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

MONEYVAL(2013)2

Report on Fourth Assessment Visit

Anti-Money Laundering and Combating the Financing of Terrorism

POLAND

11 April 2013

Poland is a member of MONEYVAL. This evaluation was conducted by MONEYVAL and the mutual evaluation report on the 4th assessment visit of Poland was adopted at its 41st Plenary (Strasbourg, 9-12 April 2013)

TABLE OF CONTENTS

I. PREFACE 7

II. EXECUTIVE SUMMARY 9

III. MUTUAL EVALUATION REPORT 18

1. GENERAL 18

1.1 General Information on Poland 18

1.2 General Situation of Money Laundering and Financing of Terrorism 24

1.3 Overview of the Financial Sector and Designated Non-Financial Businesses and Professions (DNFBPS) 29

1.4 Overview of Commercial Laws and Mechanisms Governing Legal Persons and Arrangements 35

1.5 Overview of Strategy to Prevent Money Laundering and Terrorist Financing 37

2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES 46

2.1 Criminalisation of Money Laundering (R.1) 46

2.2 Criminalisation of Terrorist Financing (SR.II) 58

2.3 Confiscation, Freezing and Seizing of Proceeds of Crime (R.3) 66

2.4 Freezing of Funds Used for Terrorist Financing (SR.III) 76

2.5 The Financial Intelligence Unit and its functions (R.26) 89

2.6 Law enforcement, prosecution and other competent authorities - the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27) 106

3. PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS 116

3.1 Risk of money laundering / financing of terrorism 116

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to R.8) 117

3.3 Third Parties and Introduced Business (R.9) 132

3.4 Financial institution secrecy or confidentiality (R.4) 134

3.5 Record Keeping and Wire Transfer Rules (R.10 and SR. VII) 136

3.6 Monitoring of Transactions and Relationship Reporting (R. 11 and R. 21) 142

3.7 Suspicious Transaction Reports and Other Reporting (R. 13 and SR.IV) 145

3.8 Foreign Branches (R.22) 150

3.9 Shell Banks (R.18) 152

3.10 The Supervisory and Oversight System - Competent Authorities and SROs / Role, Functions, Duties and Powers (Including Sanctions) (R. 23, 29 and 17) 153

3.11 Money or value transfer services (SR. VI) 177

4. PREVENTIVE MEASURES – DESIGNATED NON FINANCIAL BUSINESSES AND PROFESSIONS 181

4.1 Customer due diligence and record-keeping (R.12) 182

4.2 Suspicious transaction reporting (R. 16) 187

4.3 Regulation, supervision and monitoring (R. 24) 193

5. LEGAL PERSONS AND ARRANGEMENTS AND NON-PROFIT ORGANISATIONS 197

5.1 Legal persons – Access to beneficial ownership and control information (R.33) 197

5.2 Legal arrangements – Access to beneficial ownership and control information (R.34) .. 208

5.3 Non-profit organisations (SR.VIII) 209

6. NATIONAL AND INTERNATIONAL CO-OPERATION 217
6.1 National co-operation and co-ordination (R. 31 and R. 32) 217
6.2 The Conventions and United Nations Special Resolutions (R. 35 and SR.I) 222
6.3 Mutual legal assistance (R. 36, SR. V) 225
6.4 Other Forms of International Co-operation (R. 40 and SR.V) 230
7. OTHER ISSUES 236
7.1 Resources and Statistics (R.30 and R.32) 236
7.2 Other Relevant AML/CFT Measures or Issues 236
7.3 General Framework for AML/CFT System (see also section 1.1) 236
IV. TABLES 237
8. Table 1. Ratings of Compliance with FATF Recommendations 237
9. Table 2: Recommended Action Plan to improve the AML/CFT system 251
10. Table 3: Authorities' Response to the Evaluation (if necessary) 263
V. COMPLIANCE WITH THE 3RD EU AML/CFT DIRECTIVE 264
VI. LIST OF ANNEXES 283
Annex 1. Details of all Bodies met on the on-site visit 283
Annex 2. Key Laws, Regulations and other Documents 285
Annex 3. List of Key Law, Regulations and Other materials provided to Evaluation Team 314
Annex 4. Status of Implementation of the Vienna Convention, the Palermo Convention and the UN International Convention for the Suppression of the Financing of Terrorism 315
Annex 5 Status of Implementation of the UN Security Council Resolutions 319
Annex 6. International agreements signed by Poland 325
Annex 7. Inter-agency agreements signed by Law Enforcement 339
Annex 8. MoUs signed by the GIFI 340

LIST OF ACRONYMS USED

ABP	Banks Association of Poland
AML/CFT Act	Act on countering money laundering and terrorism financing
BMWP	International Police Cooperation Bureau
CC	Criminal Code
CCP	Code of Criminal Procedure
CDD	Customer Due Diligence
CEIDG	Central Records and Information on Economic Activity
CETS	Council of Europe Treaty Series
CFT	Combating the financing of terrorism
CPC	Criminal Procedure Code
CTR	Cash transaction report
DNFBPs	Designated Non-Financial Businesses and Professions
EAW	European Arrest Warrant
EC	European Commission
ETS	European Treaty Series [since 1.1.2004: CETS = Council of Europe Treaty Series]
EU	European Union
EUR	Euro
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FT	Financing of Terrorism
GIFI	General Inspector of Financial Information
GRECO	Group of States against Corruption
LEA	Law Enforcement Agency
ISA (ABW)	Internal Security Agency
IT	Information technologies
KRS	Register of Entrepreneurs of the National Court Register
KYC	Know your customer
ML	Money Laundering
MLA	Mutual legal assistance
MLCO	Money Laundering Compliance Officer
MoU	Memorandum of Understanding
MVT	Money Value Transfer

NCCT	Non-cooperative countries and territories
NCR	National Court Register
NBP	National Bank of Poland
NPO	Non-Profit Organisation
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control (US Department of the Treasury)
OGBS	Offshore Group of Banking Supervisors
PEP	Politically Exposed Persons
PSEC	Polish Securities and Exchange Commission
REs	Reporting entities
SR	Special recommendation
SRO	Self-Regulatory Organisation
STRs	Suspicious transaction reports
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCSP	Trust and company service providers
TIN	Tax identification number
UN	United Nations
UNSCR	United Nations Security Council resolution
UTR	Unusual Transaction Report
ZUS	Social Security Office

I. PREFACE

1. This is the fourteenth report in MONEYVAL's fourth round of mutual evaluations, following up the recommendations made in the third round. This evaluation follows the current version of the 2004 AML/CFT Methodology, but does not necessarily cover all the 40+9 FATF Recommendations and Special Recommendations. MONEYVAL concluded that the 4th round should be shorter and more focused and primarily follow up the major recommendations made in the 3rd round. The evaluation team, in line with procedural decisions taken by MONEYVAL, have examined the current effectiveness of implementation of all key and core and some other important FATF recommendations (i.e. Recommendations 1, 3, 4, 5, 10, 13, 17, 23, 26, 29, 30, 31, 32, 35, 36 and 40, and SRI, SRII, SRIII, SRIV and SRV), whatever the rating achieved in the 3rd round.

2. Additionally, the examiners have reassessed the compliance with and effectiveness of implementation of all those other FATF recommendations where the rating was NC or PC in the 3rd round. Furthermore, the report also covers in a separate annex issues related to the Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter the "The Third EU Directive") and Directive 2006/70/EC (the "implementing Directive"). **No ratings have been assigned to the assessment of these issues.**

3. The evaluation was based on the laws, regulations and other materials supplied by Poland, and information obtained by the evaluation team during its on-site visit to Poland from 27 May to 2 June 2012, and subsequently. During the on-site visit, the evaluation team met with officials and representatives of relevant government agencies and the private sector in Poland. A list of bodies met is set out in Annex I to the mutual evaluation report.

4. The evaluation was conducted by an assessment team, which consisted of members of the MONEYVAL Secretariat and MONEYVAL experts in criminal law, law enforcement and regulatory issues and comprised: Mr. Yehuda Shaffer (Deputy State Attorney of the Ministry of Justice, Israel) who participated as legal evaluator, Mr. Gyula Kerdö (senior AML expert in the Financial Supervisory Authority, Hungary), Mr. Oleksiy Feshchenko (First Deputy Head of the State Committee for Financial Monitoring (SDFM), Ukraine) who participated as financial evaluators, Ms. Maja Golik (Department of International Co-operation and Legal Affairs - Financial Inspectorate of the Ministry of Finance, Croatia) who participated as a law enforcement evaluator, Mr. John Ringguth (Executive Secretary to MONEYVAL) and members of the MONEYVAL Secretariat. The experts reviewed the institutional framework, the relevant AML/CFT Laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs), as well as examining the capacity, the implementation and the effectiveness of all these systems.

5. The structure of this report broadly follows the structure of MONEYVAL and FATF reports in the 3rd round, and is split into the following sections:

1. General information
2. Legal system and related institutional measures
3. Preventive measures - financial institutions
4. Preventive measures – designated non-financial businesses and professions
5. Legal persons and arrangements and non-profit organisations
6. National and international cooperation

7. Statistics and resources

Annex (implementation of EU standards).

Appendices (relevant new laws and regulations)

6. This 4th round report should be read in conjunction with the 3rd round adopted mutual evaluation report (as adopted at MONEYVAL's 23rd Plenary meeting – 5-7 June 2007), which is published on MONEYVAL's website[1]. FATF Recommendations that have been considered in this report have been assigned a rating. For those ratings that have not been considered the rating from the 3rd round report continues to apply.

7. Where there have been no material changes from the position as described in the 3rd round report, the text of the 3rd round report remains appropriate and information provided in that assessment has not been repeated in this report. This applies firstly to general and background information. It also applies in respect of the 'description and analysis' section discussing individual FATF Recommendations that are being reassessed in this report and the effectiveness of implementation. Again, only new developments and significant changes are covered by this report. The 'recommendations and comments' in respect of individual Recommendations that have been re-assessed in this report are entirely new and reflect the position of the evaluators on the effectiveness of implementation of the particular Recommendation currently, taking into account all relevant information in respect of the essential and additional criteria which was available to this team of examiners.

8. The ratings that have been reassessed in this report reflect the position as at the on-site visit in 2012 or shortly thereafter.

[1] http://www.coe.int/moneyval

II. EXECUTIVE SUMMARY

1. Background Information

1. This report summarises the major anti-money laundering and counter-terrorist financing measures (AML/CFT) that were in place in the Republic of Poland at the time of the 4th on-site visit (27 May – 2 June 2012) and immediately thereafter. It describes and analyses these measures and offers recommendations on how to strengthen certain aspects of the system. The MONEYVAL 4th cycle of evaluations is a follow-up round, in which Core and Key (and some other important) FATF Recommendations have been re-assessed, as well as all those for which Poland received non-compliant (NC) or partially compliant (PC) ratings in its 3rd round report. This report is not, therefore, a full assessment against the FATF 40 Recommendations 2003 and 9 Special Recommendations 2001, but is intended to update readers on major issues in the AML/CFT system of the Republic of Poland.

2. Key findings

2. The fight against money laundering and terrorist financing is one of the Polish strategic priorities. It was reflected by the National Security Strategy of the Republic of Poland adopted in 2007. Additionally, the specific crimes of money laundering and terrorism financing are among the priority areas identified by the draft National Program for Counteracting and Combating Organised Crime for the years 2012-2016 and the draft National Program for Combating Terrorism for the years 2012-2016. Cooperation is also an essential component of the Polish AML/CFT strategy.

3. Money laundering is criminalised by Article 299 of the Penal Code, based on an "all-crimes" approach. Since the 3rd round evaluation an autonomous offence of terrorist financing has been added to the Penal Code (section 165a) although the offence, as legislated, is not fully in line with requirements on the criminalisation of financing of terrorism. The deficiencies previously identified in the 3rd round mutual evaluation report (MER) of Poland regarding the lack of all aspects of the physical and material elements of the Vienna and Palermo conventions have unfortunately not yet been addressed. Association with or conspiracy to commit money laundering (ML) is still not covered in the legislation. The number of investigations and prosecutions for ML offences appears low compared to the level of funds-generating crime in Poland.

4. With regard to the criminalisation of the financing of terrorism, Poland has introduced a new terrorist financing (TF) offence to the Criminal Code, however this Article is not fully in line with the TF Convention.

5. The provisions in Articles 44 and 45 of the Penal Code remain unchanged since the 3rd round evaluation and contain the necessary powers to confiscate the proceeds of crime. Nevertheless the confiscation regime remains incomplete as instrumentalities, especially when owned by third parties, are not included in the legal framework. Furthermore, the level of final confiscations appears low compared to the level of funds-generating crime in Poland.

6. United Nations (UN) Resolutions 1267 and 1373 (in respect of Non-European Union internals[2]) are legally implemented through European Union (EU) mechanisms. Since the 3rd round Poland has

[2] EU internals include persons, groups and entities having their roots, main activities and objectives within the EU (see EU Regulation 2580/2001).

introduced Article 20d of the Act on Countering Money Laundering and Terrorism Financing (AML/CFT Act), which provides a clear legal mechanism that would potentially cover designations in Poland in respect of EU citizens or named persons not covered by the EU clearing house list proposed by other member states; however, the Polish authorities have not yet applied this mechanism.

7. The General Inspector of Financial Information (GIFI), supported by the Department for Financial Information, comprises the Polish financial intelligence unit (FIU), which is an administrative unit. The functions and responsibilities of the FIU, are set out in AML/CFT Act, and appear to sufficiently cover the core requirements set out in Recommendation 26.

8. Several law enforcement investigative units are authorised to conduct money laundering investigations, but seem to be over - focused on investigation of self - laundering and especially on tax related predicate offences. Most of the investigative units seem to lack both a proactive approach and the necessary training for conducting more complex ML investigations and rely totally on the prosecutorial initiative.

9. The reporting institutions demonstrated a high-level of awareness of the suspicious transaction reporting requirements and appreciated the GIFI Reporting Guide. The highest number of suspicious transaction reports (STRs) were filed by banks. The number of STRs from designated non-financial businesses and professions (DNFBPs) has increased; nevertheless, the reporting level of certain DNFBPs still appears inadequate. Furthermore, there are still several technical shortcomings in the reporting requirement.

10. All financial institutions and service providers are subjected to the AML/CFT legislation. Poland has a broadly sound legal structure for the preventive standards. However, the evaluators noted that the legislative provisions dealing with customer due diligence (CDD) requirements are still not entirely in line with the FATF Standards. In particular, there is no clear requirement to identify the ultimate beneficial owner and no requirement to verify the customer's identity from reliable and independent sources.

11. The Polish Financial Supervisory Authority (PFSA) plays a positive role in the supervision of financial institutions, in full cooperation with the GIFI. The National Bank of Poland (NBP) is responsible for the supervision of the currency exchange offices, while the National Savings and Credit Cooperative Union (NSCCU) supervised the credit unions, at the time of the on-site visit of the evaluation team. All financial institutions are required to be licensed or registered. The GIFI and the supervisory bodies independently carry out a number of on-site inspections to control the compliance with the AML/CFT requirements according to detailed manuals.

12. The AML/CFT framework generally applies to DNFBPs as well. The DNFBPs demonstrated a basic understanding of their AML/CFT obligations although they indicated the need for more sector-specific guidance from the GIFI and the supervisory authorities.

13. There is no requirement for the Register of commercial companies to identify the beneficial owners of a company which holds shares of another registered company. Polish law does not require adequate transparency concerning beneficial ownership and control of legal persons.

14. Poland can provide a wide range of mutual legal assistance and co-operation. Legal provisions for providing mutual legal assistance and co-operation are laid down in domestic law, bilateral and multilateral treaties and apply both to ML and TF.

3. Legal Systems and Related Institutional Measures

15. Money laundering is criminalised by Article 299 of the Penal Code, based on an "all-crimes" approach. The deficiencies previously identified in the 3rd round MER of Poland regarding the lack of all aspects of the physical and material elements of the Vienna and Palermo conventions have unfortunately not yet been addressed. Additionally, conspiracy to commit ML is still not covered in the legislation. Quasi-criminal liability has been extended to legal persons, though this has not yet been tested in ML cases.

16. The evaluation team was also pleased to see that progress has been made on the number of ML convictions. It was noted that in the last three years, convictions for money laundering were successfully obtained in 2009 (18), 2010 (21), 2011 (19), including three stand-alone money laundering prosecutions. However, the number of investigations and prosecutions for money laundering (ML) offences appears low compared to the level of funds-generating crime in Poland

17. The evaluation team concluded that the inability to establish a predicate offence is a major cause for termination of money laundering proceedings. This may imply that prosecutors are requiring a high degree of specificity in respect of a particular predicate offence. Most cases appear to relate to self-laundering and the problem of proving the predicate offence is often addressed by prosecuting the money laundering and predicate offences in the same indictment.

18. Since the 3rd round evaluation an autonomous offence of terrorist financing has been added to the Penal Code (section 165a). Unfortunately the offence, as legislated, does not cover funding a terrorist organisation or an individual terrorist for any purpose, and requires proof of intention to finance an offence of a terrorist character.

19. It seems to the evaluators that, whereas the risk of terrorist activity in Poland may be legitimately perceived as low, the risk of terrorist financing in Poland should be treated as being as high as in any other jurisdiction. Nevertheless, in the absence of any criminal investigations for financing of terrorism, assessment of the effectiveness of the system was not possible.

20. The provisions in Articles 44 and 45 of the Penal Code remain unchanged since the 3rd round evaluation and contain the necessary powers to confiscate proceeds of crime and additionally provide for reversing the burden of proof in certain cases and in ensuring confiscation in the event of a transaction intended to defeat confiscation. Recent Supreme Court decisions have confirmed the interpretation of these provisions - especially as they relate to the identification and confiscation of "indirect proceeds" arising from an offence. Nevertheless the confiscation regime remains incomplete as instrumentalities, especially when owned by third parties, are not included in the legal framework. The discretionary character of the confiscation of the instrumentalities raises concerns. Furthermore, the level of final confiscations appears low compared to the level of funds-generating crime in Poland.

21. UN Resolutions 1267 and 1373 (in respect of Non-European Union internals) are legally implemented through EU mechanisms. Since the 3rd round an amended Article 20d of the AML/CFT Act has provided a clear legal mechanism, which would potentially cover designations in Poland in respect of EU citizens or named persons not covered by the EU clearing house list proposed by other member states. Unfortunately the Polish authorities have not applied this mechanism yet. There remain no freezing orders under the United Nations Security Council Resolutions (UNSCRs).

22. The AML/CFT Act provides for the powers and functions of the GIFI. The General Inspector of Financial Information (GIFI), supported by the Department for Financial Information, comprises the Polish FIU, which is an administrative unit. The FIU employees are skilled, motivated and regularly trained. The GIFI's staff has recently been augmented by a senior appointment from law enforcement. The FIU has direct access to a variety of external databases in order to conduct financial analysis.

Additionally, the FIU is authorised to supervise obliged institutions. The FIU is active in building relationships with the obliged institutions and in raising their awareness through trainings and seminars.

23. The GIFI is required and empowered to analyse STRs and disseminate its reports to the Public Prosecutors' offices and law enforcement bodies. However, the largest number of reports sent to other bodies were disseminated to the fiscal control authority; consequently, most of the FIU information seems to be utilised for fiscal purposes. The GIFI has managed to build the necessary trust with law enforcement agencies and prosecutors to develop active cooperation.

24. Law enforcement agencies refer to the FIU as an effective channel for obtaining bank information of persons suspected of committing predicate offences and for freezing their accounts. Nevertheless, the FIU is not approached systematically to detect suspicion of money laundering by entities unknown to law enforcement agencies; accordingly these agencies make little use of reports sent to them by the FIU regarding such suspicions. There have also been very few requests by Police to the GIFI in respect of above threshold transactions, despite the fact that the FIU receives on an annual basis around 30 million such reports.

25. At the time of the 3rd round evaluation, the evaluators concluded that the pro-active approach by the Polish law enforcement authorities to ML/FT investigations was limited. During the 4th round the evaluators noted that the situation had not improved significantly as ML/FT cases are rarely being actively investigated or prosecuted.

4. Preventive Measures – financial institutions

26. Since the 3rd round mutual evaluation Poland has made welcome progress in aligning its AML/CFT legal framework with international standards. In particular, the risk-based approach has been introduced within the Polish AML/CFT regime. This means that financial institutions may allocate resources and calibrate the application of customer due diligence measures in accordance with the ML/FT risks posed by a particular transaction or client. Limited information was provided on the ML/FT risks in Poland since no formal risk assessment was carried out by the Polish authorities.

27. According to the legal requirements, reporting institutions are obliged to establish due diligence procedures. The identification and verification of the identity of a natural or legal person and of the beneficial owner on the basis of the identity documents, as well as data or information obtained from a reliable and independent source is required by the AML/CFT Act. Enhanced CDD is required by law for relationships established with politically exposed persons (PEPs), correspondent current accounts and non-face to face relationships.

28. The evaluators noted that financial institutions in Poland are generally aware of the CDD requirements as a result of the significant efforts invested in outreach to the financial sector by the GIFI and the PFSA. Such outreach generally takes the form of training programmes and clarification notes published on the websites of the GIFI and the PFSA. In addition, a guide entitled "Counteracting money laundering and terrorism financing" was issued by the GIFI to assist financial institutions and other reporting entities in the practical application of their AML/CFT requirements.

29. The scope of AML/CFT obligations covers all financial institutions (FI) as defined by the FATF standard.

30. Although the AML/CFT Act provides for reliance on third parties a number of significant gaps exist in the legislation. The provisions on reliance should therefore be entirely amended to be brought in line with the criteria set out under the FATF Recommendations.

31. In Poland no financial institution secrecy law inhibits the implementation of the FATF Recommendations. The information presented to the evaluation team by the Polish authorities and the private sector did not reveal any instances where professional secrecy provisions limited the information exchange in practice.

32. Although, the GIFI, other competent authorities and financial institutions did not report that they had experienced any problem in obtaining information, the record-keeping period in relation to customer data is not linked to the date of the termination of an account or a business relationship and there is no requirement to retain business correspondence. Nonetheless, in practice obligated institutions do maintain all necessary documents for more than 5 years following the termination of a business relationship.

