul>
26. Regulation and supervision of financial institutions	<b>PC</b>	<ul style="list-style-type: none"> <li>• There are gaps in the requirements for preventing criminals and their associates from beneficially owning or otherwise controlling FIs.</li> <li>• There is no information on to what extent core principles institutions are supervised in line with core principles requirements.</li> <li>• There are gaps at the technical level with regard to meeting the precise language of the FATF on the components of risk-based supervision and supervision itself is not wholly risk based.</li> <li>• There is no written policy or procedure in relation to the frequency of review assessment of a FI's risk rating.</li> <li>• There is scope for the UKNF, GIFI and NBP to develop more comprehensive approaches to risk assessment and supervision.</li> <li>• Not all non-core FIs are covered by the framework.</li> <li>• For banks, the management board and supervisory board are subject to a reputation, honesty and integrity test, which would cover association with criminals only to some extent.</li> <li>• For cooperative savings and credit unions, 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.</li> <li>• For currency offices, there is no legal requirement in relation to beneficial owners (unless they are a shareholder/partner) or where a person is an associate of a criminal.</li> </ul>
27. Powers of supervisors	<b>LC</b>	<ul style="list-style-type: none"> <li>• There is no power to suspend a license nor to require an obligated institution to take action;</li> <li>• Not all supervisors are empowered to compel the production of information to reporting entities;</li> <li>• The powers of sanction are not wholly proportionate and dissuasive.</li> </ul>

<b>Recommendations</b>	<b>Rating</b>	<b>Factor(s) underlying the rating</b>
28. Regulation and supervision of DNFBBs	<b>PC</b>	<ul style="list-style-type: none"> <li>• There are gaps in preventing control of casinos by criminals in relation to beneficial owners, senior management, and associates of criminals;</li> <li>• The absence of registration and requirements to prevent criminals and their associates from professional practice or control of a range of DNFBBs negatively affects supervisory designation in practice and the ability to exercise supervisory powers;</li> <li>• There is an absence of powers to suspend registrations of those entities which are registered and to require an obligated institution to undertake specific acts;</li> <li>• Beyond a generic power in the AML/CFT Law there are no risk-based policies or procedures, no risk rating of DNFBBs and risk-based supervision is limited.</li> </ul>
29. Financial intelligence units	<b>C</b>	
30. Responsibilities of law enforcement and investigative authorities	<b>LC</b>	<ul style="list-style-type: none"> <li>• No designated LEAs with specific responsibility to investigate ML and TF offences, except for two authorities (the CBA and the KAS);</li> <li>• No clarity regarding the authority responsible for investigating TF offences that are not against state's security.</li> </ul>
31. Powers of law enforcement and investigative authorities	<b>LC</b>	<ul style="list-style-type: none"> <li>• No powers available to LEAs in relation to undercover agents.</li> </ul>
32. Cash couriers	<b>PC</b>	<ul style="list-style-type: none"> <li>• No declaration system for cash or BNIs within the EU;</li> <li>• Limited powers to stop and restrain cross-border cash.</li> </ul>
33. Statistics	<b>PC</b>	<ul style="list-style-type: none"> <li>• Shortcomings in relation to the statistics on property frozen, seized and confiscated which are available only for ML and TF and not for all proceeds generating crimes;</li> <li>• There is no information on recovered property;</li> <li>• The statistics on SARs are not broken down on ML and TF suspicions.</li> <li>• There are no comprehensive statistics on MLA, both out-going and in-coming requests for all crimes and with a breakdown by jurisdiction.</li> <li>• There are no statistics on pending, executed and refused MLA requests, including the average time of completing the requests.</li> </ul>
34. Guidance and feedback	<b>PC</b>	<ul style="list-style-type: none"> <li>• Lack of specific and comprehensive guidance to assist financial institutions and DNFBBs in detecting and reporting suspicious transactions</li> </ul>
35. Sanctions	<b>PC</b>	<ul style="list-style-type: none"> <li>• There are gaps in the proportionality and dissuasiveness of sanctions applicable to FIs and DNFBBs;</li> <li>• Sanctions cannot be applied in all cases where there is a failure to comply with a requirement of the AML/CFT;</li> <li>• In the absence of criminal sanctions for failing to report or comply with TFS, sanctions on FIs and DNFBBs are not fully dissuasive;</li> <li>• Sanctions applicable to senior members of management, board members and employees with responsibility for implementing AML/CFT obligations are not proportionate or dissuasive;</li> <li>• The absence of a wider power to prohibit individuals and the relatively short maximum period for which individuals can be prohibited by the UKNF means that the overall range of administrative sanctions is partly proportionate and dissuasive.</li> </ul>
36. International instruments	<b>LC</b>	<ul style="list-style-type: none"> <li>• No full implementation of the relevant Conventions due to the deficiencies under R. 3, 4 and 5 (art. 6 and 10 of the Palermo Convention, art. 3 of the Vienna Convention and art. 26 of the Merida Convention) and the unclarity regarding the implementation of certain non-self-executing provisions (art. 15 of the Vienna Convention and art. 53 of the Merida Convention).</li> </ul>