33. In respect of the wire transfers requirements, Poland specifically relies on European regulations Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds implementing FATF Recommendations on wire transfers. The requirements seem to be comprehensively and adequately covered by EU Regulation 1781/2006 which is mandatory for the Member States of the EU and therefore directly applicable in Poland. The requirements appear to be effectively applied in practice.

34. Although there is no specific requirement to pay special attention to unusual transactions, to some extent several financial institutions appeared to conduct an analysis of such transactions. The manner in which Article 8a paragraph 1 is drafted could potentially deflect the focus from complex, unusual large transactions or unusual patterns of transactions, which is the primary purpose of the FATF Recommendation.

35. There is no requirement to give special attention to business relationships with persons from or in countries which do not or insufficiently apply the FATF Recommendations and no requirement to apply appropriate counter-measures.

36. The requirement to submit STRs is primarily set out under the AML/CFT Law. It has to be noted that the reporting obligation provided by the AML/CFT Act refers to "*transactions*" and not to "*funds*" and potentially limits the scope of the reporting obligation. Reporting of attempted transactions is partially covered under the AML/CFT Act.

37. In terms of effectiveness, the highest number of STRs was filed by banks. In fact, banks have submitted 87% of the total number of reports received by the GIFI. The other significant contributors were investment funds, cooperative units, brokerage houses and insurance companies. On the whole, it appears that all financial institutions are active in submitting reports to the GIFI.

38. There is no explicit obligation for branches and subsidiaries of Polish financial institutions established in a foreign jurisdiction to apply higher standards when the AML/CFT requirements of home and host countries differ. The Polish authorities informed the evaluation team that all branches/subsidiaries of Polish financial institutions are situated within EU member states, with one exception (a subsidiary situated in Ukraine). Therefore, it is presumed that all such branches and subsidiaries are subject to AML/CFT measures which are equivalent to those in Poland. Additionally, there is no requirement to inform the home country supervisor where it is impossible to apply AML/CFT measures which are at least equivalent to those in force in Poland.

39. Poland has implemented most of the recommendations made in the 3rd round report in relation to shell banks within its legislative framework. During the on-site visit the evaluators were not aware of any shell banks operating in Poland or any banks which had corresponding relations with shell banks or those banks that allowed shell banks to use their accounts. Representatives of financial institutions

demonstrated that they apply proper risk policies when establishing a business relationship *inter alia* before establishing correspondent banking relationship.

40. All financial institutions are subject to the AML/CFT Act and are therefore subject to the supervision of the GIFI and other supervisory authorities, including the PFSA, the NBP and the NSCCU[3]. Further provisions on the regulation and supervision of financial institutions are found in the sector-specific laws and in GIFI guidelines.

41. The GIFI is responsible for monitoring financial institutions' compliance with the requirements under the AML/CFT Act. According to the AML/CFT Act compliance monitoring of financial institutions may also be carried out by the PFSA, the NBP and the NSCCU within the legislative framework setting out the powers and functions of such supervisory authorities.

42. The GIFI and the supervisory bodies independently carry out a number of on-site inspections to control compliance with the AML/CFT requirements. The PFSA's AML/CFT unit appears to be understaffed. Annually the PFSA sets up a risk-based plan for on-site visits, though at the time of the on-site visit of the evaluation team there were no regulations on their frequency. The GIFI and the supervisory authorities carry out the on-site inspections according to detailed manuals. Overall, the evaluators reached the conclusion that AML/CFT supervision is effectively carried out by the GIFI and all supervisory authorities.

43. The requirements related to prevention of criminals from controlling FIs and the fit and proper criteria are in place through sectoral laws.

44. Since the 3rd round evaluation, the Polish authorities have introduced a number of administrative sanctions for breaches of the AML/CFT Act. The maximum fine that can be applied by the GIFI amounts to approximately €180,000. However, considering the number of sanctions imposed and the number of compliance letters sent by the GIFI and the PFSA to financial institutions, the evaluators believe that the sanctioning regime is effective and proportionate. As a result, the evaluators concluded that the sanctioning regime is sufficiently dissuasive.

45. Since the 3rd round report Poland has enacted the Act on Payment Services, which transposes the Payment Services Directive (PSD). Since Poland has only recently implemented the PSD, the licensing process was still underway at the time of the on-site visit; consequently, the evaluators could not determine the effectiveness of the licensing system.

5. Preventive Measures – Designated Non-Financial Businesses and Professions

46. In Poland almost all DNFBPs specified by the FATF Recommendations are covered by the AML/CFT Act and all the obligations applicable to the FIs are relevant for the DNFBPs too.

47. Poland has demonstrated significant progress in the implementation of the AML/CFT requirements for DNFBPs since 3rd Round Evaluation. The Gambling Law in some cases requires casinos to apply even stricter CDD measures than prescribed by the AML/CFT Act.

48. The legal system is largely in place and the AML/CFT provisions apply equally to DNFBPs. DNFBPs during the on-site visit demonstrated a high level of awareness of the AML/CFT requirements. However, similarly to financial institutions, the understanding and awareness of the

[3] Since 27 October 2012 the PFSA is responsible for the supervision over co-operative savings and credit unions and the National Association of Co-operative Savings and Credit Unions. Nonetheless the NCCSU can also supervise savings unions.

obligations dealing with the identification beneficial owners of DNFBPs does not appear to be adequate.

49. Since the 3rd round MER, the number of STRs from DNFBPs has increased. Nevertheless, the reporting level of certain DNFBPs is still considered to be inadequate. The FIU performed outreach activities to DNFBPs, however, no sector-specific guidelines have been issued to assist these sectors.

50. During the on-site interviews, the representatives of the DNFBPs demonstrated a high level of awareness of their reporting obligations. The reporting regime for DNFBPs contains all the positive elements and deficiencies of the reporting regime applicable to financial institutions.

51. Casinos are subject to comprehensive supervision. During the interviews, the casino representatives indicated that the Customs Service inspects casinos more than once annually (mainly for fiscal reasons). The FIU conducts a one-week inspection of every casino approximately every 2 to 3 years. Additionally, the National Bank conducts annual inspections (for casinos that operate exchange offices).

52. The GIFI is not, however, sufficiently equipped with human resources in order to conduct an adequate level of on-site inspections of all DNFBPs.

53. Casinos, notaries and legal professionals receive sufficient attention from supervisory bodies. This is due to the involvement of Customs Service in the supervision of casinos and self-regulatory organisations (SROs) for the legal professionals. For the real estate agents, the GIFI's resources are not adequate, especially taking into account the complete absence of reporting and the high ML vulnerability of the real estate sector.

6. Legal Persons and Arrangements & Non-Profit Organisations

54. The Code of Commercial Partnerships and Companies is a comprehensive source of commercial law and regulates the formation, structure, operation, dissolution, merging, division and transformation of commercial partnerships and companies.

55. However, Polish law does not clearly provide requirements for information about the beneficial ownership of companies as it is defined in the Glossary to the FATF Recommendations (i.e. one who ultimately owns or has effective control). There is no requirement for the Register of Commercial Companies to identify the beneficial owners of a company which holds shares of another registered company. Similarly where foreign companies are registered in Poland beneficial ownership information is not available. During the on-site visit several representatives from different law enforcement agencies all conveyed to the evaluators their frustration due to the inadequacy of available information as to beneficial ownership both with regard to domestic and foreign legal entities; this is compounded by the failure to require financial institutions to identify the ultimate beneficial owner.

56. It thus appears to the evaluators that Polish law does not require adequate transparency concerning beneficial ownership and control of legal persons and it is bound to be a difficult and lengthy process for competent authorities to obtain the necessary information. Polish authorities can in practice rely on investigative and other powers of law enforcement to produce from company records the immediate owners of companies. However if these in turn are also legal persons, the competent authorities have to investigate further up the chain.

57. With respect to non-profit organisations (NPOs) there has been no formal review of the adequacy of laws and regulations which relate to NPO. There are very limited measures in place to prevent terrorist organisations from posing as legitimate NPOs or preventing funds or the assets collected by

or transferred through non-profit sector from being diverted to support the activities of terrorists or terrorist organisations.

7. National and International Co-operation

58. In the view of the evaluation team, since the 3rd round evaluation, the Polish authorities have continued to improve and strengthen cooperation between the main stakeholders as an important part of the AML/CFT system.

59. The fight against money laundering and terrorist financing is one of the Polish strategic priorities. The strategy of combating money laundering and terrorism financing adopted after the 3rd round of the mutual evaluation by the Polish authorities involved actions in numerous key areas. In particular, the Polish authorities: adopted measures to create and implement legal provisions in the area of combating money laundering and terrorism financing; facilitated the implementation of international AML/CFT standards; created an effective inter-institutional cooperation; participated in national, regional and international AML/CFT initiatives; and provided assistance to other countries in the area of AML/CFT.

60. The specific crimes of money laundering and terrorism financing are among the priority areas identified by the draft National Program for Counteracting and Combating Organised Crime for the years 2012 – 2016 and the draft National Program for Combating Terrorism for the years 2012 -2016.

61. The GIFI appears to be central policy maker in the Polish AML/CFT system. Nevertheless, there is no legal basis in place for any formal mechanism for domestic coordination in the AML/CFT area and there is no body which takers overall responsibility for coordinating activities in the area of AML/CFT. However, cooperation is an essential component of the Polish AML/CFT strategy and appears to operate effectively in practice.

62. On a practical level, the GIFI cooperates with law enforcement authorities, especially with the Public Prosecutors' Office and the Police. In the course of an ML/FT investigation the Police and the Public Prosecutors' Office co-operate closely with the GIFI. In fact, the GIFI is commonly relied upon by the Police to obtain additional information, whether such information is to be obtained from a reporting entity or from a foreign authority.

63. Poland is a party to international agreements, such as the 1959 European Convention on Mutual Legal Assistance in Criminal Matters and its additional protocol, the 1957 Council of Europe Convention on Extradition and its two protocols and the 1990 Strasbourg Convention. Furthermore, Poland has also signed and ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism.

64. Poland can provide a wide range of mutual legal assistance and co-operation. In the Polish law, no financial institution secrecy law appears to inhibit the implementation of the FATF Recommendations.

65. Pursuant to the provisions of the AML/CFT Act, the GIFI on its own initiative or on the basis of a request, can send, receive or exchange information and documents with foreign authorities. The law enforcement authorities use informal channels, such as Interpol and Europol, for the exchange of information in the course of criminal investigations.

8. Resources and statistics

66. Since the 3rd round, the GIFI has gone through a restructuring process and has established various new units: a unit for domestic co-operation responsible for the effective exchange of information with

reporting entities; a special unit for complex analysis; a unit entrusted with the function to carry out preliminary analysis of submitted STRs; and other units for data modelling and data processing, including IT infrastructure.

67. At the time of the on-site visit, the Department of Financial Information of the GIFI employed 52 persons, including the Director and two Deputy Directors. The evaluators are of the opinion that the Department is not adequately staffed, especially considering the large number of STRs received. All the employees of the Department possess higher education qualifications, are skilled and highly motivated. All staff members must be subject to a security clearance process. The confidentiality rules of the AML/CFT Act apply to the GIFI and the employees of the Department of Financial Information.

68. The employees of the Department are trained on a regular basis. According to the Polish authorities, constant vocational training of the staff has become a common practice especially focusing on skills related to the use of IT tools in the analysis of information and security of processed information. The analysts have at their disposal a comprehensive range of analytical software. In addition, regular training in the area of AML/CFT risks and vulnerabilities, legal awareness and financial law is provided.

69. Law enforcement bodies and prosecution authorities appear to have adequate human and technical resources. The officers of competent authorities maintain high professional standards, including standards concerning confidentiality and integrity. They are appropriately skilled. Integrity standards to be followed are set out in sectoral laws prescribing legal conditions for employment.

70. In the 3rd round evaluation the number of AML/CFT experts within the Polish supervisory authorities was deemed to be insufficient, especially within the Polish Securities and Exchange Commission (PSEC). Furthermore, the evaluators determined that CFT training was needed for financial supervisors. Most of these shortcomings have been addressed by the PFSA.

71. Nonetheless, the number of AML/CFT inspectors within the Control Unit of the GIFI and the PFSA does not appear to be adequate. This has implications for the effectiveness of the on-site inspection mechanism and on the entire AML/CFT supervisory structure as a whole. No information was provided by the NSCCU with respect to structure, staffing and funding of this entity. This was also the case with the NBP which only provided information on the number of on-site inspectors. In addition, neither the NSCCU nor the NBP provided information on the provisions ensuring professional standards and integrity of its officers.

72. The statistics kept by the Polish authorities are quite comprehensive and contain almost all the necessary data for an accurate analysis of effectiveness. However, no information on the predicate offence is contained in the statistics on ML investigations, prosecutions and convictions. The situation of the statistics maintained by the supervisors has improved since the 3rd MER. The GIFI and supervisory authorities maintain accurate statistical information on the type and number of sanctions imposed on financial and other institutions.

III. MUTUAL EVALUATION REPORT

1. GENERAL

1.1 General Information on Poland

1. This section provides a factual update of the information previously detailed in the third round mutual evaluation report on Poland covering: the general information on the country, its membership of international organisations and key bilateral relations aspects, economy, system of government, legal system and hierarchy of norms, transparency, good governance, ethics and measures against corruption[4].

2. The Republic of Poland – *Rzeczpospolita Polska* – is a parliamentary democratic republic. It is situated in the geographical centre of Europe and borders on Russia's Kaliningrad enclave, Lithuania, Belarus, Ukraine, Slovakia, Czech Republic and Germany. Its area is 312,677 sq. km (120,725 sq. miles) and population is estimated as of 38,2 million people[5]. Poland joined OECD in 1996, NATO in 1999 and has been the European Union's member since 1 May 2004.

3. The reader should also refer for further details to the section of the third round mutual evaluation report (paragraphs 46-53).

Economy

4. The Economy of Poland is a high income economy[6] and is the sixth largest in the EU and one of the fastest growing economies in Europe, with a yearly growth rate of over 3.0% before the late-2000s recession. Having a strong domestic market, low private debt, flexible currency, and not being dependent on a single export sector, Poland is the only member country of the European Union to have avoided a decline in GDP, meaning that in 2009 Poland has created the most GDP growth in the EU. As of December 2009 the Polish economy had not entered recession nor contracted.

5. Poland has steadfastly pursued a policy of liberalising the economy. In 2009 Poland had the highest GDP growth in the EU. As of February 2012, the Polish economy has not entered a recession in the wake of the global financial crisis.

6. The privatization of small and medium state-owned companies and a liberal law on establishing new firms have allowed the development of an aggressive private sector. As a consequence, consumer rights organizations have also appeared. Restructuring and privatisation of "sensitive sectors" such as coal, steel, rail transport and energy has been continuing since 1990.

7. The Polish economy is currently undergoing economic development. The most notable task on the horizon is the preparation of the economy to allow Poland to meet the strict economic criteria for entry into the Eurozone. Some businesses already accept the euro as payment. In addition, the ability to establish and conduct business easily has been cause for economic hardship and the World Economic Forum recently ranked Poland near the bottom of OECD countries in terms of the clarity, efficiency and neutrality of its legal framework for firm to settle disputes.

8. Since the United Kingdom, Ireland and some other European countries opened their job markets for Poles, many workers, especially from rural regions, have left the country to seek a better wages abroad. However, Poland has experienced a rapid growth in salaries, a booming economy, the strong

[4] The reader is referred to the information set out under this section in the Third round detailed assessment report on Poland (MONEYVAL(2006)24), which was based on the legislation and other relevant materials supplied by Poland and information gathered by the evaluation team during its on-site visit to Poland from 14-21 May 2006. The report was adopted by MONEYVAL at its 23rd Plenary meeting (5-7 June 2007).
[5] Source: Demographic yearbook of Poland, 2011, by Polish Central Statistical Office.
[6] **http://data.worldbank.org/about/country-classifications/country-and-lending-groups#High_income**

value of Polish currency and rapidly decreasing unemployment (from 14.2% in May 2006 to 12.4% in 2011).

9. According to the Central Statistical Office of Poland, in 2011 the Polish economic growth rate was 4.3%, which was one of the best results in Europe.

Table 1: Economic indicators[7]:

	2007	2008	2009	2010	2011
GDP at market prices (millions of EURO)	311,001.7	363,153.7	310,418.2	354,310.0	395,682.0
GDP year growth in %	6.8	5.1	1.6	3.9	4.3%
GDP per capita €	8,200	9,500	8,100	9,300	10,392.70
Inflation rate	2.6	4.2	2.7	3.9	4.2%[8]

10. As of 28 February 2012 the average exchange rate of EUR and USD to PLN are as follows (according to the National Bank of Poland:

1 EUR = 4.1630 PLN with average yearly rate for 2011 of 1 EUR = 4.1198 PLN

1 USD = 3.0977 PLN with average yearly rate for 2011 of 1 USD = 2.9634 PLN

System of Government

11.The politics of Poland take place in the framework of a parliamentary representative democratic republic, whereby the Prime Minister is the head of government of a multi-party system and the President is the head of state.

12.The Polish public administrative system is based on the division into central and regional (self-government) administration. According to a cardinal principle included in the Constitution, local authorities are elected by citizens. The structure of the Polish local self-government consists of: 2478 communes, 379 counties and 16 voivodships (a Polish geographical unit of administration).

13.Executive power is exercised by the Council of Ministers. Legislative power is vested in both the government and the two chambers of parliament (known together by the very same name as the lower house "Sejm"), the Sejm and the Senate. The Judiciary is independent of the executive and the legislature.

14.Executive power is exercised by the government, which consists of a council of ministers led by the Prime Minister. Its members are typically chosen from a majority coalition in the lower house of parliament (the Sejm), although exceptions to this rule are not uncommon. The government is

7 http://www.imf.org/external/pubs/ft/weo/2011/02/weodata/weorept.aspx?sy=2008&ey=2011&scsm=1&ssd=1&sort=country&ds=.&br=1&c=964&s=NGDPD%2CNGDPDPC%2CPPPGDP%2CPPPPC%2CLP&grp=0&a=&pr.x=59&pr.y=12

8 http://www.worldbank.org/en/country/poland

formally announced by the president, and must pass a motion of confidence in the Sejm within two weeks.

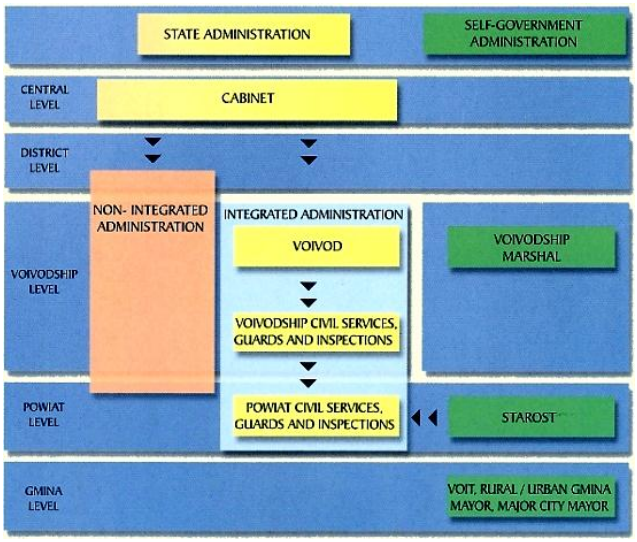
15.Legislative power is vested in both the government and the two chambers of parliament, Sejm and Senate. Members of parliament are elected by proportional representation, with the proviso that non-ethnic-minority parties must gain at least 5% of the national vote to enter the lower house. Currently four parties are represented. Parliamentary elections occur at least every four years.

16.The president, as the head of state, is the supreme commander of the Armed Forces and has the power to veto legislation passed by parliament, but otherwise has a mostly representative role. Presidential elections occur every 5 years.

17.The political system is defined in the Polish Constitution, which also guarantees a wide range of individual freedoms.

18.The judicial branch plays a minor role in politics, apart from the Constitutional Tribunal, which can annul laws that violate the freedoms guaranteed in the constitution.

Table 2: Structure of administration in Poland



19.The Constitution of the Republic of Poland, adopted in April 1997 (after a referendum) states that Poland is a unitary state (Article 3) and that local government ensures decentralization of public authority (Article 15).

Legal system and hierarchy of laws

20.The Polish Constitution provides for a distinction between universally binding law and internal law. Universally binding law is binding on all entities in the country, governs the legal situation of citizens and other entities (such as legal persons, business operators, associations, organisations etc.) and determines their rights and obligations.

21.Enactments of internal law (subject to the proviso that they are binding only within the jurisdiction of the body which issues them and within the limits of the powers laid down by law) solely concern the legal situation of entities within the organisational structure of the body issuing such enactments.

22.Chapter III of the Constitution (Articles 87-94) lists the sources of universally binding law. These are:

- the Constitution;
- statutes;

- ratified international agreements;
- regulations, and
- enactments of local law.

23. In addition to the above, Article 234 of the Constitution provides for the following universally binding law – regulations having the force of statute, issued by the President of the Republic, solely in cases tightly defined by the Constitution (e.g. during martial law or whenever the Sejm is unable to assemble for a sitting).

24. A further source of universally binding law is constituted by the legislation of international organisations if the international agreement establishing such organisations provides for the legislation established by them to have effect under domestic law (Article 91(3) of the Constitution). This Article concerns Community secondary legislation.

25. Publication of the full text of Acts, regulations and enactments of local law is subject to their being reproduced in full in one of Poland's official publications (Article 88 of the Constitution). There are currently three such publications: the Journal of Laws of the Polish Republic, the Official Gazette of the Polish Republic (Polish Monitor) and the Official Gazette of the Polish Republic (Polish Monitor B). Enactments of universally binding law are published in the Journal of Laws.

26. **The Polish Constitution** (dated 2 April 1997) is the most important source of universally binding law in Poland. The Constitution is an Act, i.e. a universally binding law. It is adopted and amended in a different way from ordinary Acts (Article 235 of the Constitution). The Constitution is regarded as a basic law in view of its particular contents, form and legal force. It governs Poland's political, social and economic system and lays down the fundamental rights and freedoms of Polish citizens. The Constitution occupies the highest position in the hierarchy of sources of law in Poland. It indicates the other sources of law, their scope and their autonomous or executive nature. All other normative acts must be compatible with the Constitution.

27. The Constitutional Court upholds compatibility with the Constitution of other normative acts and also compatibility of subordinate normative acts with higher-ranking legislation. In addition, under Article 79 of the Constitution, any person whose constitutional rights or freedoms have been violated is entitled to lodge a complaint with the Constitutional Court in respect of the compatibility with the Constitution of an Act or other normative act, further to which a court or public body has issued a definitive judgment on their constitutional rights, freedoms or obligations.

28. **International agreements** are ratified by the President of the Republic. However, where an international agreement concerns fundamental issues such as: peace, political or military arrangements, citizens' freedoms, rights and responsibilities, membership of international organisations, major financial commitments on the part of the State and matters governed by an Act or in respect of which the Constitution requires legislation, ratification is contingent on prior agreement being enshrined in that Act (Article 89 of the Constitution). After a ratified international agreement has been published in the Journal of Laws, it becomes part of the national body of law and is directly applicable, except where application requires the promulgation of an Act. In addition, an international agreement ratified with prior consent enshrined in an Act takes precedence over an Act if it is incompatible with the agreement. Legislation passed by an international organisation is also applied directly and takes precedence in the event of a conflict with Acts where this is provided for in the agreement setting up that organisation and ratified by Poland (Article 91 of the Constitution).

29. Article 91 of the Constitution defines the place of Community law in the domestic legal order. EU primary legislation in the form of international agreements forms part of the domestic legal order, is directly applicable and takes precedence over Acts. EU secondary legislation is directly applicable and takes precedence in the event of a conflict with Acts.

30. Acts are subordinate to the Constitution and to international agreements ratified with prior consent enshrined in an Act, but rank higher than regulations. An Act may be passed on any subject, but the most important issues can only be regulated by an Act (e.g. the Budget Act, legislation defining the legal status of citizens, the rules governing local government systems and their mandate). Normative acts passed by government bodies can be issued only by virtue of an authorisation enshrined in an Act with a view to its implementation. The Constitution sometimes requires the adoption of the corresponding Act, outlining the solutions it provides for.

31. **Regulations** are issued by the bodies indicated in the Constitution by virtue of a detailed authorisation enshrined in an Act with a view to its implementation. The authorisation should designate the body empowered to issue the regulation, the scope of the matters to be regulated and guidelines on the contents of the Act (Article 92 of the Constitution). The following bodies are empowered by the Constitution to issue regulations: the President, the Cabinet, the Chairman of the Cabinet, the Minister responsible for the government administration, the committee chairman appointed by the Cabinet and the National Radio and Television Broadcasting Council. The body designated to issue the regulation may not transfer that authorisation to another body. The purpose of a regulation is to implement an Act and as such, it cannot be either incompatible with the Act or go beyond the scope of the delegated powers.

32. Regulations are subject to checks by the courts. For that reason, they can be disputed by the Constitutional Court and also by a judicial or administrative tribunal. If a court rules in a specific set of proceedings that a regulation or the provisions thereof infringe higher legislation (i.e. an Act), it may refrain from applying it in the case in question and treat it as null and void.

33. **Enactments of internal law** (e.g. Orders) are internal in nature and are binding only on the organisational entities subordinate to the body issuing such enactments (Article 93 of the Constitution). Examples of enactments of internal law include cabinet ordinances and orders issued by the President and Ministers. Orders may be issued only on the basis of an Act. They cannot form the basis of a decision concerning citizens, legal persons or other entities.

34. **Enactments of local law** are issued by local government bodies (e.g. municipal resolutions) and central government administrative bodies on the basis and within the scope of authorisations laid down in an Act (e.g. provinces' implementing regulations and orders (Article 94 of the Constitution). These enactments are binding only within the jurisdiction of the bodies which issue them but, in view of their universally binding nature, they may be addressed to all entities and establish their rights and obligations.

35. **Legislative procedure** is governed by the Constitution (Articles 118-124) and the Rules of Procedure of Parliament (the Sejm) and the Senate.

36. The right to initiate legislation lies with the Cabinet, a group comprising at least 15 Members of Parliament, the Senate, the President of the Republic and a group comprising at least 100,000 citizens. Bills are submitted to the Sejm, where they are dealt with in three readings. In the course of this process the Sejm examines the bill and transmits it to the appropriate parliamentary committees for amendment. The bill is then returned to the Sejm, which votes on the amendments and the bill as a whole. The Sejm approves the bill by a simple majority, subject to at least half of the statutory number of Members being present. Once it has been passed by the Sejm, the bill is transmitted to the Senate, which has one month in which to adopt it without amendment, amend it or throw it out. If a bill is amended or thrown out by the Senate, it must be re-examined by the Sejm. In this case the Sejm needs an absolute majority, subject to at least half of the statutory number of Members being present, in order to override a recommendation by the Senate. If Parliament completes the legislative process, the bill is transmitted to the President, who should sign it within three weeks and order its publication in the Journal of Laws. Before signing a bill, the President can refer it to the Constitutional Court for constitutional review. If the Constitutional Court deems the bill to be compatible with the Constitution, the President may not refuse to sign it. The President also has the option of not referring

a bill to the Constitutional Court but returning it to the Sejm for a further reading ("presidential veto"). However, the Sejm may reject a presidential veto by a majority of 3/5, subject to at least half of the statutory number of Members being present. If the bill is once again adopted by the Sejm, the President has one week in which to sign it and order its publication.

37. **Case-law does not constitute a source of law in Poland**. Under Article 178(1) of the Constitution, judges in Poland are subordinate only to the Constitution, Acts, and international agreements ratified with prior consent enshrined in an Act. This means that the courts are duty bound to apply the Constitution, Acts and the aforementioned international agreements. The courts cannot refuse to apply these normative acts on the grounds that they are unconstitutional. However, pursuant to Article 193 of the Constitution, they may address a legal question to the Constitutional Court regarding the compatibility of a given normative act with the Constitution, ratified international agreements or Acts if the outcome of a case pending before the courts hangs on the answer to that legal question. However, judges are not bound by enactments which are subordinate to Acts, such as regulations and, when examining a given case, may determine, on an independent basis, whether such enactments are compatible with Acts and with the Constitution. Should an enactment be found to be incompatible, the court may refuse to apply it and disregard it when handing down a ruling.

38. However, case-law and, in particular, the case-law of the Supreme Court, plays a crucial role in interpretations of statute by the courts.

International cooperation

39. In relation to international participation of Poland the reader should refer to the relevant section of the previous mutual evaluation report (paragraph 52).

Transparency, good governance, ethics and measures against corruption

40. This section of the report should be read in conjunction with paragraph 53 of the third round mutual evaluation report of Poland.

41. On 17 February 2009 - The Council of Europe's Group of States against Corruption (GRECO) published its Third Round Evaluation Report on Poland. Regarding the criminalisation of corruption[9], GRECO recognised that, on the whole, Polish legislation complies with the Council of Europe's Criminal Law Convention on Corruption (ETS 173) and its Additional Protocol (ETS 191). GRECO acknowledged the legislative measures undertaken, including recent amendments relating to private sector bribery.

42. Nevertheless, GRECO called on Poland to address some deficiencies identified in the current legislation, regarding among other issues, the applicability of corruption offences to foreign arbitrators as defined by the Additional Protocol to the Convention, the jurisdiction over corruption offences committed abroad and the potential of misuse involved in the defence of 'effective regret', which occurs when an offender reports a crime after its commission.

43. Moreover, further efforts are needed to significantly reduce the occurrence of corruption in Poland, all the more so as new types of corruption have recently been identified by the authorities in areas such as sport and the private sector, where only a few cases have been investigated so far.

44. Concerning transparency of party funding[10], the existing legal and institutional framework is well-developed and largely in line with the provisions of Recommendation Rec(2003)4 of the Committee of Ministers of the Council of Europe on Common Rules against Corruption in the Funding of Political Parties and Electoral Campaigns. However, it appears that the system of political financing suffers from a lack of substantial and pro-active monitoring to go beyond the formal examination of submitted information.

[9] http://www.coe.int/t/dghl/monitoring/greco/evaluations/round3/GrecoEval3%282008%292_Poland_One_EN.pdf
[10] http://www.coe.int/t/dghl/monitoring/greco/evaluations/round3/GrecoEval3%282008%292_Poland_Two_EN.pdf

45. The report as a whole addressed 13 recommendations to Poland. GRECO assessed the implementation of these recommendations under its specific compliance procedure in December 2010[11] and December 2012[12] at its plenary meetings. [13]

46. According to Transparency International corruption perception index, Poland was ranked 41st out of 174 countries and territories around the world. This indicates that it has been a significant improvement in the perception of corruption in Poland since the previous MER when it was ranked 61st out of 163 countries.

1.2 General Situation of Money Laundering and Financing of Terrorism

Money laundering

47. The Polish authorities identified penal-fiscal crimes (carousel fraud), drug trafficking, fraud and extortion, illegal turnover of tobacco and spirits products, illegal or fictitious scrap or fuel trade, unauthorised access to bank accounts, VAT fraud in CO_2 emission trading, crimes related to financial and goods transactions within the European Union and with third countries and corruption, as being the most frequent sources of illegal proceeds, with the primary source being the carousel fraud (VAT fraud).

48. The authorities provided the table below, which presents an overview of convictions for the reference period 2007-2011:

Table 3: Recorded Criminal Offences[14]

	2007	2008	2009	2010	2011
CRIMINAL OFFENCES AGAINST PROPERTY					
Theft	241,104	214,414	211,691	220,455	230,247
Burglary	141,606	124,066	135,383	140,085	135,611
Fraud	34,775	33,028	27,945	32,084	36,179
Robbery	27,637	26,159	26,458	27,218	26,231
Theft of vehicles	21,284	17,669	17,271	16,539	16,575
Concealment					
Other CO against property	155,007	161,757	172,513	171,083	90,885
CRIMINAL OFFENCES of					

[11] http://www.coe.int/t/dghl/monitoring/greco/evaluations/round3/GrecoRC3%282010%297_Poland_EN.pdf
[12] http://www.coe.int/t/dghl/monitoring/greco/evaluations/round3/GrecoRC3%282012%2919_Second%20Poland_EN.pdf
[13] It should be mentioned that GRECO on 1 January 2012 launched the Fourth Evaluation round of Poland. The on-site visit to Poland was conducted by the GRECO evaluation team on 16-20 April 2012. The Fourth Round MER of Poland was discussed and adopted by the GRECO plenary on 19 October 2012 and published it on 25 January 2013 on GRECO's website. This GRECO's report was not considered since it was adopted after the on-site visit.
[14] Annual police reports

ECONOMIC NATURE					
Business fraud					
Fraud	38,618	40,488	49,137	54,524	55,501
Issuing of an uncovered cheque,	2	2	2	0	0
misuse of a credit card	9,551	10,182	10,061	9,508	8,239
Tax evasion	277	387	384	373	422
Forgery	21,988	16,681	15,921	20,218	20,870
Abuse of authority or rights	2,118	1,016	941	2,631	2,545
Embezzlement	6,035	5,154	5,413	4,801	5,425
Usury	15	10	6	57	13
Abuse of Insider Information	6	1	8	5	28
Abuse of Financial Instruments Market	1	0	0	0	0
Unauthorised Use of Another's Mark or Model	1,214	1,713	1,719	3,256	1,807
Other CO of economic nature	63,283	59,671	67,673	58,968	56,805
Approximate economic loss or damage from c.o. of economic nature[15] (PLN '000,000)	1,737	1,747	1,567	2,444	1,742
OTHER CRIMINAL OFFENCES					
Production and trafficking with drugs	20,565	16,436	20,123	22,448	22,075
Illegal migration	6	2	8	9	17
Production and trafficking with arms	1,778	1,518	1,504	1,340	1,185
Falsification of money	3,405	3,538	4,033	3,563	3,279
Corruption	9,631	7,706	8,305	12,487	12,192

[15] Figures are provided in Polish currency (PLN)

Extortion	2,830	2,781	3,396	3,840	3,327
Smuggling	28	44	26	26	11
Murder,	848	759	763	680	662
Grievous bodily harm	14,848	14,274	15,101	15,695	16,447
Prohibited Crossing of State Border or Territory	144	44	82	226	48
Trafficking in Human Beings	22	60	46	36	427
Violation of Material Copyright	34,292	33,812	40,956	29,498	27,841
Kidnapping, False Imprisonment	403	327	383	350	329
Burdening and Destruction of Environment	46	36	30	29	23
Unlawful Acquisition or Use of Radioactive or Other Dangerous Substances	64	81	70	53	36
Pollution of Drinking Water					
Tainting of Foodstuffs or Fodder					
TOTAL	1,152,993	1,082,057	1,129,577	1,138,523	1,159,554

49. As the statistics show the majority of recorded criminal offences against property consist of theft, burglary, fraud. Under the criminal offences of economic nature the majority of recorded crimes are fraud, forgery, misuse of credit cards, tax crimes. Other criminal offences are illicit trafficking in narcotic drugs and psychotropic substances, corruption, violation of material copyrights.

50. The provided statistics on ML cases by the Polish authorities show that from 2007 to 2011 there were 121 convictions for ML. In addition to this information the Polish authorities submitted a list of predicate offences relevant for the years of 2008 – 2010. However no information was provided on the number of underlying predicate offences for 2009 – 2012 and in this respect it was impossible for the evaluation team to determine what the typical predicate offences are for ML.

Main offences that generate proceeds

Penal-fiscal crimes

51. In the years 2007 – 2011 the GIFI carried out numerous analytical proceedings concerning money laundering from penal-fiscal crimes in particular, so called carousel transactions used for obtaining undue benefits from tax settlements (including those regarding transactions related to illegal or fictitious trade in fuels and scrap metal). From the GIFI's experience carousel transactions involve entities from several, or even a dozen or so countries.

Laundering of money deriving from trafficking in narcotic drugs and trading in pharmaceutics

52. With regard to this field of money laundering, in 2007-2011 the GIFI initiated several analytical cases based on a suspicion of money laundering connected with the trade in drugs. It was noted that each case featured a broad base of involved entities, the use of the banking sector for purposes of money laundering and persons previously convicted of criminal offences.

Money laundering and CO_2 emissions trading

53. In the years 2009-2010, a number of cases of fraud linked to VAT settlement were detected in the market of the joint CO_2 emissions trading system. The GIFI opened several cases relating to laundering of money from fraud in the area of CO_2 emissions trading.

Financial and goods transactions with foreign countries including goods turnover within the EU

54. Among the analytical proceedings initiated by the GIFI in 2010 and 2011, a large part was suspected of money laundering from crimes related to financial or goods transactions with foreign countries. According to the Polish authorities, in such cases, money was transferred to Poland, mainly from North America and Western Europe. Transfers of funds from Poland were mainly sent to Asian countries.

Scrap metal cases

55. The GIFI receives notifications about suspicious transactions regarding turnover of scrap metal and recyclable materials. Cash obtained from such illegal activity is later introduced to financial circulation. According to the Polish authorities the scale of the phenomenon is increasing, which is testified by the number of scrap metal cases initiated by the GIFI and the total value of suspicious transactions about which the GIFI notified the public prosecutor's offices. The results of the conducted analytical proceedings, regarding scrap metal and recyclable materials' circulation, indicate that a network of entities has been established for the purpose of providing funds which is completed with disbursement of cash.

Fuel cases

56. The GIFI receives notifications about suspicious transactions regarding transfer of funds related to actual or fictitious circulation of liquid fuels and components for their production. The scale of the phenomenon, in spite of the activities undertaken by relevant state authorities, is still significant.

Frauds and extortions

57. Another identified area of money laundering were transactions performed as a result of fraud and extortion. The money was legalised with the use of the targeted account technique – transfers of funds for the purpose of their immediate disbursement in cash and by means of circulation of securities. On the other hand, the depositing stage was omitted. On account of the nature of certain predicate offences, e.g. credit extortion, resulting in the fact that the funds which are the subject matter of the crime are located in cash-free financial circulation, it is difficult to distinguish transactions performed within the framework of a predicate offence from transactions related to money laundering.

Unauthorised access to bank accounts

58. Additional direction of activities was transactions related to money laundering derived from extortion of funds from bank accounts (an area excluded from the previous field encompassing other frauds and extortions). The funds extorted in this manner were most often disbursed in cash or provided to third parties via transfers (e.g. Western Union). The above transactions have been performed with the use of small amounts in order to make it more difficult for the account holder to ascertain a decrease in funds, as well as for an obligated institution to register a suspicious transaction.

Illegal turnover of spirits and tobacco

59. Another area of money laundering were transactions implemented as a result of illegal sale of technical grade spirit for food purposes without records, in the so-called "grey zone", and tax frauds related to it. Cash obtained from such illegal activity was later introduced to financial circulation.

Methods of money laundering

60. The Polish authorities consider the abovementioned offences as widely spread offences related to ML.

61. In the framework of its duties, the GIFI identified new trends and methods used by criminals, related to introduction into the financial circulation of assets from illegal or undisclosed sources. The above includes primarily methods relating to online money transfers. Attention is paid to, *inter alia*, PayPal, I-escrow, Mondex, e-charge Phone, InternetCash or Digital Precious Metals.

62. Two types of online money transfers are utilised; transfers based on established bank accounts, and transfers carried out through non-bank institutions.

63. In case of online money transfers, the following factors facilitate their use by the criminals to pursue their illegal activities: the lack of direct contact at the "customer-unit implementing the transaction" level (for example, a bank branch) facilitates opening of internet accounts, frequent anonymity of users carrying out financial operations, low value of transactions (e.g., PLN 200, 300), a significant number of financial operations carried out within a short period of time, the possibility of transferring funds of which the final recipient may be the person located virtually anywhere in the world.

64. The results of the analytical proceedings carried out by the GIFI in 2007 – 2011 were:

- forwarding 866 reports to the Public Prosecutor's Office on suspicion of money laundering committed by 1 960 entities (reports included the description of suspicious transactions whose subject were assets with a total value of PLN 10 billion);
- blockage of 945 accounts where funds with a total value of at least PLN 209,71 million were accumulated, pursuant to art. 18 and 18a of the Act; and
- forwarding to authorised bodies and units 1289 information pursuant to art. 33 (3) of the Act (i.e. on GIFI's own initiative).

Counteracting Terrorist Financing

65. The Polish authorities assess the terrorist threat level in Poland as low. However, the government devotes significant resources to counterterrorism activities to ensure the threat does not rise. Through participation in initiatives including the Proliferation Security Initiative and the Global Initiative to Combat Nuclear Terrorism, Poland remained an active participant in various international undertakings to combat terrorist threats.

66. For better coordination and cooperation of state administration in the area of counteracting terrorism the Inter-ministerial Team for Terrorist Threats was established on the basis of the Order no. 162 of the Prime Minister of 25 October 2006. This is a subsidiary body of the Cabinet which ensures cooperation of the governmental administration in the field of identifying, preventing and combating terrorism. The basic tasks of the Team include: monitoring terrorist threats; presenting opinions and conclusions for the Cabinet; elaborating projects of standards and procedures in the field of combating terrorism; initiating and coordinating actions taken by the competent authorities of the governmental administration; and organising cooperation with other countries in the area of combating terrorism. The GIFI is a member of it, as well as the Permanent Group of Experts which comprises representatives of the bodies being members of the Inter-ministerial Team for Terrorist Threats.

67. In the framework of the implementation of its statutory tasks with respect to counteracting terrorist financing in years 2007 - 2011, the GIFI initiated 60 analytical proceedings concerning suspicious transactions which could be related to terrorism financing. The proceedings were initiated on the basis of reports from obligated institutions and on GIFI`s own initiative. The basis for initiation of these proceedings were transactions carried out by persons from countries suspected of supporting terrorism or in which terrorist groups are active. In view of the specific nature of financing terrorist organisations, both legal transactions and transactions, in case of which the initial identification allowed to assume that the examined activity is the criminal activity, were checked. As a result of analysis with respect to the above-mentioned analytical proceedings in 2007 – 2011, the GIFI sent 99 reports, under art. 33 (3) of the Act on countering money laundering and terrorism financing (AML/CFT Act), to the Internal Security Agency (including the Counter –Terrorist Centre).

1.3 Overview of the Financial Sector and Designated Non-Financial Businesses and Professions (DNFBPS)

Financial Sector

68. Poland has reformed its financial supervisory system since the adoption of its 3rd round Mutual Evaluation Report, throughout a merger in its financial sector supervisory institutions. The Polish Financial Supervision Authority (PFSA) for the supervision of the securities and insurance sector was created in September 2006. The former Polish Securities and Exchange Commission (PSEC) and the Polish Insurance and Pension Funds Supervisory Commission, being the previous supervisors of the securities and insurance sectors respectively, delegated their functions to the PFSA. The General Inspectorate of Banking Supervision, supervisor of the banking sector, was incorporated into the PFSA, creating a joint supervision over the entire Polish financial market in January 2008.

69. The financial sector in Poland is mainly composed of banks, credit institutions, investment companies and custodian banks and insurance companies. It continues to be dominated by the banking sector when measured by size of activity.

Table 4: The number of entities operating in the Polish financial market

	Number of entities (March 2012)
Commercial banks	47
Cooperative banks	574
Branches of foreign institutions	21
Broker/dealers	52
Investment funds management companies	50
Life insurance companies	30
Money and currency exchange	4,415
Saving and Credit Unions	59

70. The Banking Act of 29 August 1997, which was further amended in April 2011, defines under Article 4 (1):

- **Domestic bank:** having its registered office in the territory of the Republic of Poland.
- **Credit institution:** having its registered office outside the Republic of Poland, in a country member of the European Union. It can perform in Poland, within the framework of its cross-border activity or via branch, the operations specified in Articles 5 (1) and (2) and Article 6 (1), subparagraphs 1-4 and 6-8, of the Banking Act, in the scope that derives from the authorization granted to it by the competent supervisory authority of the home Member State.
- **Foreign bank:** having its registered office in a country that is not a member of the European Union. It may pursue business in the Republic of Poland within the framework of its cross-border activity or via branch.
- **Financial institution:** is an undertaking different to a bank or a credit institution, whose main activities are related, inter alia, to equities and shares, funded loans, leasing, money transfer services, payment instruments, money market instruments, securities and brokerage services on the money market.