<b>Recommendations</b>	<b>Rating</b>	<b>Factor(s) underlying the rating</b>
37. Mutual legal assistance	<b>LC</b>	<ul style="list-style-type: none"> <li>• There is no clear process for the prioritisation and timely execution of MLA requests and no indication of a sound case management system;</li> <li>• Dual criminality remains a condition for rendering the assistance in cases which do not involve coercive actions.</li> </ul>
38. Mutual legal assistance: freezing and confiscation	<b>LC</b>	<ul style="list-style-type: none"> <li>• The shortcomings identified under R.4 hinder Poland's ability to provide assistance for freezing and confiscation, especially in relation to the lack of a single and detailed mechanism for managing/ disposing of seized or confiscated property, and the limitation of the confiscation powers regarding the intangible property.</li> </ul>
39. Extradition	<b>LC</b>	<ul style="list-style-type: none"> <li>• Lack of a clear process for prioritisation and timely execution of the extradition requests and of a sound case management system.</li> </ul>
40. Other forms of international co-operation	<b>LC</b>	<ul style="list-style-type: none"> <li>• The UKNF and NBP do not have a legal basis for co-operation with the foreign counterparts in the AML/CFT area;</li> <li>• All supervisory authorities do not have powers to conduct ML/TF related inquiries on behalf of foreign counterparts or to authorise/facilitate such inquiries to be conducted by them;</li> <li>• The restrictions on disclosure of information are not applicable in relation to all supervisory authorities;</li> <li>• No clear process for the timely execution of the requests and not most efficient ways to cooperate used by the CBA and ISA in relation to inquires coming from foreign counterparts with whom no agreement has been established, impacted by the requirement for prior agreement of the Prime minister;</li> <li>• The GIFI's powers to exchange information is restricted by the limitation regarding the classified information;</li> <li>• Not all authorities have express powers to refuse providing information in the absence of adequate protection provided by the requesting authority;</li> <li>• Not all authorities have powers to cooperate with non-counterparts.</li> </ul>

## GLOSSARY OF ACRONYMS

ACRONYM	DEFINITION
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
AML/CFT Act in Poland	Act of 1 March 2018 on Counteracting Money Laundering and Financing of Terrorism
BG	Border Guard
CBA	Central Anti-Corruption Bureau
CDD	Customer Due Diligence
CTC-ISA	Counter Terrorism Centre of the Internal Security Agency
CEIDG	Central Register and Information on Economic Activity
CEDUR	Education Centre for Market Participants
CRBO	Central Register of Beneficial Owners
CSCUs Act	Cooperative Savings and Credit Unions Act
CTR	Cash Threshold Report
DFI	Department of Financial Information
DNFBPs	Designated Non-Financial Businesses and Professions
DPMS	Dealers in Precious Metals and Stones
EBA	European Banking Authority
EC	European Commission
EDD	Enhanced Due Diligence
EEA	European Economic Area
EFTA	European Free Trade Association
EIO	European Investigation Order
EAW	European Arrest Order
EMMA	European Money Mule Actions
EU	European Union
FATF	Financial Action Task Force
FI	Financial Institutions
FIU	Financial Intelligence Unit
FSAP	Financial Sector Assessment Program
FSC	The Financial Security Committee
FT	Terrorist Financing
GIFI	General Inspector of Financial Information
HQ	Head Quarters

PPO	General Prosecutor's Office
GRECO	Group of States against Corruption
IMF	International Monetary Fund
ISA	Internal Security Agency
KAS	National Revenue Administration
LEAs	Law Enforcement Agencies
LLC	Limited Liability Company
MER	Mutual Evaluation Report
MoF	Ministry of Finance of Poland
MoJ	Ministry of Justice of Poland
ML	Money Laundering
MLA	Mutual Legal Assistance
MSB	Money Services Business
MVTS	Money or Value Transfer Services
NACSCU	National Association of Cooperative Savings and Credit Unions
NBP	Narodowy Bank Polski (National Bank of Poland)
NCR	National Court Register
NIK	Supreme Audit Office
NPOs	Non-Profit Organisations
NRA	National Risk Assessment
PEPs	Politically Exposed Persons
PCBI	Central Bureau of Investigation of the Police
PESEL (Register)	Universal Electronic System for Registration of the Population Register
PF	Proliferation Financing
PLN	Polish złoty
PNRA	Preliminary National Risk Assessment
PPO	Public Prosecutor's Office
RBA	Risk-Based Approach
REGON	National Official Register of National Economy
RE	Reporting entities
RBA	Risk-based approach
SAR	Suspicious Activity Report
STIR	Automated Risk Scoring Tool (used by the KAS)
STR	Suspicious Transaction Report
TERYT (Register)	Register of Territorial Administrative Divisions (which holds information on business and residential addresses of legal persons and individuals)
TFS	Targeted financial sanctions
TIN	Tax Identification Number

UKNF

Urząd Komisji Nadzoru Finansowego  
(office of the Polish Financial Supervision  
Authority)

© MONEYVAL

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

December 2021

Anti-money laundering and counter-terrorism financing measures

**Poland**

*Fifth Round Mutual Evaluation Report*

This report provides a summary of AML/CFT measures in place in Poland as at the date of the on-site visit (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.