71. Article 2 and 4(1) of the Banking Act of 29 August 1997, which was amended in April 2011, provide the following definitions:

- **Bank:** a legal person, established pursuant to the provisions of the statute, operating on the basis of an authorisation to perform banking operations that expose to risk funds which have been entrusted to that legal person and which are in any way repayable. Depending on where it has its registered office, it can be:
  i. **a domestic bank:** having its registered office in the territory of the Republic of Poland.
  ii. **a foreign bank:** having its registered office in a country that is not a member of the European Union. This type of institution may pursue business in the Republic of Poland within the framework of its cross-border activity or via branches.
- **Credit institution:** a legal person having its registered office in a member state of the European Union which operates in Poland through the framework of its cross-border activity or via branches. Credit institutions carry out the operations specified in Articles 5 (1) and (2) and Article 6 (1), subparagraphs 1-4 and 6-8, of the Banking Act, within the scope that derives from the authorisation granted to them by the competent supervisory authority of the home Member State.
- **Financial institution:** is an undertaking other than a bank or a credit institution, whose primary activity generating most of its income consists of the following business activities:
  - acquiring and disposing of equities and shares;
  - extending internally funded loans;
  - making assets available under leasing contracts;
  - providing services relating to the acquisition and disposal of claims;
  - providing money transfer services;
  - issuing and administering payment instruments;
  - extending guarantees or sureties, or entering into other commitments not reported in the balance sheet;

- trading for its own account or that of another natural or legal person, or an organisational unit without legal personality yet having legal capacity in:
- financial forward transactions
- money market instruments
- securities
- participating in issues of securities or providing services related to such issues;
- providing asset management services;
- providing financial advice services, including investment advice;
- providing brokerage services on the money market.

72. Poland entered into the European Union in 2004 and its banking system is highly interconnected with the European financial system. Foreign-owned banks and branches (most of them branches of credit institutions based in the euro area) account for about two-thirds of the Polish banking system. BIS consolidated data shows that foreign banks' claims on Poland amounted to 59% of GDP at the end of 2011, reflecting the openness of Poland's financial system[16].

73. Net profits of the banking sector totalled 10.8 billion PLN between January and August 2012, which was an increase of 2.5% compared with the same period of 2011[17].

74. The total number of banks in Poland over the period 2009-2011 is shown in the table below.

Table 5: Ownership structure of commercial banks

Ownership structure of commercial banks			
	Dec 09	**Dec 10**	**Dec 11**
Foreign ownership more than 50%	31	39	38
Foreign ownership less than 50%	17	9	8
Resident Shareholders 100%	1	1	1
Foreign Branches	18	21	21
Total number of banks	**67**	**70**	**68**

75. According to Article 21 of the AML/CFT Act, the prudential supervisory authorities for financial institutions are:

- Polish Financial Supervision Authority.
- National Bank of Poland – in relation to currency exchange operators.
- National Savings and Credit Cooperative Union.

[16] Source: International Monetary Fund - IMF Country Report No. 12/162 of July 2012.
[17] Source: European Banking Authority - Communication on the review of European banks' capital position conducted by the EBA of 3 October 2012.

Table 6: Structure and Supervision of the Financial Sector

Financial Institutions		
Type of business	**Prudential Supervisor**	**AML/CFT Supervisor**
1. Acceptance of deposits and other repayable funds from the public	PFSA	PFSA, GIFI
2. Lending	PFSA	PFSA, GIFI
3. Financial leasing		PFSA, GIFI
4. The transfer of money or value	PFSA	PFSA, GIFI
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	PFSA	PFSA, GIFI
6. Financial guarantees and commitments	PFSA	PFSA, GIFI
7. Trading in: (a) money market instruments (cheques, bills, CDs, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities (e) commodity futures trading	PFSA NBP	PFSA, GIFI, NBP
8. Participation in securities issues and the provision of financial services related to such issues	PFSA	PFSA, GIFI
9. Individual and collective portfolio management	PFSA	PFSA, GIFI
10. Safekeeping and administration of cash or liquid securities on behalf of other persons	PFSA	PFSA, GIFI
11. Otherwise investing, administering or managing funds or money on behalf of other persons	PFSA	PFSA, GIFI
12. Underwriting and placement of life insurance and other investment related insurance	PFSA	PFSA, GIFI
13. Money and currency changing	NBP	GIFI, NBP

76. It is contemplated that the PFSA will start supervising the Cooperative and Savings Unions[18] but the judgement of the Polish Constitutional Tribunal is still pending.

77. Savings and credit unions are small financial institutions. Their scope of activities is limited both by the catalogue of financial activities that they can perform, and the fact they can only provide such services to their members. As quoted in paragraph 78 the overall assets of these institutions are within 1 percentile of the entire banking sector assets. Currently there are 59 savings and credit unions of which one has the biggest market share. Prior to introduction of core principles supervision over this sector by the PFSA, savings and credit unions were supervised for the AML/CFT purposes by an SRO, according to Article 21 section 3 point 5 of the AML/CFT Act. With the introduction of core principles prudential supervision they also fall within the framework of the AML/CFT supervision of the Polish FSA.

78. In addition, credit and savings unions provide financial services to micro and small entrepreneurs and self-employed, mostly through basic deposits, loans and payment services, as well as insurance services through a specialised subsidiary. The average size of a deposit amounts to only €1,500 (14.6 percent of GDP per capita) while that of the loan to €1,100 (11 percent of GDP per capita) per member. The smallest loans can amount to only PLN 100 (€25). As is usual for microfinance providers, loans are usually provided with co-signers. They tend to rely less on collateral than the banks (except for car loans and mortgages). The Polish authorities informed the evaluators that credit and savings unions are treated as cooperative banks, but their market is a lot smaller. Specifically, the size of this sector is approximately €3.7 billion, which is 1% of all banking sector assets.

Designated Non-Financial Businesses and Professions (DNFBPs)

79. The DNFBP sector in Poland consists of casinos, real estate agents, dealers in precious metals and stones, the legal and accountancy profession, associations, foundations and registered churches and religious communities. According to the Polish authorities, there are no trust and company service providers (TCSP) in Poland. The number of entities operating in the Polish market is as follows:

Table 7: Structure and Supervision of the DNFBPs Sector

DNFBPs		
Type of business	**Supervisor**	**Number of entities (March 2012)**
1. Casinos (including internet casinos)	Polish Customs	30
2. Real estate agents	National Court Register	19,350
3. Dealers in precious metals and stones	National Court Register	734
4. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not mean to refer to internal professionals that are employees of other	Ministry of Justice Ministry of Finance	3,643 accountants 26,050 legal advisors 10,524 barristers 2,074 Notaries

[18] Since 27 October 2012 the PFSA is responsible for the supervision over co-operative savings and credit unions and the National Association of Co-operative Savings and Credit Unions. Nonetheless the NCCSU can also supervise savings unions.

types of businesses, nor to professional working for government agencies, who may already be subject to measures that would combat money laundering.		
5. Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere		N/A
6. Associations, registered in the Central Register of Associations	Voivodship competent for the headquarters of the association	81,967
7. Foundations, registered in the Foundations Register	Ministry of Interior Ministry of Labour and Social Policy competence Ministry of Justice	8,550
8. Registered churches and religious communities	Ministry for Administration and Digitalisation	On 22 March 2012, 178 churches and other religious associations were corporate bodies and have entered into relations with the State: • 15 operating on the basis of separate acts on regulations concerning their relations with the State • 158 denominations entered to the Register.

80. According to Article 21 of the AML/CFT Act, the supervisory authorities for DNFBPs are:

- Custom Offices – in relation to operators organizing and exercising games of chance, mutual bets and operations involving automatic machine games and automatic machine games of low prizes.
- Appeal Courts – in relation to notaries public.
- Competent voivods and governors – in relation to associations.
- Tax audit authorities.

81. **Auditors:** On the 13 October 1994 the Parliament of Poland adopted the Act on auditors and their self-governing body which is wholly devoted to the auditors' self-governing body. According to the Act (the last amendments dated 14 February 2007) the National Chamber of Statutory Auditors is independent in performing its duties and acts in compliance with the provisions of the law and its statute. Membership of the National Chamber of Statutory Auditors is compulsory and becomes

effective after registration on the list of statutory auditors. There are 7,178 statutory auditors registered in Poland.

82. **Real estate agents:** Business of providing real estate services is regulated by the Real Estate Market Act [Ustawa o gospodarce nieruchomościami] - which introduced licensing of the real estate broker's and property manager's professions. The Act was adopted by Parliament in June 1997, and has been in force since 1 January 1998.

83. **Notaries, legal advisers, barristers:** The activities of notaries public are governed by the Act of 14 February 1991 on Notary, setting forth the notary public as the public confidence person and independent profession vested with specific powers. Under the statute notaries carry out some proscribed duties such as drafting deeds of certification of inheritance, making records as well as taking into custody documents, money and securities or preparing extracts, copies and abstracts of documents. There are also two types of independent legal professionals such as legal advisers and barristers, regulated by separate statutes - Act on legal advisers of July 8 1982 and the Law on the Barrister Profession dated 26 May 1982. These professions provide wide range of legal services covering numerous areas of law.

84. **Entrepreneurs:** Entrepreneurs within the meaning of the Act of 2 July 2004 on Freedom of Economic Activity (Journal of Laws of 2007 No. 155 item 1095, with further amendments), receiving payment for commodities in cash of the value equal to or exceeding the equivalent of €15,000, also when the payment for a given product is made by more than one operation are required to follow anti-money principles. Under the said Act entrepreneurs are entitled to undertake their activities after being registered in the Entrepreneur Register in the National Court Register or in the day of submitting motion to be registered in Business Activity Record; the latter applies to natural persons. The new provisions entered into force on 1 July 2011, since then there has been a Central Record and Information Office for Economic Activity, operating under the competence of the Minister of Economy.

85. **Entities providing bookkeeping services:** Bookkeeping services may be rendered pursuant to the Act of 2 July 2004 on freedom of economic activity (Journal of Laws of 2007 No. 155 item 1095, with further amendments) and they encompass comprehensive services in book-keeping, tax calculation, audit and payroll.

86. **Tax advisers:** Tax advisers provide their services on the basis of Act on Tax Consulting of 5 July 1996 (Official Journal No 102, item 475 with further amendments). It should be noted that there is mandatory membership of tax advisers in the National Chamber of Tax Advisers, which is the professional self-government body acting pursuant to the said Act.

1.4 Overview of Commercial Laws and Mechanisms Governing Legal Persons and Arrangements

87. The Act of 15 September 2000, Code of Commercial Partnerships and Companies (published in the Journal of Laws No 94, item 1037, with the subsequent amendments) (ustawa Kodeks spółek handlowych) (further referred to as: the CPCC) is a comprehensive source of commercial law and regulates the formation, structure, operation, dissolution, merging, division and transformation of commercial partnerships and companies.

88. The Act of 20 August 1997 Provisions introducing the Act on the National Court Register (published in the Journal of Laws of 1997, No. 121, item 770 with subsequent amendments), as well as the Act of 20 August 1997 on the National Court Register (published in the Journal of Laws of 2007, No. 168, item 1186, with subsequent amendments) regulates the following:

- issues connected with the registration of the entities carrying on business activity,
- organisation and operation of the National Court Register.

89. The Act of 2 July 2004 on Freedom of Economic Activity (published in the Journal of Laws of 2010, No. 220, item 1447, with subsequent amendments) regulates the following issues:

- entering of the entrepreneur to the Central Records and Information on Economic Activity (further referred to as: CEIDG) (Chapter 3); data revealed in CEIDG is publicly available and is presumed to be true pursuant to **Article 33** of the Act on Freedom of Economic Activity;
- inspection of entrepreneurs' economic activity (Chapter 5), except for inspection of banks and other institutions operating in financial market (in this respect the provisions of the Act of 21 July 2006 on Financial Market Supervision apply),
- creation in the territory of Poland of branches and agencies of foreign entrepreneurs (Chapter 6).

90. Pursuant to **Article 4** of Act on Freedom of Economic Activity the term "entrepreneur" applies to natural persons, legal persons and organizational entities which are not legal persons and are endowed with legal capacity by force of a separate Act – carrying on economic activity in their own name. Partners in a civil partnership are considered to be entrepreneurs to the extent of an economic activity conducted by them. This Act is horizontal in terms of establishing rules for inspection of the economic activity of the entrepreneurs being natural persons (including partners to civil partnerships).

91. Each entrepreneur registered in CEIDG or in National Court Register (Register of Entrepreneurs) must place Tax Identification Number - TIN (pl. NIP) on each written statements or declarations as well as use this number in legal and business transactions. For the purposes of the registries, the entrepreneur is identified by TIN.

92. Moreover, general issues connected with activities of the companies operating in the financial market, are regulated by the following acts:

- Act of 29 July 2005 on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies (Consolidated text: Journal of Laws of 2009, No. 185, item 1439).
- The Banking Act,
- The abovementioned Act of 29 July of 2005, on trading in financial instruments
- the Payment Service Act of 19 August 2011, which entered into force on the 24th of October 2011.

93. Rules for maintaining and keeping accountancy records are established in the Accounting Act of 29 September 1994 (Journal of Laws of 2009, No. 152, item 1223 with the subsequent amendments).

94. A new database called the new Central Registry and Information on Economic Activity (CEIDG)[19] was created in 2011. The database is available from the website of the Ministry of Economic Affairs, in Polish and in English. It contains information on entrepreneurs conducting business activity as well as civil partnerships. It is accessible free of charge. All the activities that are necessary to be registered in the database are also free of charge. You may search records by the following categories:

a. NIP [Taxpayer's Identification Number] number
b. Civil partnership's NIP [Taxpayer's Identification Number] number
c. KRS [National Court Register] number
d. REGON [National Official Business Register] number

[19] https://prod.ceidg.gov.pl/CEIDG/ceidg.public.ui/Search.aspx

e. Civil partnership's REGON [National Official Business Register] number
f. First name
g. Last name
h. City
i. Voivodeship
j. Street
k. Building number
l. Door number
m. Date of economic activity commencement
n. Type of activity (PKD code)

95. The rules of functioning of the database are provided by the Act on conducting business activity, (Chapter 3). Forwarding data to the database is possible either via electronic platform of public administration services, or via electronic application forms that are published at CEIDG website or in Public Information Bulletin of the Minister competent for economic affairs. Data may also be forwarded via the local authorities that collect them and forwarded onward to the database.

96. There is also the REGON[20] database in Poland maintained by the Central Statistical Office which provides information on business activity conducted in Poland. One may search records by NIP or REGON number. It contains records on every legal form of company that is provided for by the Polish legal system.

1.5 Overview of Strategy to Prevent Money Laundering and Terrorist Financing

a. AML/CFT Strategies and Priorities

97. The fight against money laundering and terrorist financing is one of the Polish strategic priorities. It was reflected by the *National Security Strategy of the Republic of Poland* adopted in 2007.

> *"The state will oversee the stability and security of the domestic money market and the proper functioning of the banking system. Efforts will be made to enhance the monitoring of financial transactions and operational and investigative cooperation with Internal Security Agency, the Central Anti-Corruption Bureau, the Police, State Border, as well as – in the international dimension – with financial intelligence units of other countries, aimed primarily at preventing introduction into financial turnover of pecuniary values originating from illegal or undisclosed sources and counteracting financing terrorism. It is very important that we cooperate with those organisations which have as their goal counteracting money laundering*."

98. The strategy of combating money laundering and terrorism financing adopted after the third round of the mutual evaluation by the Polish authorities involved actions in numerous key areas.

99. The Polish authorities:

a. adopted measures to create and implement legal provisions in area of combating money laundering and terrorism financing,
b. facilitated the implementation of international AML/CFT standards,

[20] http://www.stat.gov.pl/regon

c. created an effective inter-institutional cooperation,
d. participated in national, regional and international AML/CFT initiatives,
e. they provided assistance to other countries in the area of AML/CFT.

100. The specific crimes of money laundering and terrorism financing are among the priority areas identified by the National Program for Counteracting and Combating Organised Crime for the years 2012 – 2016 and National Program for Combating Terrorism for the years 2012 -2016. The Ministry of Internal Affairs, in cooperation with other relevant governmental institutions, among others the GIFI, has prepared two draft strategic documents. The main goal of the first one is to streamline the Polish system for counteracting and combating organised crime. The document also refers to the crime of money laundering as one of main symptoms of the activity of organised crime groups. The document was prepared with significant participation of the Ministry of Finance (especially the GIFI). It has been designed on the basis of "Diagnosis of organised crime in Poland" (document prepared last year by the Ministry of Interior with broad cooperation of other governmental bodies (including active participation of the GIFI). The second document - National Program for Combating Terrorism for the years 2012 -2016 - is dedicated to all issues connected with terrorism and its determinants.

101. The Report on Security Level in Poland is an annual report prepared on the basis of information from numerous law enforcement agencies supervised by the Ministry of Interior, as well as data from other sources (incl. the GIFI and the Customs). The report describes areas of risk, among others – money laundering. It is published on the Ministry of Interior website, in Polish.

102. Cooperation is also an essential component of the Polish AML/CFT strategy. The Polish authorities work together thanks to information sharing and participation in different task forces. As a result of conducted analyses, the GIFI sends to the public prosecutor reports on justified suspicions of money laundering along with all financial information gathered in the course of analyses (including information protected by bank secrecy).

103. Apart from reports on the money laundering offence, submitted to the Public Prosecutor's Office, GIFI provides information on suspicious transactions to: fiscal control offices, the police, the Internal Security Agency (including the Counter -Terrorist Centre), Border Guards, the Central Anticorruption Bureau, tax authorities.

b. The institutional framework for combating money laundering and terrorist financing

104. The following are the main bodies and authorities involved in combating money laundering or financing of terrorism on the financial side.

The National Bank of Poland

105. The role of the National Bank of Poland (NBP) is twofold: on one hand, pursuant to Article 2 (§ 1d) of the AML/CFT Act, the NBP belongs to the category of obligated institutions (within the scope of its operations in respect of bank accounts of legal persons, numismatics sale, gold purchasing and exchange of damaged legal tender). On the other hand, the NBP also belongs to the entities cooperating with authorities competent for counteracting money laundering and terrorist financing. Hence, the NBP carries out inspections with regard to entities engaged in foreign currency exchange. Moreover, the NBP has to cooperate with the GIFI, including *inter alia* keeping the register of suspicious transactions.

Polish Financial Supervision Authority (PFSA)

106. The Polish Financial Supervision Authority (further referred to as PFSA) has been the consolidated financial regulator in Poland since 1st January 2008. The merger of three separate regulatory authorities was finalised once the PFSA started to apply the unified approach towards supervision and on-site visits in all sectors of the Polish financial market. In late 2008 a Unit in the

Enforcement Department (within PFSA) was created in order to coordinate all AML/CFT related issues in the PFSA, and also to conduct on-site visits together with other Departments of the PFSA.

107. Since September 2009 the above mentioned Unit has been given the entire responsibility to conduct on-site visits in all financial institutions in Poland. Consequently, the process of unification of the PFSA's AML/CFT supervision over financial institutions has been finalised.

Ministry of Interior

108. The Ministry of Interior is the supervisory body for the Police. In accordance with statutory obligations (Act on Police; Penal Code), the role of the police in combating money laundering and financing of terrorism is to carry out preliminary investigations and preparatory proceedings in cases related to money laundering and financing of terrorism. Moreover, the Police carry out tasks ordered by a public prosecutor. In accordance with the AML/CFT Act, the Police are obligated to inform the FIU of each initiation of preparatory proceedings in the AML/CFT field.

Ministry of Justice

109. The Ministry of Justice determines regulations providing for the internal official procedures of the prosecuting authorities and defines their internal structure.

The Public Prosecution service

110. This part of the report should be also read in conjunction with paragraphs 89-91 of the 3rd round report of Poland.

111. On 9 November 2009 the Public Prosecutor's Office Act was substantially amended. The function of Prosecutor General is no longer exercised by the Minister of Justice. For the time being, the Prosecutor General is appointed by the President for a term of six years. Candidates for the position of Prosecutor General are elected by the National Council of Judiciary and the National Council of Prosecutors. On 24 March 2010 a new Ordinance of Minister of Justice on office work of Prosecution Offices was adopted. Concerning monitoring and supervision over AML/CFT investigations and collection of statistical data, by virtue of the Ordinance of Deputy Prosecutor General of 10 June 2010, the powers previously exercised by the Organized Crime Bureau of the National Prosecutor's Office were handed over to the Department for Organized Crime and Corruption of the Prosecutor General's Office.

Ministry of Foreign Affairs

112. The Ministry of Foreign Affairs (MFA) provides general co-ordination of internal policy in relation to international sanctions (including combating terrorism). The information regarding sanctions is transmitted to the MFA by the international bodies and then distributed to other appropriate departments and institutions, in order to work out the common position of the Government.

Ministry of Finance

113. The Polish Ministry of Finance has a wide range of responsibilities related to AML/CFT issues. The Tax Department operates within the structure of the Ministry of Finance. They also co-operate with the FIU and with fiscal departments in the area of inspections. Through this co-operation, the FIU has access to the data bases of tax departments. In addition, the Ministry also gives licences, approves rules of the games in casinos, issues certificates of profession and registers gambling devices.

Customs

114. The Customs Service is part of the Ministry of Finance. It deals with all customs issues (in this field they actively co-operate with the FIU, especially by sending information concerning transfer of money across the border).

Financial Intelligence Unit (FIU)

115. The Polish FIU, named "The General Inspector of Financial Information – GIFI" is an administrative FIU, located in the Ministry of Finance. It is the main authority for combating money laundering and financing terrorism and is at the centre of the Polish system.

116. For more information in respect of the Polish FIU the reader should refer to section 2.5 of this report.

Inter-Ministerial Committee of Financial Security

117. The Inter-Ministerial Committee of Financial Security is a consultative and advisory body within the scope of application of specific restrictive measures against persons, groups and entities, acting under the auspices of the General Inspector. The Committee presents proposals concerning a list of persons, groups or entities subject to the freezing of the assets (the minister competent for financial institutions after consultation with the minister competent for foreign affairs can determine such a list, by Regulation). According to the Article 20d of the AML/CFT Act the Committee consists of the representatives of different governmental entities.

Inter-ministerial Team for Terrorist Threats

118. The Inter-ministerial Team for Terrorist Threats is a subsidiary body of the Cabinet which ensures cooperation of the governmental administration in the field of identifying, preventing and combating terrorism. The basic tasks of the Team include monitoring terrorist threats, presenting opinions and conclusions for the Cabinet, elaborating projects of standards and procedures in the field of combating terrorism, initiating and coordinating actions taken by the competent authorities of the governmental administration, organising cooperation with other countries in the area of combating terrorism, etc.

119. The body comprises:

a. Chairperson – the Minister of the Interior;

b. Deputy – the Minister competent for Financial Institutions, the Minister of National Defence, the Minister of Foreign Affairs and the Minister of Justice;

c. members:

a) Secretaries or Undersecretaries of State in the Ministry of the Interior,

b) the Secretary of the Security Services Board,

c) the Chief of National Civil Defence,

d) the Head of the Internal Security Agency,

e) the Head of the Foreign Intelligence Agency,

f) the Head of the Government Protection Bureau,

g) the Police Commander-in-Chief,

h) the Border Guard Commander-in-Chief,

i) the Chief Commandant of the State Fire Service,

j) the Chief of the General Staff of the Polish Armed Forces,

k) the Chief of the Military Intelligence Service,

l) the Chief of the Military Counterintelligence Service,

m) the Commander-in-Chief of the Polish Military Gendarmerie,

n) the General Inspector of Fiscal Control,

o) the General Inspector of Financial Information,

p) the Head of Customs Service,

r) the Director of the Government Centre for Security or a person acting as his/her Deputy.

Permanent Group of Experts (PGE)

120. A significant role in the area of monitoring terrorist threats is played by the Task Force – Permanent Group of Experts (PGE) which substantively supports the Inter-ministerial Team for Terrorist Threats. The PGE comprises experts of the management level of the services and institutions represented by members of the Inter-ministerial Team for Terrorist Threats.

121. The basic tasks of the PGE are monitoring, analysis and assessment of terrorist threats. PGE also monitors actions taken by the competent authorities of the governmental administration within the scope of using information on terrorist threats and assesses preparations of the public administration of the Republic of Poland for identifying, preventing and combating terrorism. Within the work of the PGE there are also elaborated proposals concerning improvement of the state of preparation of the public administration for preventing and combating terrorism. In 2010, PGE prepared (in cooperation with the GIFI) assumptions for adoption of the "National Programme for Counteracting Terrorist Threats in the Republic of Poland".

Counter-Terrorist Centre of Internal Security Agency

122. The Counter-Terrorist Centre (CTC) was created within the structure of the Internal Security Agency on 1 October 2008. It comprises officers of the Internal Security Agency, seconded officers, soldiers and employees of the Police, the Border Guard, the Government Protection Bureau, the Foreign Intelligence Agency, the Military Intelligence Service, the Military Counterintelligence Service and the Customs Service. They carry out tasks within competences of the institution which they represent. Furthermore, together with the Counter-Terrorist Centre other bodies which participate in the system of anti-terrorist protection of the Republic of Poland actively cooperate. Such bodies include the Government Centre for Security, the Ministry of Foreign Affairs, the State Fire Service, the General Inspector of Financial Information, the General Staff of the Polish Armed Forces, the Polish Military Gendarmerie etc. The CTC operates in a twenty-four-hour system and 7 days a week.

123. The core of the operation system of the CTC of the Internal Security Agency is the coordination of the process of exchanging information among participants of the system of anti-terrorist protection which makes it possible to implement common responding procedures in the event of the occurrence of one of the four categories of the defined threat:

a. a terrorist act outside Poland which has an influence on security of the Republic of Poland and its nationals;

b. a terrorist act in the territory of Poland which has an influence on security of the Republic of Poland and its nationals;

c. receipt of information on potential threats which can occur in the territory of Poland and outside the Republic of Poland;

d. receipt of information on money laundering or transfers of financial resources which can be evidence of financing terrorist activities.[21]

National Asset Recovery Office

124. An important tool in the fight against money laundering is the recovery of profits derived from illegal activity. To facilitate cooperation in tracing and identifying crime-related assets, the Minister of Interior, the Minister competent for Financial Institutions and the General Prosecutor signed the Declaration of Cooperation of December 18 2008. The parties undertook, within their powers, to work together in order to effectively carry out the tasks of detection and identifying illegally obtained proceeds and other property derived from criminal activity. The Parties have established proxies for the implementation of the Declaration of Cooperation.

125. On 15 September 2009, as an accomplishment of the Declaration of Cooperation, an Agreement between the Minister of Interior, Minister competent for Financial Institutions and General Prosecutor was signed. The Parties agreed to cooperate in the scope of the detection and identification of the proceeds of crime or other crime-related assets and decided to impose the tasks on the National Asset Recovery Office (ARO). The ARO was located within the Criminal Bureau of Investigation of the National Police Headquarters.

126. The ARO: a) ensures international information exchange, b) cooperates with national units, c) manages the set of best practice, d) conducts international cooperation and e) prepares proposals for legislative change.

127. An Act on information exchange with law enforcement authorities of EU Member States was passed on 16 September 2011, which came into force on 1 January 2012. According to the Act, bodies entitled to international exchange of information on proceeds from, or other property related to, crime through Polish Asset Recovery Office are:

- Police
- Internal Security Agency
- Central Anticorruption Bureau
- Customs Service
- Border Guard
- fiscal auditing bodies
- Military Police
- Minister competent for Financial Institutions
- General Inspector of Financial Information
- Fiscal Offices and Chambers
- Prosecutors.

128. The above mentioned bodies are also obligated to assist, within the scope of their competence, the Polish Asset Recovery Office in tracing and identifying crime-related assets for the purpose of exchange information with AROs from other EU Member States and other countries.

[21] http://www.antyterroryzm.gov.pl

c. The approach concerning risk

129. The AML/CFT risk assessment is taken at the EU level as well as at the national one. The representatives of the Polish authorities participate *inter alia* in the EU-FIU Platform and the Committee for Counteracting Money Laundering and Terrorism Financing (also known as Prevention Committee - CPMLTF) existing EU law concerning AML and CFT (e.g. the Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorism financing) is discussed and revised. Moreover, there is a forum for a discussion on the creation of the European Terrorist Financing Tracking System, as well the some issues of supervision over the reporting entities and risk areas (e.g. CO_2 emission trading and its misuse for ML) which require more attention on the part of the member states.

130. Apart from the above mentioned activity Poland conducts its own AML/CFT risk assessment resulting in some changes of the legal base. For instance, in 2011 Poland has implemented the rules concerning payment services and their providers in the domain of their supervision, as well as AML/CFT duties. Furthermore, in the same year, in connection with the possibilities of existing omnibus accounts for registering securities –the law on trading of financial instruments and the AML/CFT were amended, inter alia within the scope of entitlement of the GIFI to obtain of the information on the owners of securities gathered on such accounts, as well as to blocking such accounts (also partially – blocking of only these asset values which are used to commit the crime) in case of suspicion of ML or FT.

d. Progress since the last mutual evaluation

131. Several positive changes have taken place in the Polish AML/CFT system since the adoption of the third round MER. The AML/CFT Act was radically amended in 2009, transposing the EU legislation under Directive 2005/60/EC (3AML Directive) and Directive 2006/70/EC (Implementation Directive) and the recommendations and measures recommended in the third round MER. The new Act amending the Act on counteracting the introduction to the financial circulation of financial assets originating from illegal or undisclosed sources and counteracting terrorism financing and amending other Acts, referred further to as "the AML/CFT Act" broadened the scope of the AML/CFT regime in Poland and continued to implement MONEYVAL recommendations. The Act was adopted on 25 June, 2009 and entered into force on 22 October, 2009.

132. The result of the above mentioned amendment was *inter alia* implementation of new rules concerning:

- **customer due diligence**, i.e. identification and verification clients and beneficial owners as well as monitoring of current economic relationships with a customers.
- **the risk-based approach** has been adopted. The law introduced, *inter alia,* provisions related to enhanced and simplified customer due diligence measures, provisions for exemptions from certain CDD measures where financial activity is conducted on an occasional or very limited basis.

133. Furthermore, the amended AML/CFT Act now includes new or improved prescriptions on:

- feedback to obligated institutions and cooperative units on usage of their reports on suspicious transactions and activities,
- cooperation with cooperative units (i.e. other administrative bodies),
- pecuniary penalties imposed on obligated institutions for breach of the AML/CFT obligations.

134. Article 21 §3a thereof stipulates, that relating to the violations, identified by the control the GIFI impose penalties. Moreover, the amendment of the AML/CFT Act extended the scope of

violations subjected to penal sanctions. Changes mentioned above increased the effectiveness of the system by better execution of AML/CFT requirements and control over obligated institutions.

135. It should be noted that in view of the amendment to Article 14 (2) of the Act, the Prosecution Office, the Internal Security Agency, the Central Anti-Corruption Bureau and the units subordinated to the minister competent for internal affairs and supervised by him, immediately inform the GIFI, within the limits of its statutory authority, on all the cases involving receipt of information indicating suspicion of crimes having been committed as referred to in Article 165a (TF offence) and Article 299 (ML offence) of the Penal Code.

136. Moreover the rules of reporting transactions under suspicion of money laundering and terrorist financing, as well as internal procedure related to the account blockade and transaction suspension, were modified.

137. At the same time, the GIFI undertook legislative measures aiming at preparation of regulations, the issue of which was provided for in the provisions of amended AML/CFT Act. On 20 October 2009 the *Ordinance of the Minister competent for Financial Institutions on list of equivalent countries* (Dz. U. No. 176, item 1364.) was issued.

138. The amendment of the AML/CFT Act has introduced several significant legal changes. One crucial amendment to Polish law, as far as the FATF Special Recommendation II is concerned, is adding a new regulation to the Penal Code– Article 165a, which provides for an autonomous offence of financing of terrorism.

139. Definition and penalisation of financing of terrorism also fulfils the obligations of the Republic of Poland following from recommendations of the Counter-terrorism Committee of the UN Security Council and the 1999 International Convention for the Suppression of the Financing of Terrorism.

140. As far as FATF Special Recommendation III is concerned, the changes in the Polish law contain regulations on freezing and confiscation of properties belonging to terrorists and persons financing the terrorist acts. These are amendments to the Penal Code, fiscal code and penal proceedings code, referring to forfeiture of property.

141. This has introduced a requirement that any obligated institution shall perform freezing of the asset values with due diligence, with the exception of movable and immovable property, on the basis of the European Union legislation imposing specific restrictive measures directed against certain persons, groups or entities, and regulations issued pursuant to Article 20d paragraph 4 of AML/CFT Act.

142. The AML/CFT Act determines also the manner of:

- introducing and removing subjects from the list created according to the regulation: and
- releasing assets from freezing.

143. The GIFI also worked on amendments to the regulation in order to comply with statutory delegation contained in Article 13 of the AML/CFT Act and thereby to determine the model of the transaction register, the manner of keeping it and of providing data to the GIFI by obligated institutions, as well as the manner of providing other data referred to in the Act.[22]

144. On 1 May 2008, in Poland the Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism prepared in Warsaw on 16 May 2005 became binding.

145. Poland ratified the Convention upon approval expressed in the Act of October 27, 2006 on ratification of the Convention of the Council of Europe on Laundering, Search, Seizure and

[22] These works are still in progress at the time of the on-site visit.

Confiscation of the Proceeds from Crime and on the Financing of Terrorism prepared in Warsaw on May 16, 2005 (Dz.U. No. 237 item 1712).

146. It should be noted that the Gambling Law of 19 November 2009 (Journal of Laws No. 201, item 1540, with further amendments) entered into force on 1 January 2010. The Law sets forth the conditions of establishment and the principles of conducting activity within the field of games of chance, betting and gaming machines.

147. The new Act of 26 May 2011 on the amendment of the Gambling Law and some other Acts completes the Gambling Law in force with provisions regulating to technical aspects of the functioning of the gambling market in Poland. The provisions encompassed by the amendment were notified to the European Commission in compliance with the Directive 98/34/EC of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.

148. It should also be noted that Act on Payment Services (OJL No 199, item 1175) entered into force of 22 August 2011. This act set forth at the national level a legal framework ensuring the coordination of national provisions on prudential requirements, the access of new payment service providers to the market, information requirements and the respective rights and obligations of payment services users and providers in line with Payment Service Directive. To this end the AML/CFT Act was amended accordingly. Consequently, payment institutions, branches of EU payment institutions, agencies of payment institutions and their agents within the meaning of the said Act are covered by AML/CFT regime.

149. Moreover, due to inserting into the national legal system omnibus account (by the Act of 29 July 2005 on trading in financial instruments), there were also relevant modifications in the AML/CFT Act with regard either to definition of accounts or blocking account measures, were implemented in 2011. In case of the omnibus account the blockage therefore might apply to certain asset values collected on the account.

2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalisation of Money Laundering (R.1)

2.1.1 Description and analysis

Recommendation 1 (rated LC in the 3rd round report)

Summary of 2007 factors underlying the rating

150. In the previous round of evaluation of Poland Recommendation 1 was rated 'Largely Compliant' based on the following deficiencies:

- Some of the legislative provisions needed further clarification on the physical aspects of money laundering (conversion, acquisition, possession or use).
- Not all essential criteria were provided for in Polish Law, e.g. financing of terrorism as a predicate offence; conspiracy as an ancillary offence.
- Lack of clarity as to what constitutes proceeds.
- More emphasis should be put on third party laundering and clarifying the evidence required to establish the underlying predicate criminality in autonomous prosecutions.

Legal Framework

151. Poland has criminalised ML through Article 299 of the Penal Code.

152. The ancillary offences are incorporated in the general part of the Penal Code (Chapter II, Forms of Commission of an Offence) which applies to all the offences in the specific part of the Code (including ML offence) and also to the offences prescribed in other pieces of law.

153. The Polish authorities have provided the evaluators with draft amendments to the Penal Code, especially related to Article 299, which aim to implement the MONEYVAL's recommendation regarding the criminalisation of ML but which has not yet been submitted to the Parliament.

Criminalisation of money laundering (c.1.1 – Physical and material elements of the offence)

154. Both the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) and the 2000 United Nations Convention against Transnational Organized Crime (the Palermo Convention) have been signed and ratified by Poland. Money laundering has been criminalized under Article 299 of the Penal Code, which reads as follows:

> *"§ 1. A person who accepts, transfers or takes abroad the instruments of payment, financial instruments, securities or other foreign exchange, property rights, movable or immovable property, originated from the benefits related to the committed crime, helps to transfer their ownership or possession or undertakes other activities that may foil or substantially obstruct the ascertainment of their criminal origin, the place they have been stored, their detection, seizure or forfeiture decision, shall be subject to imprisonment from 6 months to 8 years.*
>
> *§ 2. An employee or a person acting on behalf of a bank, financial institution or other entity legally obligated to record the transactions and persons carrying out the transactions who accepts, against legal regulations, instruments of payment, financial instruments, securities, money or other foreign exchange in cash, executes their transfer or conversion or accepts them in the circumstances implying justified suspicion that they have originated from the crime referred to in § 1, or who renders other services aimed to conceal their criminal origin*

or services rendered in order to prevent them from being seized, shall be subject to penalty referred to in § 1.

§ 3. repealed

§ 4. repealed

§ 5. If the perpetrator, acting in conspiracy with other persons, commits an illegal act specified in§ 1 or 2, he shall be subject to imprisonment from 1 to 10 years.

§ 6. A perpetrator who acquires a property-related benefit of considerable value while committing the crime specified in § 1 or 2 above shall be subject to punishment referred to in § 5.

§ 7. In case of sentencing a person for the crime specified in § 1 or 2, the court decrees a forfeiture of implements derived directly or indirectly from the crime and a forfeiture of the benefits gained as a result of the crime or their equivalent, even if they do not belong to the perpetrator himself. Forfeiture shall not be decreed in part or in whole in case a given implement, benefit or its equivalent shall be returned to the wronged person or other entity.

§ 8. A person who voluntarily disclosed the information relating to the persons committing the crime and the circumstances of the crime to an authority appointed for penal prosecution shall not be subject to a punishment defined in § 1-4, provided that the disclosure prevented the commitment of another crime; the court shall apply an extraordinary mitigation of punishment if the perpetrator has undertaken attempts aiming at disclosing the information and circumstances of the crime. "

155. Since the 3rd round evaluation § 3 and § 4 of Article 299 have been repealed. Also a maximum fine which can be imposed besides deprivation of liberty has been raised up to €1,500,000 (previously €1,000,000).

156. The language in Article 299 of the Penal Code to date does not clearly replicate the language of the Conventions and does not cover conversion or transfer for the purposes of concealing/disguising the proceeds' illicit origin. Also not covered is the conversion or transfer of such property for the purpose of helping any person involved in the commission of a criminal offence. It is less clear whether concealment or disguise of the true nature, source, location disposition, etc. would be covered. Acquisition, possession or uses, which the 2006 evaluators found were missing elements, are still uncovered.

157. The absence of the concealment element in the current definition of money laundering raises special concern, as the concept of concealment is not strange to the criminal Polish jurisprudence and exists in Article 300 of the Penal Code which criminalises the concealing of assets from creditors in bankruptcy proceedings. This raises special concern as to possible claims with regard to the limited scope of the currently drafted crime of ML.

158. Although, the Polish authorities believe that the wording of Article 299 § 1 *"…undertakes other actions"* covers any other possible actions including "concealment, disguise, acquisition, possession and use", these actions are qualified in the sense that such actions *"…may obstruct or considerably hinder the assertion of criminal origin or place of depositing or detection or seizure or adjudication of the forfeiture".* Therefore, this particular provision does not cover the requisite physical elements, especially in the light of the fact that Article 6 (1) of the Palermo Convention does not restrict the *actus rea* by any supplementary conditions for the money laundering offence

159. As stated above, under the legal framework the draft amendments to the Penal Code, including some amendments attempting to address previous remarks by MONEYVAL, have not been submitted to the Parliament. The explanation given by the Polish authorities is their reluctance to frequently amend the Penal Code. This reasoning can perhaps be understood but not be accepted to justify shortcomings of the Penal Code with regard to the FATF standards. Especially since other

amendments to the Penal Code where in fact adopted by the Parliament in recent years. The reading of drafted Article 299 § 1 of the Penal Code provides as follows:

> "*A person who acquires, accepts, possesses, transfers or takes abroad the instruments of payment, securities or other foreign exchange, property rights, movable or immovable property, originated from the benefits related to the committed crime, helps to transfer their ownership or undertakes its conversion or other activities that foil or substantially obstruct the ascertainment of their criminal origin, the place they have been stored, their detection, seizure or forfeiture decision, shall be subject to imprisonment from 6 months to 8 years."*

The laundered property (c.1.2) & proving property is the proceeds of crime (c.1.2.1)

160. The language of Article 299 of the Penal Code seemed to limit the scope of the types of property which the ML offence is extended to "…instruments of payment, financial instruments, securities or other foreign exchange, property rights, movable or immovable property" does not seem to include the full range of rights to property which is obligatory in nature as '*in rem*'. The Palermo Convention Article 2 (d) and the Vienna Convention article 1 (q) both define property as: "assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets".

161. The Polish authorities informed the evaluators that Article 115 (9) of the Penal Code should be taken into consideration to fully understand the scope of types of property covered by Article 299.

§ 9. A movable item or chattel is also Polish or foreign currency or other means of payment and a document which entitles to obtain a sum of money or includes the obligation to pay principal, or interest, share in the profits or a declaration of participation in a company [or partnership].

162. According to the Palermo Convention, Article 2(d) "property" shall mean "*assets of every kind, weather corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets*".

163. The evaluators concerns were related to the scope of the subject matter of the money laundering offence as it is defined by Article 299 paragraph 1, particularly whether "property rights, movable or immovable properties" cover every kind of incorporeal or intangible asset.

164. The Polish authorities have explained that the definition of movable property has not been encoded in any legal act and exists only in jurisprudence. According to that definition, within the category of movable property fall all the items which have not been defined in the Civil Code as real estate (negative definition of movable property). In this understanding "movable and immovable properties" is an exhaustive formulation which encompasses every kind of assets.

165. This explanation is not fully embraced by the evaluators as long as in the Polish legislation can be found provisions which refer to "movable and immovable property" not as to an exhaustive concept (e.g. *Article 20d of the AML/CFT Law 1. Any obligated institution shall perform freezing of the asset values with due diligence, with the exception of movable and immovable property….*). If it is an exhaustive concept how could be a subcategory of "asset values"?

166. In addition, the Polish authorities provided some supplementary explanation, in particular:

- Article 44 of the Polish Civil Code provides the definition of "property" as follows: "*Property is ownership and other property rights".*
- The civil law classification of the rights in the Polish legal system mirrors the classification accepted by other European countries following the tradition of the Roman Law.
- To clear up that issue, it must be stated that the term "property" in the Polish Civil Code covers both *iura in rem* (represented by "ownership") which are effective universally *(erga omnes)* and *iura in personam* (represented by "property rights")

e.g. debts, rights to claim etc., effective only between parties of an obligation originated by a contract or a tort.

- Consequently, the concept of "property rights" encompasses both incorporeal and intangible asset which have any economic value.

167. Following the additional explanation provided by the Polish authorities, the evaluation team agreed that the definition of property covers both *jus in rem* and *jus in personam.*

168. As defined by the Palermo and Vienna Conventions, proceeds of crime shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence. According to Article 299 §1 of the Penal Code of Poland the subject matter of the ML offence shall be "*derived from the benefits relating to the commission of a prohibited act*". This approach appears not to cover property directly obtained through the commission of an offence.

169. The Polish authorities consider that it is clear both for practitioners and jurisprudence that property directly or indirectly obtained represents proceeds of crime and is subject to money laundering. The authorities have added that in one of the latest rulings of the Supreme Court of Poland, passed on 2nd February 2011 (Ref. no II KK 159/10), the same position was taken. The court stated that "for committing the offence set forth in Article 299 § 1 PC it is necessary that the objects listed in that provision originate from the benefits related to a committed crime. Therefore, it is essential to establish a committed crime and also benefits derived directly or indirectly from the crime by a perpetrator or other person (…)".

170. Another judgement of the Supreme Court of 4 October 2011 (III KK 28/11) stated *"Pursuant to Article 299 § 1 of the penal code the subject matter of acts specified in this Article may be exclusively legal tenders, financial instruments, securities, foreign currency values, property rights or other real or movable property* ***obtained from profits of a prohibited act committed****".* The evaluators observed that this judgement is referring also to object "originated from the benefits related to a committed crime", but in a slightly different wording.

171. With respect to this possible interpretation of the text of Article 299 the Polish authorities admitted in one of their remarks that the issue of directly obtained proceeds, as a subject matter of ML offence, raised concerns among some judges and prosecutors before the ruling of the Supreme Court of Poland of 2 February 2011 passed.

172. In conclusion, the evaluation team believes that the wording of Article 299 para.1 of the Penal Code may still raise doubts related with the scope of the offence in respect of the subject matter of the penalised acts. According to the English version provided by the Polish authorities, the subject matter of money laundering is the property that has "*derived from the benefits related to the committed crime*". This could be understood that the property derived from the committed crime (directly obtained) is not covered by the legal provisions. As the provision currently stands, a benefit is generated by the prohibited act, from which the property listed in Article 299 is then derived.[23]

173. Interpretation of Article 299 §1 PC and judicial practice indicate that property subject to money laundering cannot originate merely from illegal activity or undisclosed sources. Moreover, it is not sufficient to prove that property originates from an undefined offence or from some general category of offences. It was therefore essential for prosecutors and courts to precisely identify the predicate

[23] An excerpt from the guidelines on interpretation of Article 299 CC issued by the Deputy Prosecutor General of Poland (ref. no PG III PZ 404/17/12), on 18 December 2012 states the following:
"It must be reiterated that since passing the ruling of the Supreme Court of 2 February 2011 (ref. no II KK 159/10), there exists a fairly unanimous view across the judiciary that for the commission of the offence under Article 299 of the Criminal Code it is essential that the property subject to money laundering should originate from the benefits related to the committed crime, which must be understood as proceeds derived directly or indirectly from the predicate offence by a perpetrator thereof or a third party".

offence and determine its legal qualification. This somewhat high threshold was lowered in the ruling of the Supreme Court of Poland, passed on 4th October 2011 (Ref. no III KK 28/11), where the court stated that "it is not necessary that committing of an offence generating material benefits, has been established in the ruling of any judicial entity, in particular a final conviction. (…)". This explanation of the Supreme Court clearly shows that it is necessary to identify only the kind of offence, not all the factual circumstances of it. Moreover, high evidentiary standard as to a predicate offence was also lowered by the Supreme Court explanation that the legislator does not require determining by the court that an act being a source of financial gains meeting the characteristics of "dirty money" meets all the criteria of an offence. This is why in Article 299 § 1 CC the notion of "prohibited act", instead of "offence" is used, according to the Polish authorities explanation therefore there is no need to determine a specific perpetrator, his or her fault or any other additional premises conditioning penal liability.

The scope of the predicate offence (c.1.3) & Threshold approach for predicate offences (c.1.4)

174. In Poland, an "all crimes approach" has been applied, which means that categories of predicate offences have not been limited whatsoever and include all the offences generating proceeds.

175. Furthermore, the Polish criminal legislation provides for criminalisation mechanisms in relation to each of the 20 "designated categories of offences" in the Glossary annexed to the Methodology, in line with Criterion 1.3.

176. The Polish legislation covers the FATF designated categories of offences as indicated in Table 8.

Table 8: Designated categories of predicate offences

Designated categories of offences based on the FATF Methodology	**Offence in domestic legislation**
Participation in an organised criminal group and racketeering;	**Article 258 of the Penal Code**
Terrorism, including terrorist financing	**Articles134 to136, 163 to165, 166 to167, 182 of the Penal Code -Terrorism** **Article 165a of the Penal Code – Terrorist financing**
Trafficking in human beings and migrant smuggling	**Articles 189a**
Sexual exploitation, including sexual exploitation of children;	**Articles 199 to 200b**
Illicit trafficking in narcotic drugs and psychotropic substances;	**Articles 53 to 67 of the Act on counteracting Drug Addiction**
Illicit arms trafficking	**Article 263 of the Penal Code**
Illicit trafficking in stolen and other goods	**Articles 291 and 292 of the Penal Code**
Corruption and bribery	**Articles 228 to 231 of the Penal Code**

Fraud	**Article 286 and 297 to 298 of the Penal Code**
Counterfeiting currency	**Article 310 of the Penal Code**
Counterfeiting and piracy of products	**Articles 303 to 308 of the Act on intellectual property**
Environmental crime	**Article 181 to 188 of the Penal Code**
Murder, grievous bodily injury	**Articles 148, 156 of the Penal Code**
Kidnapping, illegal restraint and hostage-taking	**Articles 189, 123, 252 of the Penal Code**
Robbery or theft;	**Articles 278, 280 of the Penal Code**
Smuggling	**Article 86 of the Fiscal Penal Code**
Extortion	**Article 282 of the Penal Code**
Forgery	**Article 270 of the Penal Code**
Piracy	**Article 166**
Insider trading and market manipulation	**Articles 179 to 181 and 183 of the Act on Trading in Financial Instruments of 29 July 2005**

Extraterritorially committed predicate offences (c.1.5)

177. Current provisions of the Polish Penal Code provide for no obstacles to investigate money laundering if a predicate offence occurred in another country and would have constituted a predicate offence had it occurred domestically. For example, the evaluators were advised of a number of existing investigations concerning money laundering of proceeds generated by "phishing attacks" in Germany and Switzerland.

178. Nevertheless only one conviction relating to an extraterritorially committed predicate offence exists which causes some concern both with regard to the prioritisation and resource allocation of the Polish law enforcement authorities with regard to such cases, and as to possible lack of effectiveness in these untested jurisprudential trails.

179. The limited extraterritorial scope of the TF offence, as described with regard to SR II, may affect the effective prosecution of ML with TF as a predicate performed abroad.

Laundering one's own illicit funds (c.1.6)

180. Since the first amendment of Article 299 PC which entered into force on 23 June 2001, the offence of money laundering applies also to persons who commit the predicate offence, and in fact several, if not most of the money laundering cases are self-laundering.

Ancillary offences (c.1.7)

181. The Polish Penal Code provides for appropriate ancillary offences to the offence of money laundering, including attempt, aiding and abetting, facilitating, and counselling the commission. The ancillary offences are incorporated in the general part of the Penal Code (Chapter II - Forms of Commission of an Offence) which applies to all the offences in the specific part of the code (including money laundering) and also offences prescribed in other pieces of law.

182. The FATF standards require that countries criminalize either conspiracy or association to commit money laundering. Conspiracy as generally known in common law system is not criminalised under the Polish legislation, which is a civil-law jurisdiction. The Polish legislation criminalises "preparation" through Article 16 paragraph 1 of the Penal Code which would apparently meet the requirement of Criterion 1.7 related to "association with". The wording of this article is as follows *"Preparation only occurs when the perpetrator, in order to commit a prohibited act, undertakes activities aimed at creating the conditions for effecting an act leading directly to commission of the prohibited act, particularly when, for this purpose, he enters into an arrangement with another person, acquires or makes ready the means, gathers information or concludes a plan of action"*. The paragraph 2 of this article provides further that *"preparation is subject to a penalty only when the law so provides"*. Article 299 to date does not provide in this respect and consequently the provisions of paragraph 1 of Article 16 are not applicable.

183. As to conspiracy, section § 5 of Article 299 states it is a crime "If the perpetrator, acting in conspiracy with other persons, commits an illegal act specified in § 1 or 2". Though the term conspiracy is specifically mentioned in the statute it does not however cover conspiracy as meant in the methodology - an agreement between 2 or more persons to commit money laundering where the offence is not completed. There have been no changes on this point since the last evaluation in the legislation. The proposed amendment provides for criminalisation of the preparation to commit a money laundering crime. On the assumption that this would be covered by the notion of preparation set forth in Article 16 § 1 of the Penal Code - then the deficiency would be remedied with conspiracy being one of the forms of preparation to commit a crime.

Additional element

If an act overseas which does not constitute an offence overseas but would be a predicate offence if occurred domestically leads to an offence of ML (c.1.8)

184. According to Article 111 § 1 the liability for an act committed abroad is subject to the condition that the liability for such an act is likewise recognized as an offence, by a law in force in the place of its commission.

185. The court may take the differences between the Polish penal law and the law in force in the place of commission, into account in favour of the perpetrator , according to the Article 111 §2.

186. If offences committed abroad fall into one of the categories indicated in Article 112 (an offence against the internal or external security of the Republic of Poland, an offence against Polish offices or public officials, an offence against essential economic interests of Poland, an offence of false deposition made before a Polish office) then the Polish Penal Code is applied notwithstanding if the predicate offence is criminalized in the place of its commission.

187. If the proceeds of crime are derived from conduct of the above mentioned categories of offences and laundered in Poland, then Article 299 P.C. can be applied.

188. According to the Article 113 of the Penal Code, notwithstanding regulations in force in the place of commission of the offence, the Polish penal law shall be applied to a Polish citizen or an alien, with respect to whom no decision on extradition has been taken, in the case of the commission abroad of an offence which the Republic of Poland is obligated to prosecute under international agreements.

Recommendation 32 (money laundering investigation/prosecution data)

Table 9: Number of investigations, prosecutions and convictions for ML in 2008 – 2011

	2008	**2009**	**2010**	**2011**
ML Investigations	741	796	866	754
ML prosecutions (number of cases/ number of persons)	74/-	65/360	74/128	71/290
Convictions (number of cases/ number of persons)	27/53	18/41	21/45	19/47

Table 10: Breakdown with respect to different paragraphs of Article 299

	2009	2010	2011
Investigations (total number)	**796**	**866**	**754**
Art. 299 § 1 P.C. or Art.299 § 1 and § 5 or § 6 P.C.	796	865	751
Art. 299 § 2 P.C.	1	1	3
Prosecutions (total number)	**65**	**74**	**71**
Art. 299 § 1 P.C.	15	11	14
Art. 299 § 2 P.C.	0	1	2
Art. 299 § 1 and § 5 or § 6 P.C.	50	62	55
Convictions (total number)	**18**	**21**	**19**
Art. 299 § 1 P.C.	4	7	5
Art. 299 § 2 P.C.	0	1	1

Art. 299 § 1 and §5 or § 6 P.C.	14	13	13

Table 11: Highest and lowest sanctions imposed with respect to ML offence

	Money laundering		**Terrorist financing**	
	Highest sanction imposed	Lowest sanction imposed	Highest sanction imposed	Lowest sanction imposed
2008	Imprisonment for a term of 3 years and 6 months; forfeiture of €8,000 obtained from the commission of an offence,	Imprisonment for a term of 1 year	-	-
2009	Imprisonment for a term of 2 years; forfeiture of €494,971 obtained from the commission of an offence	Imprisonment for a term of 1 year	-	-
2010	Imprisonment for a term of 4 years; forfeiture of €62,122.59 obtained from the commission of an offence	Imprisonment for a term of 1 year	-	-
2011	Imprisonment for a term of 4 years and 6 months; a fine of €2,500; forfeiture of €62,122.59 obtained from the commission of an offence	Imprisonment for a term of 6 months	-	-

Effectiveness and efficiency

189. The Polish authorities have advised the evaluators that since 2007, monitoring of ML/TF investigations have been carried out on the basis of Ordinance of 27 July 2007 issued by the Minister of Justice and the order of 28 September 2007 issued by the Head of Organized Crime Bureau at the National Prosecutor's Office. According to this order, the Appellate Prosecutors and Heads of Local Departments of Organized Crime Bureau are obligated to submit precise and complex information on

money laundering investigations conducted by the subordinated prosecutors. This information is meant to be analysed by the Central Unit of Organised Crime Bureau of the National Prosecutor's Office, which is tasked with producing reports comprising statistical data relevant to assessment of the effectiveness of the Polish law enforcement with regard to combating money laundering. Among the data collected are: the number of the on-going and completed investigations, the number of suspects and convicts, the number of verdicts passed and types of sanctions imposed, the number of MLA requests and requests for other forms of co-operation. Since 2009, the National Prosecutor's Office was replaced by the Prosecutor General's Office and the Organized Crime Bureau by the Department for Organized Crime and Corruption.

190. There appears to be a steady and growing number of money laundering investigations (796 in 2009; 866 in 2010, 754 in 2011). The evaluation team was also pleased to see that progress has been made on the number of ML convictions. It was noted that in the last three years, convictions for money laundering were successfully obtained in 2009 (18), 2010 (21), 2011 (19), including three stand-alone money laundering prosecutions.

191. While welcoming these results, the evaluation team considers that further efforts are necessary to enhance the effectiveness of the application of the money laundering offences, particularly in respect of the evidence required to prove stand-alone money laundering offences on the basis of inferences drawn from facts and circumstances in order to establish general predicate offending and the mental element in such cases.

192. The Polish authorities have reassured the evaluators that focus has been put on autonomous prosecution of money laundering (by third parties) and has been included in training seminars both for judges and prosecutors. From the statistics provided it appears that 2 convictions were achieved for autonomous money laundering in 2009, 3 in 2010 and 3 in 2011. Money laundering therefore appears now to have been successfully prosecuted as an autonomous offence. So far there have been no indictments and/or convictions of legal persons of money laundering or any other economic crime.

193. On 9 November 2009 the Public Prosecutor's Office Act was amended, reinforcing the independence of the Prosecutor General and the highly professional Polish Prosecution Service. The tasks and powers of the newly established Department for Organized Crime and Corruption are the same as exercised previously by the Organized Crime Bureau of The National Prosecutor's Office.

194. Several law enforcement investigative units are authorised to conduct money laundering investigations, but seem to be over - focused on investigation of self - laundering and especially on tax related predicate offences. In the Polish prosecution service there are no prosecutors specialized in specific types of crime. Therefore all prosecutors in the field can be involved in AML investigations and/or prosecutions.

195. Difficulties were expressed to the evaluators by investigators and prosecutors with regard to obtaining bank information (citing bank secrecy though no actual legal impediment seems to exist) and information on beneficial ownership.

196. As conveyed to the evaluators, the predicate offences are mostly related to fiscal fraud. Most of the investigative units seem to lack both a proactive approach and the necessary training for conducting more complex AML investigations and rely totally on the prosecutors' initiative. The prosecutorial effort should be reinforced by clear and firm prosecutorial guidance on AML evidence issues in autonomous ML cases from the Prosecutor General, which encourage prosecutors to challenge the courts with more of these types of cases across the whole range of predicate offences.

197. One of the three prosecutors met by the evaluators conveyed what he described as a common opinion among some prosecutors regarding the difficulty in proving the mental element of ML. The evaluators were somewhat uneasy to hear the opinion that with a lack of confession it would be practically impossible in a Polish criminal court to prove the necessary *mens rea* for a ML conviction. It is accepted by the evaluators that in 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). Nevertheless, analysis of some recent Polish supreme court decisions on this point leave the evaluators unsure if the intentional element of the offence of ML can, in practice, be inferred from objective factual circumstances in a Polish courtroom.

198. In its Ruling of 18 January 2007 (III KK 440/06) the Supreme Court established the principle in Polish criminal law of "deductive reasoning, that is reaching real conditions to real conclusions, as logically reliable, corresponds to the principles of proper reasoning and therefore lies within the principle of free assessment of evidence". The Polish prosecutors assured the evaluators that in line with the principle of free assessment of evidence prescribed in article 7 of the Penal Procedure Code, proving *mens rea* of ML may be inferred (as all other elements of a given offence) from objective factual circumstances established in the course of a trial. Nevertheless, the actual decision in the above mentioned case was dismissing the cassation by recognising it as evidently groundless. The Polish authorities rely on this case and emphasize that any views expressed by the Supreme Court even on secondary issues, in particular construction of various provisions of Penal Code and/or Penal Procedure Code, are traditionally recognized by the practitioners as a credible interpretation of law which is consequently reflected in their own decisions.

199. In a separate Ruling of 2 December 2008 (III KK 221/08) the Supreme Court pointed out that factual findings do not have to always result from particular evidence. They may also result from irrefutable logics of the situation established on the basis of particular evidence, if this situation is such that it becomes an obvious premise on the basis of which life experience gives an explicit conclusion that the given factual circumstances occurred. This court case did not specifically address the issue of *mens rea* but again the view of the Polish authorities is that it is the position of the Supreme Court referred to any factual findings establish during the investigation and trial including *mens rea*.

200. Another reason for some concern is the perceived lack of effectiveness of the judiciary. The evaluators were advised of the protracted nature of legal proceedings which have led in many of the cases mentioned to the evaluators to prosecutors agreeing to relatively low punishment without conducting a trial, under what seems to be the civil law version of a common law plea bargain according to article 335 of the Code of Criminal Procedure Act of 6 June 1997.

201. Some of the prosecutors candidly admitted that in fact adding a money laundering offence to the indictment of a drug or tax fraud case would rarely add anything to the actual sentencing, which leads to serious concern as to the dissuasiveness of the *de-facto* penalties imposed by the courts for ML. The statistics provided by the Polish authorities demonstrate relatively short incarceration periods (6 months to 4 years) but whereas most of these cases were self - laundering, it remains unclear what segment of these verdicts can be reasonably attributed to the ML conviction.

202. One reason for this may be linked to possible confusion by the Polish judiciary and perhaps some prosecutors as to the true sense of the protected value of the ML offence which is commonly interchanged with tax evasion and other fiscal crimes, and not perceived also as an offence against the integrity of financial institutions and intermediaries, as a separate protected value.

203. In general, statistics related to ML cases maintained by the Polish authorities do not show the number of different categories of underlying predicate offences. This led the evaluation team to the conclusion that the Polish authorities consider information related to predicate offences as not important and useful. In addition, the evaluators consider that without such statistics it will be difficult for Poland to review the effectiveness of their system for combating money laundering and terrorist financing as a whole.

2.1.2 Recommendations and comments

Recommendation 1

204. Money laundering is criminalised by Article 299 of the Penal Code, based on an "all-crimes" approach. The deficiencies previously identified in the 3rd round MER of Poland regarding the lack of all aspects of the physical and material elements of the Vienna and Palermo conventions have unfortunately not yet been addressed. Additional shortcomings have been identified by the evaluators namely the definition of the TF offence and the scope of property covered by the ML offence. Additionally, association with or conspiracy to commit ML is still not covered in the legislation.

205. The Polish authorities are encouraged to amend Article 299 to ensure that conversion, concealment, disguise, acquisition, possession and use, as well all the types of property, are fully covered by legislation.

206. The examiners recommend that financing of terrorism in all its forms, as explained in the Interpretative Note to SR.II, should be clearly covered as a predicate offence to money laundering.

207. The Polish authorities should clarify (either by legislation or by binding interpretative mechanism) that the subject matter of money laundering offence covers property obtained directly through the commission of an offence.

208. Associations with or conspiracy to commit money laundering should be recognised as a criminal offence, unless this is not permitted by a fundamental principle of domestic law. The examiners have not been advised that this ancillary offence would be contrary to fundamental principles of domestic law.

209. Though the Polish authorities consider that this is possible, it may still be helpful to clarify by guidance that the predicate base of money laundering extends to conduct which occurs in another country but which is not an offence in that country, but would be an offence if it occurs in Poland (Additional Criterion 1.8).

210. Knowledge that such property is proceeds - as widely defined in the Palermo and Council of Europe Convention – is impliedly covered by Article 299, but it would be helpful if it is formally set out in the legislation. However, it is advised to set out in guidance that knowledge (the intentional element) can be inferred from objective factual circumstances. The Polish authorities may also wish to consider an alternative lower mental element, like suspicion, for Article 299 (1), with appropriately lower penalties, to cover situations where knowledge cannot clearly be proved. Equally, introducing the concept of negligent money laundering might also assist the prosecutorial effort.

211. Prosecutions for money laundering are being brought, though the absence of detailed information about the cases and their underlying predicate offences (as relevant statistical data is lacking) makes a judgment of the effectiveness of the implementation difficult.

212. It seems that the inability to define a predicate offence is a major cause for termination of money laundering proceedings. This may imply that prosecutors are requiring a high degree of specificity in respect of a particular predicate offence. Most cases appear to relate to self-laundering and the problem of proving the predicate offence is often addressed by prosecuting the money laundering and the predicate offence in the same indictment. In any event, the examiners consider that emphasis could be placed on autonomous prosecution of money laundering by third parties. To achieve this, it is necessary for the Polish authorities to address the issue of the evidence required to establish the predicate criminality in autonomous money laundering cases. It may be useful to make it clear in legislation or guidance that the underlying predicate criminality can be proved by inferences drawn from objective facts and circumstances in money laundering cases brought in respect of both domestic and foreign predicate offences, and to give more guidance generally to prosecutors on the amount of

evidence needed to establish underlying predicate offence (for example, that it may be sufficient to establish that e.g. drug trafficking has occurred, but not drug trafficking on a specific date or time, etc.).

Recommendation 32

213. More detailed statistics on money laundering investigations, prosecutions, convictions, and their predicate offences should be maintained.

2.1.3 Compliance with Recommendation 1

	Rating	Summary of factors underlying rating
R.1	**PC**	• The physical elements of money laundering offence do not fully correspond to the Vienna and Palermo Conventions; in particular conversion, concealment, disguise, acquisition, possession or use are not covered in all circumstances; • Not all essential criteria are provided for in the Polish legislation, e.g. association with or conspiracy as an ancillary offence; • Shortcomings in the definition of TF as a predicate offence; **Effectiveness** • The overall effectiveness of ML criminalisation raises concerns considering a low number of convictions for ML, given a high level of proceeds generating offences in Poland; • The perception among practitioners with regard to high evidentiary standards for some of elements of the ML offence, e.g. mental element, has a negative impact on effectiveness.

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and analysis

Special Recommendation II (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

214. In the 3rd round evaluation report, Poland was rated 'NC' for Special Recommendation II. The conclusion of the evaluation team was based on the following factors:

- The Polish authorities rely on the possibility of proceeding for aiding and abetting an offence of terrorist character as indicated in Article 115 § 20 of the Penal Code or an offence involving groups or associations set up with the purpose of committing terrorist crime. There are no cases and therefore there is no jurisprudence. Criminalising terrorist financing solely on the basis of aiding and abetting is not in line with the Methodology. The present incrimination of terrorist financing appears not wide enough to clearly sanction criminally:
    - The collection of funds with the intention that they should be used or in the knowledge that they should be used in full or in part to carry out acts referred to in Article 2 § 1 of the UN Convention for the Suppression of the Financing of Terrorism (including whether or not the funds are actually used to carry out or attempt to carry out a terrorist act);

- The provision or collection of funds for a terrorist organisation for any purpose including legitimate activities;
- The collection and provision of funds with the unlawful intention that they should be used in full or in part by an individual terrorist (for any purpose);
- All types of activity which amount to terrorist financing so as to render all of them predicate offences to money laundering.

Legal framework

215. Poland has adopted and ratified the International Convention for the Suppression of the Financing of Terrorism. This document is binding for Poland since 13 December 2004. At the time of 3rd MER financing of terrorism was criminalised on the basis of aiding and abetting an "act of terrorism". The lack of an autonomous FT was the main reason for the NC rating in the previous round of evaluation.

216. By virtue of an Act of 25 June 2009, the Penal Code was amended by means of introducing Article 165a which provides for an autonomous offence of financing of terrorism which should be read as follows:

> *"Whoever gathers, conveys or offers legal tenders, financial instruments, securities, foreign currencies, property rights or other movable or unmovable property for the purpose of financing a crime of a terrorist nature, shall be subject to the depravation of liberty for a term of between 2 to 12 years."*

217. An offence of a terrorist character is defined by Article 115 paragraph 20 of the PC as:

> *"An act prohibited under penalty of deprivation of liberty up to at least 5 years, committed with the purpose of:- serious intimidation of many people;- forcing a public body of the Republic of Poland or of another state or of a body or an international organisation to take certain steps or refrain from certain actions;- serious disturbing in a system of state or economy of the Republic of Poland, of another state or of an international organization, as well as a threat to commit such an act."*

Criminalisation of financing of terrorism (c.II.1)

218. The combination of Articles 165a and paragraph 20 of Article 115 of the PC is a welcome step forward by Poland in addressing the deficiencies identified previously by the evaluators. The Polish authorities consider that the language of the amendment covers also the collection of funds for a terrorist organization with the purpose of committing an offence of a terrorist character as defined in paragraph 20 Article 115 of the PC, which is accepted.

219. The financing of terrorism offence is said to cover provision or collection of funds in respect of the two distinct types of terrorist acts in the TF Convention: Article 2 (1) (a) TF Convention (acts constituting offences in the treaties annexed to the Convention) and Article 2 (1) (b) TF Convention offences (any other acts intended to cause death or serious injury to intimidate a population or to compel a government or international organization to do, or refrain from doing, any act). Article 2 (1) (b) TF Convention acts appear to be clearly covered by Article 115 PC. Most of the Article 2(1) (a) TF Convention offences in the Annex to the TF Convention appear to be broadly covered in the PC, though it is not entirely clear how the linkage is made between these various offences in the PC and the requirement for the TF offence to apply to offences of a terrorist character as defined in Article 115 paragraph 20.

220. On a very broad construction all TF Convention annex offences that appear in the PC might be considered as offences involving "serious disturbing in a system of the State of the Republic of Poland (or of another State)". While this may be a common sense conclusion that a court may come to, it is advised that the linkages should be more clearly made in Article 115 paragraph 20 to make direct reference also to the relevant TF Convention Annex Offences that appear in the PC.

Table 12: Conventions listed in the Annex of the FT Convention

Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970	Ratified on 21 March 1972 **Article 166**
Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation done at Montreal on 23 September 1971	Ratified on 28 January 1975 **Article 167, Articles 173 and 174**
Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973	Ratified on 14 December 1982 **Article 136, Article 148, Article 190**
International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979	Ratified on 25 May 2000 **Article 252**
Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980	Ratified on 08 September 1983 **Articles 120 and 121**
Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988	Ratified on 12 August 2004 **Article 156, Article 160, Article 288**
Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988	Ratified on 1 March 1992 **Articles 166 and 167, Article 269**
Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988	Ratified on 01 March 1992 **Article 115**
International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997	Ratified on 3 February 2004 **Articles 163-165**

221. More than this, Article 2 (1) (a) TF Convention doesn't require any specific common purpose for those acts constituting offences in the treaties annexed of the Convention. The mental element of the FT offense is described as "intention that the funds should be used or in knowledge that they are to be used, in full or in part, in order to carry out an act which constitutes an offence within the scope of as defined in one of the treaties listed in the annex". To be considered as an offence of terrorist character, according with Article 115 paragraph 20 of the Polish Penal Code, the prohibited act should be committed with one of three specific purposes. In conclusion for example if a financing of a theft or robbery of nuclear material (as it is provided by the Convention on the Physical Protection of Nuclear

Material, Vienna, 1980) is not committed with one of those three purposes, will be not possible to consider this act as an act with terrorist character and consequently will be not possible to apply the Article 165a of the Penal Code.

222. SR. II requires countries to go further than the Convention and criminalise *the "wilful provision or collection of funds intending that they be used by a terrorist organization or an individual terrorist for any purpose."*

223. As the financing of terrorism offence in Poland is limited to the financing of an offence of a terrorist character the Polish authorities advise that the provision of funding for any purpose to a terrorist organization is covered by Article 258 §2 PC, participation in an organized group of a terrorist character. This offence is set out beneath.

> *"Article 258. § 1. Whoever takes part in an organised group or a criminal organisation intending to commit a crime or a fiscal crime shall be subject to the penalty of the deprivation of liberty for a term of between 3 months and 5 years.*
>
> *§ 2. In the event that the group or organisation specified in § 1 are of a military character or their purpose is to commit a crime of a terrorist nature, the perpetrator shall be subject to the penalty of the deprivation of liberty for a term of between 6 months and 8 years.*
>
> *§ 3. Whoever sets up a group or organisation specified in § 1 including those that are of a military character or leads or the same, shall be subject to the penalty of the deprivation of liberty up to 10 years.*
>
> *§ 4. Whoever sets up or leads or commands a group or an organisation intending to commit an act of a terrorist nature, shall be subject to the penalty of the deprivation of liberty for a minimum term of up to 3 years.*

224. There is no jurisprudence confirming the Polish authorities interpretation of Article 258§2 PC that this would be covered as an act of participation though it is clear that in some cases this article may indeed be applicable. After discussing this with the Polish authorities it seems to the evaluators that Article 258 does not fully cover all the possible situations of collection of funds intending that they be used by a terrorist organization for a legitimate purpose (e.g. charitable activity) whereas Article 258 requires an additional mental element of "intending to commit a crime or a fiscal crime".

225. Also the funding of an individual terrorist for "any purposes" as required specifically by SR.II is not fully covered by the law. In particular, the funding of an individual terrorist is only covered when that is done "*in order to finance an offence of a terrorist character"*, as long as the standards refer to *"the funding with the unlawful intention that the funds should be used or in the knowledge that they are to be used by an individual terrorist".*

226. Terrorist financing offence as prescribed above can be committed only with intent. It means that the perpetrator is willing to commit an offence or foreseeing the possibility of perpetrating it, he/she accepts it. (Article 9 § 1 P.C.)

227. Article 165a PC refers to instruments of payment, securities or other foreign exchange, property rights, movable or immovable property. The list of assets in that provision seems not to be limited, so that financing commission of an offence of a terrorist character by other means is punishable.

228. The Polish authorities have indicated that in order to completely understand the scope of Article 165a of the PC, provisions of Article 115 § 9 of the PC should be taken into consideration:

> *Article 115.*
>
> *§ 9. A movable item or chattel is also Polish or foreign currency or other means of payment and a document which entitles to obtain a sum of money or includes the obligation to pay principal, or interest, share in the profits or a declaration of participation in a company [or partnership].*

229. The Terrorist Financing Convention defines funds as assets of every kind, whether tangible or intangible, movable or immovable, however, acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.

230. The evaluators considered, based on the same explanation presented under Section 2.1 of this report (criterion 1.2 of Recommendation 1) that "property rights, movable or immovable property" in conjunction with the definitions of "financial instruments" (provided by the Act on Trading in Financial Instruments of 29 July 2005) do cover a full range of assets enumerated by the TF Convention to define "funds".

231. Article 165a PC does not require assets to be finally used for financing an offence of a terrorist character. The assets have to be only collected, transferred etc. for that purpose and a terrorist offence must be specified.

232. The provisions of the General Part of the Penal Code fully apply to the offence of terrorist financing, including the provisions on attempt to commit a crime (Chapter II, Article 13 – Article 15 of the Penal Code) and in this way the Essential Criteria II.1(d) is fulfilled.

233. The Essential Criteria II.1 (e) requires to criminalise the engagement in any types of conduct set out in Article 2(5) of the TF Convention (participate as an accomplice, organize or direct others to commit, contribute to the commission of one or more offences as set forth in the Convention by a group of person acting with a common purpose). Pursuant to Chapter II of the Penal Code a wide range of ancillary offenses are applicable as discussed under Recommendation 1 above. In particular, attempt to commit, aiding and abetting, facilitating and counselling the commission of an act as covered by the provision of Chapter II of the Penal Code, criminalise the above mentioned types of conduct.

Predicate offence for money laundering (c.II.2)

234. Due to the "all crime approach" applied in Poland the above offence is a predicate one for money laundering.

Jurisdiction for Terrorist financing offence (c.II.3)

235. The prosecution of perpetrators of international crimes defined in the Polish Penal Code's provisions apply to a Polish citizen who committed a crime abroad, as well as an alien who committed abroad an offense directed against the interests of Poland and Polish citizen who committed abroad an offense of terrorist type.

236. The Polish Penal Code may be applied in case when an alien commits abroad an offense other than those listed above, if the offense is in the Polish criminal law punishable by more than 2 years imprisonment and the offender abides in Poland and the Polish authorities decided not to give him away.

237. The condition of liability for an act committed abroad is the recognition of such an act a crime also by an Act which is in force at place of its perpetration. The following Articles of the Penal Code are relevant:

Chapter XIII

Liability for offences committed abroad

Article 109. The Polish penal law shall be applied to Polish citizens who have committed an offence abroad.

Article 110. § 1. The Polish penal law shall be applied to aliens who have committed abroad an offence against the interests of the Republic of Poland, a Polish citizen, a Polish legal person or

a Polish organisational unit not having the status of a legal person and a aliens who have committed a terrorist act abroad.

§ 2. The Polish penal law shall be applied to aliens in the case of the commission abroad of an offence other than listed in § 1, if, under the Polish penal law, such an offence is subject to a penalty exceeding 2 years of deprivation of liberty, and the perpetrator remains within the territory of the Republic of Poland and where no decision on his extradition has been taken.

Article 111. § 1. The liability for an act committed abroad is, however, subject to the condition that the liability for such an act is likewise recognised as an offence, by a law in force in the place of its commission.

§2. If there are differences between the Polish penal law and the law in force in the place of commission, the court may take these differences into account in favour in the perpetrator.

§ 3. The condition provided for in § 1 shall not be applied to the Polish public official who, while performing his duties abroad has committed an offence there in connection with performing his functions, nor to a person who committed an offence in a place not under the jurisdiction of any state authority.

Article 112. Notwithstanding the provisions in force in the place of the commission of the offence the Polish penal law shall be applied to a Polish citizen or an alien in case of the commission of:

1) an offence against the internal or external security of the Republic of Poland;

2) an offence against Polish offices or public officials;

3) an offence against essential economic interests of Poland,

4) an offence of false deposition made before a Polish office,

5) an offence, from which a material benefit has been gained even

indirectly, on the territory of the Republic of Poland.

Article 113. Notwithstanding regulations in force in the place of commission of the offence, the Polish penal law shall be applied to a Polish citizen or an alien, with respect to whom no decision on extradition has been taken, in the case of the commission abroad of an offence which the Republic of Poland is obligated to prosecute under international agreements.

238. Even though conduct that occurred in another country is not explicitly covered in terrorism financing offence, in fact it is implicitly covered by general principles of territorial jurisdiction, which are set forth in Chapter XIII of Penal Code.

239. Based on these articles, it is the Polish authority's position that CHAPTER XIII of the Penal Code is fully applicable with regard to terrorist financing offence when committed abroad.

240. Nevertheless the evaluators remain unsatisfied as to potential lack of criminality in a situation of wilful provision or collection of funds abroad intending that they be used by a terrorist organisation or an individual terrorist for a purpose considered legitimate under Polish law (e.g. charitable activity) which may not be considered an "offence against the interests of the Republic of Poland" (section 110 above). In such a case it is questionable under current legislation if criminal proceedings could be initiated in Poland.

241. The same concerns could be raised in relation with the acts constituting offences in the treaties annexed to the Convention, committed (or to be committed) abroad and which are not characterised by at least one of the purposes provided by Article 115 paragraph 20 of the Polish Penal Code.

The mental element of the FT (c.II.4 – applying c.2.2 in R.2)

242. It is accepted 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). For further discussion on the concerns the evaluators had with regard to this principle and its effective implementation with regard to ML please refer to the discussion regarding R1.

243. The concerns expressed there over the effectiveness of the actual implementation of this principle in ML cases are amplified with regard to the implementation of Article 165a especially in cases involving legitimate activity of the terrorist organization, which would obviously make it more challenging to prove the necessary criminal intent.

Liability of legal persons (c.II.4 – applying c.2.3 & c.2.4 in R.2)

244. Pursuant to Article 16 § 1 item 12 of the Act of 28 October 2002 on the Liability of Collective Entities for Acts Prohibited under Penalty, in case of commission a terrorist financing offence by a natural person , a collective entity will be liable for such an act, provided that a perpetrator :

> *"1) acts in the name or on behalf of the collective entity under the authority or duty to represent it, make decisions in its name, or exercise internal control, or whenever such person abuses the authority or neglects the duty,*
>
> *2) is allowed to act as the result of abuse of the authority or neglect of the duty by the person referred to in point 1 above,*
>
> *3) acts in the name or on behalf of the collective entity on consent or at the knowledge of the person referred to in point 1,*
>
> *4) is an entrepreneur*
>
> *- if such conduct did or could have given the collective entity an advantage, even of non-financial nature."*

245. The sanctions for legal persons are set out in Articles 7, 8 and 9 of this Act. The penalty for offences committed by corporate entities is a fine ranging from PLN 1,000 to PLN 5,000,000 (approx. €250 to €1,250,000). However, the fine may not exceed 3% of the entity's revenue earned in the financial year in which the offence was committed. The court may also order the forfeiture of any object or benefit which derived from the offence. Moreover, the court is competent to prohibit the corporate entity from carrying out promotions and advertising, benefiting from grants, subsidies or assistance from international organisations or bidding for public contracts. It can also decide to publicise the judgment. All the above-mentioned bans may be imposed for a period of one year to five years.

246. Pursuant to the provisions of Article 6 of the Act, the individual liability of the perpetrator employed in a collective entity is not excluded even if such an entity does not incur liability provided by the Act. Neither the existence nor non-existence of liability of the collective entity under the principles set out in this Act shall exclude its civil, administrative or personal legal liability for the inflicted damage

247. The quasi-criminal liability of an entity is secondary to the criminal liability of an individual acting on its behalf (i.e. the entity can be held criminally liable only after the person who committed the offence has been found guilty and sentenced by a court of law), and therefore prolonged criminal proceedings to establish the liability of an individual could produce the effect of discouraging courts from considering the liability of corporate entities.

Sanctions for FT (c.II.4 – applying c.2.5 in R.2)

248. The penalties in relation to natural persons in respect of terrorist financing are set in Article 165a of the PC. The penalty (imprisonment from 2 to 8 years) is in conformity with European Union standards and is to be considered effective, proportionate and dissuasive.

249. Up to now there have been no cases with regard to TF in Poland in this respect assessing the effectiveness is impossible.

Recommendation 32 (terrorist financing investigation/prosecution data)

250. According to the statistics provided by the Polish authorities, since 2007 the GIFI disseminated 60 TF cases to the Internal Security Agency. However, there were no investigations, indictments or convictions. The Polish authorities informed the evaluation team that a reason behind this, is that the Internal Security Agency probably didn't confirm that the submitted transactions were related to TF.

Effectiveness and efficiency

251. Polish officials indicated to the evaluators that they do not consider terrorist financing to be a domestic problem. It seems to the evaluators that whereas the risk of terrorist activity in Poland may be legitimately perceived as low, the risk of terrorist financing in Poland should be treated as high as any other jurisdiction.

252. Nevertheless in the absence of any criminal investigations for financing of terrorism, assessment of the effectiveness of the system seems impossible. Noteworthy is the fact that while there have been no indictments for financing of terrorism, reports have been sent by the GIFI to law enforcement (see SR.IV beneath).

2.2.2 Recommendations and comments

Special Recommendation II

253. Since the third evaluation an autonomous offence of terrorist financing has been added to the Penal Code (section 165a). Unfortunately the offence, as legislated, does not cover funding a terrorist organization or an individual terrorist for any purpose, and requires proof of intention to finance an offence of a terrorist character.

254. Poland should amend its legislation to bring it in line with Article 2 (1) (a) of the TF Convention which doesn't require any specific common purpose for those acts constituting offences in the treaties annexed of the Convention.

255. The Polish authorities are strongly encouraged to urgently address the shortcomings identified in the TF regime, especially with regard to criminalisation of funding terrorist organisation and individual terrorists for "any purpose".

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	**PC**	• Funding terrorist organisation for "any purpose" not fully criminalised; • The funding of an individual terrorist is not criminalised in all circumstances; • Terrorist Financing abroad is not fully covered; • There are purposive supplementary elements for some of the acts constituting offences in the treaties annexed of the Convention.

2.3 Confiscation, Freezing and Seizing of Proceeds of Crime (R.3)

2.3.1 Description and analysis

Recommendation 3 (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

256. Recommendation 3 was rated PC based on the following deficiencies:

- The confiscation regime contains no clear provision allowing for confiscation of instrumentalities which have been transferred to third parties (as they have to belong to the offender);
- There is a limited ability to confiscate criminal proceeds in financing of terrorism cases as the offence itself is limited.
- The effectiveness of the legal framework remains questionable, as only few statistics could be provided. More statistics on provisional measures and confiscation are needed.

Legal framework

257. The general legal basis for the Polish confiscation regime (known as "forfeiture") can be found in the Penal Code which provides for both general forfeiture measures and for special forfeiture in money laundering cases. The general confiscation system is mainly based on Articles 44 and 45 of the Penal Code which have not been amended since the 3rd round of evaluation. Other specific confiscation regimes exist for money laundering (Article 299 paragraph 7 of the Penal Code) and fiscal crimes (Article 33 of the Penal Fiscal Code).

258. Article 217. § 1 of the Criminal Procedure Code and subsequently Articles 291 to 295 of the Criminal Procedure Code provide provisional measures against the property of the suspect and/or accused.

259. Article 44 of the Penal Code covers objects derived directly from an offence and instrumentalities that served the crime or were used to commit the crime and reads:

> *Article 44 Forfeiture*
>
> *§ 1. The court shall order the forfeiture of items coming directly as a result of an offence.*
>
> *§ 2. The court may order, and in specified cases shall order, the forfeiture of the items that were used or were intended to be used to commit the offence.*
>
> *§ 3. If the forfeiture described in § 2 is not commensurate with the severity of the offence committed, the court may order exemplary damages to be paid to the State Treasury instead.*
>
> *§ 4. If the forfeiture of items specified in §§ 1 or 2 is not possible, the court may order the forfeiture of items with a monetary value equivalent to the items coming directly as a result of the offence, or items used or intended to be used to commit the offence.*
>
> *§ 5. The items specified in §§ 1 or 2 are not subject to forfeit if they can be returned to the aggrieved party or any other authorized party.*
>
> *§ 6. If the offender is convicted of violating a prohibition on producing, possessing, trading in or transporting specific items, the court may order, and in specified cases shall order, the forfeiture of such items.*
>
> *§ 7. If the items referred to in §§ 2 or 6 are not the property of the offender, the court may only order their forfeiture in the cases provided for in law; in the case of co-ownership, the*

order only covers the forfeiture of the share owned by the offender, or the obligation to pay a monetary equivalent.

§ 8. Items that are subject to forfeiture are transferred to the ownership of the State Treasury when the sentence becomes final.

260. Especially noteworthy is the regime stipulated in section 45 reversing the burden of proof with regard to convicted person's property. Though this is possible only with regard to property that belonged to the convicted person "*during the time of crime or after the crime was committed".*

261. Article 45 covers property related benefits and in the circumstances referred to therein, indirect proceeds are capable of forfeiture. The article reads:

Article 45

§ 1. If a perpetrator received any benefit from an offence, even indirectly, which shall not be subject to forfeiture of items referred to in article 44 § 1 or 6, a court shall impose forfeiture of such benefit or pecuniary equivalent of its value. Forfeiture shall not be applied to the benefit as a whole or its part if the benefit or its pecuniary equivalent is subject to return to the injured person or another entity.

§ 2. In case the perpetrator has been convicted for the crime as a result of which he acquired, even indirectly, a property-related benefit of considerable value, it is assumed that the property he has taken into possession or in relation to which he acquired any title of ownership during the time of crime or after the crime was committed shall constitute a benefit acquired by committing the crime till the moment a judgement – even an invalid judgement -has been pronounced, unless the perpetrator or other interested party shows evidence to the contrary.

§ 3. In case the circumstances are very likely to indicate that the perpetrator referred to in § 2 has actually ceded, under any legal title, the property constituting the benefit acquired by committing the crime to a natural person, legal person or an entity without legal personality, it is assumed that the implements remaining an intrinsic possession of such a person or entity as well as their property rights belong to the perpetrator, unless the interested person or entity shows the evidence of their lawful acquisition.

262. The special forfeiture regime set forth for money laundering cases, which enables forfeiture of equivalent value to proceeds of crime is stipulated in § 7 of Article 299. which reads:

"In the event of conviction for the offence specified in § 1 or 2, the court shall decree the forfeiture of implements derived either directly or indirectly from the crime, and also forfeiture of benefits from the crime or its equivalent even though they are not the property of the perpetrator. A decision on the forfeiture in part or in whole shall not be made if benefits from the crime or its equivalent are to be returned to a wronged person or other authorized entity."

263. In addition a special specific forfeiture regime exists in Article 33 of the Penal Fiscal Code and it is referred to cases of fiscal crimes, including some that are money laundering predicates (e.g. tax fraud, customs fraud). This article follows Article 45 of the Penal Code in form and wording.

Confiscation of property (c.3.1)

264. The deficiency previously indicated in the 3rd round evaluation with regard to the confiscation regime not covering instrumentalities transferred to third parties has not yet been amended by the Polish authorities and Section 44 (7) still reads – *"§ 7. If the items referred to in § 2 or 6 are not the property of the perpetrator, the forfeiture may be decided by the court only in the cases provided for in the law; in the case of co-ownership, the decision shall cover only the forfeiture of the share owned by the perpetrator, or the obligation to pay a pecuniary equivalent of its value ".*

265. The Polish authorities have attempted to address this deficiency. A draft amendment to the Penal Code, prepared by the Bureau for Organized Crime modifies the rules of confiscation. Paragraph 9 of the Article 299 P.C. provides for forfeiture of both direct and indirect property representing proceeds of crime. Paragraph 10 of the Article 299 PC also provides for the possibility to decree a forfeiture of instrumentalities which served the perpetrators of ML, and have been transferred to the third parties.

> *Article 299*
>
> *§ 9. In case of sentencing a person for the crime specified in § 1 or 2, the court shall decree a forfeiture of implements derived directly or indirectly from the crime and a forfeiture of the benefits gained as a result of the crime or their equivalent, even if they do not belong to the perpetrator himself. Forfeiture shall not be decreed in part or in whole in case a given implement, benefit or its equivalent shall be returned to the wronged person or other entity.*
>
> *§ 10. In case of sentencing a person for the crime specified in § 1,2 or 7, the court may decree a forfeiture of implements, that served the crime or were used to commit the crime, even if they do not belong to the perpetrator.*

266. Other than that the legislation seems to cover benefits objects and instrumentalities (though not always mandatory). The confiscation of "instrumentalities" is a subject of a discretionary decision of a court (Art 44 § 2 "*The court may order the forfeiture")*. The real impact of this subjective character of the confiscation measure is impossible to be assessed in the absence of relevant data related to the number and nature of cases when instrumentalities were seized and finally the courts decided not to confiscate them (if exist).

267. As previously noted in the 3rd round evaluation (section 162) it is questionable whether funds of "clean origin" e.g. with regard to terrorist financing may be confiscated. Given that terrorist funds may be from a lawful origin, it is questionable whether the ability to confiscate "*items directly derived from an offence*" or "*served or were designed for committing the offence*" (Article 44 of the Penal Code) or "*any benefit from an offence*" (Article 45 the Penal Code) is sufficient when the funds were not "derived" from a crime or a "benefit".

Provisional measures to prevent any dealing, transfer or disposal of property subject to confiscation (c.3.2)

268. The Criminal Procedure Code provides for appropriate provisional tools to seize the property covered by recommendation 3.1. Article 217. § 1 of the Criminal Procedure Code states that objects which may serve as evidence, or be subject of seizure or in order to secure penalties regarding property, penal measures involving property or claims to redress damage, should be surrendered when so required by the court, the state prosecutor, and in urgent cases by the Police or another authorized agency.

269. Subsequently, Articles 291 to 295 of the Criminal Procedure Code provide provisional measures against the property of the suspect and/or accused. Such measures may consist of the seizure of movables, liabilities and other property rights and in the prohibition of selling and encumbering real estate. These powers extend also to bank accounts.

Initial application of provisional measures ex-parte or without prior notice (c.3.3)

270. The Polish Law does not expressly provide for the initial application to freeze or seize property subject to confiscation to be made ex-parte or without prior notice. According to the Polish authorities Section 291 of the criminal procedure code covers this element since it states that "*the execution of this decision may be secured ex officio on the property of the accused*". Articles 217 and 220 of the CPC are also considered by the Polish authorities to be relevant within this context.

Adequate powers to identify and trace property that is or may become subject to confiscation (c.3.4)

271. Law enforcement agencies, the FIU or other competent authorities in Poland are given powers to identify and trace property that is, or may become subject to confiscation or is suspected of being the proceeds of crime.

272. Noteworthy of mentioning in this context is the establishment of the Polish Asset Recovery Office. Following the Council Decision 2007/845/JHA concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to crime (OJ EU L 332, 18.12.2007, p. 103), Polish Police Commander-in-Chief amended the organizational regulations of National Police Headquarters (KGP) functioning, establishing it as the Polish Asset Recovery Office and creating Asset Recovery Department within Criminal Investigation Bureau of National Police Headquarters. Among the tasks of this newly created unit according to the Commander-in-Chief's decree n.372 of the 14th of April 2008 is

> *(…)§ 10 Tasks of Asset Recovery Department:. Assurance of information exchange (of identification, disclosure, protection and recovery of assets that have any connection with crime) between Police units and other national entitled authorities and institutions of EU Member States(…)*

273. In addition and in order to facilitate cooperation in tracing and identifying crime-related assets, the Minister of Interior, the Minister competent for Financial Institutions and the General Prosecutor signed The Declaration of Cooperation of 18th December 2008. The parties undertook, within their powers, to work together in order to effectively carry out the tasks of detection and identifying illegally obtained proceeds and other property derived from criminal activity. The parties have established authorised proxies for the implementation of the Declaration of Cooperation.

274. On 15 September 2009, as an accomplishment of The Declaration of Cooperation, an Agreement between Minister of Interior, Minister competent for Financial Institutions and General Prosecutor has been signed. The Parties agreed to cooperate within the detection and identification of the proceeds of crime or other crime-related assets within the scope of tasks of the National Asset Recovery Office. The authorised agents set up a Steering Group responsible for coordinating the collaboration, analysis and evaluating the agreement implementation. The Contact Points were established to coordinate the exchange of information from databases generated, collected and processed by the bodies subordinate to or supervised by the parties.

275. On 16 September 2011 an Act on information exchange with law enforcement authorities of EU Member States was passed. This Act implemented several Council Decisions i.e. above mentioned Decision 2007/845/JHA and Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. According to Act of 16 September 2011, bodies entitled to international exchange of information about proceeds from, or other property related to crime through Polish Asset Recovery Office are: the Police, The Internal Security Agency, The Central Anticorruption Bureau, The Customs Service, the Border Guard, The fiscal auditing bodies, The Military Police, The Minister competent for Financial Institutions, the General Inspector of Financial Information, The Fiscal Offices and Chambers, the Prosecutors.

276. The above mentioned bodies are also obligated to assist, within the scope of their competence, Polish Asset Recovery Office (ARO) in tracing and identifying crime-related assets for the purpose of exchange information with AROs from other EU Member States.

277. The Act on information exchange with law enforcement authorities of EU Member States also amended Act on Police of 6th April 1990 adding to its Article 145k, which became new legal base for Polish Asset Recovery Office: "(…) Article 145k. 1. National Police Headquarters manage the tasks of national asset recovery bureau stipulated in the article 1 section 1 of the Council Decision 2007/845/WSiSW from 6th December 2007 concerning cooperation between Asset Recovery Offices

of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime (L 332/103):

> *Cooperation, within the meaning provided in the provisions of Council Decision 2007/845/WSiSW, between national Asset Recovery Offices of the Member States in particular in the field of exchange of information aimed in and identification of proceeds from, or other property related to, crime and processing of such data, is maintained in accordance with provisions stipulated in the Act on information exchange with law enforcement authorities of EU Member States (…).*

278. While the evaluators welcome all these initiatives which demonstrate the positive policy of the Polish government with regard to combating crime and asset forfeiture, they were not presented with actual outcome as a result of these organisational measures, which leaves the onus on the Polish authorities to hopefully present such results in the future.

279. Pursuant to Article 213 § 1 of the Criminal Procedure Code the following data concerning the suspect should be established in the course of the proceedings: identity, age, family and financial status, educational status, profession, employment and his sources of income, as well as information about his criminal record.

280. To that end, prosecutors are entitled to request the Revenue Offices to submit the documents showing suspects' property, income and amount of taxes paid. In case of allegation of having undisclosed source of income, a prosecutor may request a fiscal control to be carried out. In the course of investigation all data bases are being searched to identify suspect's movable/immovable property, securities, etc.

Police

281. The basis for Police powers useful in subject to confiscation assets tracing and identification can be found in the Act on Police of 6 April 1990. The most relevant are Articles 15 and 20 of the Act.

282. Pursuant to article 15 .1, Police officers performing activities referred to in Article 14, shall have the right to:

> *(…)*
>
> *(6) require necessary assistance from State institutions, central and local government authorities and economic units carrying out public utility activity; the institutions, authorities and units referred to are obligated, within their scope of activity, to provide assistance within the provisions of law in force,*
>
> *(7) request necessary assistance from other economic units and social organizations, and from any person to provide temporary assistance in cases of emergency under the legal provisions in force,*

Article 20:

> *1. The Police, within the limits provided for in Article 19, may obtain information, inter alia secretly, as well as store, check and process this information.*
>
> *2a. The Police may collect, process and use for accomplishment of its tasks arising from legal basis personal data of persons suspected of crimes prosecuted on indictment, of juvenile offenders who have committed crimes prohibited under the Act as crimes prosecuted on indictment, of persons of unknown identity or persons who try to conceal their identity, persons wanted, with or without their awareness and consent.*
>
> *Information mentioned in section 2a may include the following:*
>
> *(…)*

(b) education, profession, workplace, and the post occupied, as well as financial and assets status,

(…)

3. Where necessary for effective prevention of crimes specified in Article 19 (1), detection thereof, or establishment of perpetrators and collection of evidence, the Police may use information included in insurance contracts, in particular data which are processed by insurance companies and which concern the entities or individuals that signed insurance contracts, as well as privileged information processed by banks.

283. In the course of the preparatory proceedings, officer conducting the investigation may also request the prosecutor supervising the case for certain procedural acts performance in criminal proceedings. In particular he can request for issuing the decision on lifting of bank or fiscal secrecy.

284. Concerns over difficulties mentioned by law enforcement representatives with respect to obtaining beneficial ownership information, which gives reason to doubt whether the actual possibility of confiscating assets of legal entities, and which may explain the relatively low confiscation figures.

Protection of bona fide third parties (c.3.5)

285. The criminal law and criminal proceedings in Poland provide protection for the rights of *bona fide* third parties. Forfeiture of implements derived directly from the crime or implements that served the crime or were used to commit the crime cannot be forfeited if they are subject to the return to a wronged person or other authorised entity (Article 44 § 5 PC).

286. In addition orders regarding search, seizure and concerning material evidence and other actions are subject to interlocutory appeal by persons whose rights have been violated; interlocutory appeal to an issued order or action performed in the preparatory proceedings is examined by the district court where the proceedings are pending (Article 236 of the Penal Procedure Code).

Power to void actions (c.3.6)

287. There is the ability in Polish law to take steps to void actions where the persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in their ability to recover property subject to confiscation.

288. As to prevention of such action, in so far as there are shortcomings previously mentioned as to property that may be confiscated, this may have a cascading effect on the ability to take provisional measures against the property and prevent its transfer to third parties. (e.g. instrumentalities which do not belong to the perpetrator.)

289. When such actions are taken, they are void on the basis of Article 45 § 3 PC and providing that in case the circumstances are very likely to indicate that the perpetrator actually ceded, under any legal title, the property constituting the benefit acquired by committing the crime to a natural person, legal person or an entity without legal personality, it is assumed that the implements remaining an intrinsic possession of such a person or entity as well as their property rights belong to the perpetrator, unless the interested person or entity shows the evidence of their lawful acquisition.

290. The Fiscal Penal Code provides a similar solution:

Article 33 § 3 If the circumstances of a case indicate at high probability that a perpetrator, mentioned in § 2, has transferred to natural, legal person or organizational entity without legal personality, in fact or under whichever legal title, property which is a property benefit derived from committing a fiscal offence, it is considered, that things which are in independent possession of that person or entity and vested in he/she property rights, belong to a perpetrator, unless an interested person or organizational entity brings forward a prove of legally entering into their possession.

Additional elements (c.3.7)

291. Polish law does not specifically enable the confiscation of property of organizations that are found to be primarily criminal in nature (i.e. organizations whose principal function is to perform or assist in the performance of illegal activities), as it is the view of the Polish authorities that organizations which are primarily criminal in nature are not legal entities, and as such could not own any property which may be confiscated. Therefore only the property of such an organization's members is subject to confiscation. This view seems to limit the possibility of confiscating property in such cases were the property title is not of those individuals yet can be proven to be related to those organizations.

292. Polish laws provide for property subject to civil forfeiture pursuant to Article 412 of the Civil Code which reads *"Court can decree a forfeiture of a benefit for the State Treasury if the benefit was intentionally rendered in exchange for committing an act prohibited by the law or an act with a foul aim. If the object of the benefit was used or lost, its value may be forfeited."* That provision constitutes the civil forfeiture which can be applied without criminal conviction. Although the Act on Personal Income Tax of 26.07.1991 does not provide for "civil forfeiture" as such, it contains provisions which might be applied by the tax authorities in order to deprive the perpetrators of ML offence of revenues originated from undisclosed sources.

293. Pursuant to Article 30 § 1 subsection 7 of the Act, a fine consisting of a lump sum can be imposed with respect to income derived from undisclosed sources or unmatched by the disclosed sources - in the amount of 75% of income.

294. The same piece of law provides for the definition of revenues unmatched by the disclosed sources in Article 20 § 3 which reads:

> *Revenues unmatched by the disclosed sources.*
>
> *The amount of revenues unmatched by the disclosed sources or derived from undisclosed sources shall be determined on the basis of expenses incurred by the taxpayer during the tax year and the value of assets accumulated during that year, if those expenses and values are unmatched by the assets accumulated during the tax year and in previous years, derived from taxable or tax-exempt revenues.*

295. According to Polish law an offender is required to demonstrate the lawful origin of the property in case of reverse burden of proof which has been foreseen in Article 45 § 2. and § 3 P.C and Article 33 § 2 and 3 of the Fiscal Penal Code, mentioned above.

Recommendation 32 (statistics)

Table 13: Money laundering cases- Seized property

	2008	2009	2010	2011
Value of property seized	€16,350,000	€7,095,875	€51,950,870	€466,332
Number of cases in which seizure has been applied	73	47	147	13
Underlying predicate offences	Art. 54 § 1 of the Fiscal Criminal Code (tax evasion) Art. 86 § 1 of the Fiscal Criminal Code (swindle of a document concerning customs clearance) Art.56 § 1 of the Fiscal Criminal Code (tax fraud) Art.297 § 1 PC (swindle of a banking loan Art. 286 § 1 PC (fraud) Art. 271 § 1 and 3PC (intellectual forgery) Art. 270 §1PC (material forgery Art.279 § 1 PC (burglary) Art. 296 § 1 PC (causing damages in business transactions Art. 258 § 1 and 3 PC (participation in or leading a criminal group	Art. 65 § 1 of the Fiscal Criminal Code (receiving of goods subject to excise evasion) Art. 286 § 1 PC (fraud) Art. 271 § 1 and 3PC (intellectual forgery) Art. 54 § 1 of the Fiscal Criminal Code (tax evasion) Art.279 § 1 PC (burglary) Art.56 § 1 of the Fiscal Criminal Code (tax fraud) Art. 258 § 1 and 3 PC (participation in or leading a criminal group	Art. 270 §1PC (material forgery Art. 271 § 1 and 3PC (intellectual forgery) Art. 286 § 1 PC (fraud) Art. 54 § 1 of the Fiscal Criminal Code (tax evasion) Art.56 § 1 of the Fiscal Criminal Code (tax fraud) Art.62 § 2 of the Fiscal Criminal Code (making out unreliable invoices or receipts) Art. 258 § 1 and 3 PC (participation in or leading a criminal group	Art. 258 § 1 and 3 PC (participation in or leading a criminal group Art. 86 § 1 of the Fiscal Criminal Code (swindle of a document concerning customs clearance) Art. 87 § 1 of the Fiscal Criminal Code (customs fraud) Art. 54 § 1 of the Fiscal Criminal Code (tax evasion) Art.56 § 1 of the Fiscal Criminal Code (tax fraud) Art. 271 § 1 and 3PC (intellectual forgery) Art. 291 § 1 PC (receiving stolen goods)

Table 14: Money laundering cases- Property forfeited

	2008	2009	2010	2011
Value of property forfeited	€76,156	€1,868,467	€466,332	€514,055
Number of cases in which forfeiture has been decreed	6	10	13	6
Underlying predicate offences	Art. 258 § 1 and 3 PC (participation in or leading a criminal group) Art. 270 §1PC (material forgery) Art. 271 § 1 and 3PC (intellectual forgery) Art. 273 PC (usage of documents subject to material or intellectual forgery) Art.284 § 1 and 2 PC (appropriation of goods) Art. 286 § 1 PC (fraud) Art.287 § 1 PC (phishing attack) Art. 296 § 1 PC (causing damages in business transactions) Art.297 § 1 PC (swindle of a banking loan Art. 54 § 1 of the Fiscal Criminal Code (tax evasion) Art 55 § 1 of the Fiscal Criminal Code	Art. 229 § 1 PC (active bribery) Art. 258 § 1 and 3 PC (participation in or leading a criminal group) Art. 270 §1PC (material forgery Art. 271 § 1 and 3PC (intellectual forgery) Art. 273 PC (usage of documents subject to material or intellectual forgery) Art.275 § 1 PC (usage or theft of someone else's document) Art. 286 § 1 PC (fraud) Art. 54 § 1 of the Fiscal Criminal Code (tax evasion) Art.56 § 1 of the Fiscal	Art. 258 § 1 and 3 PC (participation in or leading a criminal group) Art. 271 § 1 and 3PC (intellectual forgery) Art. 273 PC (usage of documents subject to material or intellectual forgery) Art. 286 § 1 PC (fraud) Art. 54 § 1 of the Fiscal Criminal Code (tax evasion) Art.56 § 1 of the Fiscal Criminal Code (tax fraud) Art. 65 § 1 of the Fiscal Criminal Code (receiving of goods subject to excise evasion) Art.91 § 1 of the Fiscal Criminal Code (receiving of goods subject to smuggling)	Art.56 ust.3 of act on counteracting drug addiction. (trafficking in large amounts of drugs) Art. 271 § 1 and 3PC (intellectual forgery) Art. 273 PC (usage of documents subject to material or intellectual forgery) Art. 286 § 1 PC (fraud) Art.297 § 1 PC (swindle of a banking loan Art. 54 § 1 of the Fiscal Criminal Code (tax evasion) Art.56 § 1 of the Fiscal Criminal Code (tax fraud)

	(concealment of business activity) Art.56 § 1 of the Fiscal Criminal Code (tax fraud)	Criminal Code (tax fraud)		

Table 15: Statistics for seizing in non-ML cases

Year	Number of decisions on seizing	Value of seized property
2009	81,262	€76,452,954
2010	77,563	€31,025,552
2011	78,527	€87,518,305

Effectiveness and efficiency

296. The provisions in Articles 44 and 45 of the Penal Code remain unchanged since the third evaluation and contain the necessary powers to confiscate proceeds of crime and additionally provide for reversing the burden of proof in certain cases and in ensuring confiscation in the event of a transaction intended to defeat confiscation. Recent Supreme Court decisions have reassured prosecutors in the implementation of these provisions - especially as they relate to the identification and confiscation of "indirect proceeds" arising from an offence.

297. The statistics provided do in fact demonstrate the existence of a confiscation and forfeiture regime. Nevertheless there are some reasons for concern. The sums confiscated are relatively small - €500,000 annually both when comparing to the size of the Polish economy and the estimated criminal activity within its boundaries (3-5% of GDP is considered a worldwide benchmark), and in the year 2010 - when comparing to the temporary seizure of €50,000,000 that year.

298. Law enforcement representatives met during the on-site visit stated that they experienced difficulty in obtaining beneficial ownership information. This appeared to be a significant impediment to confiscating assets of legal entities, and may explain the relatively low confiscation figures

299. No statistics are available as to confiscation of proceeds of crime which are not ML or TF related, or as to the actual use of the reversal of the burden of proof.

300. The Polish authorities draw attention to the "Report on safety in Poland", prepared annually by the Ministry of Interior, among others, takes into consideration general data on the protected property and recovered, transferred in connection with the development of this document by law enforcement institutions.

2.3.2 Recommendations and comments

301. The evaluators welcome the establishing of the Polish Asset Recovery Office and creation of an Asset Recovery Department within the Criminal Investigation Bureau of National Police Headquarters.

302. Nevertheless the confiscation regime remains incomplete as instrumentalities, especially when owned by third parties, are not included in the legal framework. The discretionary character of the confiscation of the instrumentalities raises concerns.

303. The deficiencies identified in the TF offence (see supra c.II.1) potentially affect the scope of confiscation and provisional measures especially with regard to "legal" activities of terrorist organizations and individual terrorists.

304. The evaluators nonetheless encourage the Polish authorities to put more emphasis on confiscation and resources into financial investigation to improve the current results.

2.3.3 Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	**PC**	• The confiscation of instrumentalities is discretionary; • Confiscation regime does not cover instrumentalities transferred to third parties; • Limited scope of terrorist financing offence potentially affects the scope of confiscation and provisional measures especially with regard to "legal" activities of terrorist organisations and individual terrorists; **Effectiveness:** • Low effectiveness - relatively small amounts confiscated especially when compared with amounts provisionally held, and with the size of the economy and estimated crime; • Law enforcement experience difficulty in detecting criminal property and determining beneficial ownership in legal persons; • Lack of statistics on overall confiscations meant that it was not possible to assess effectiveness as to confiscation in cases other than ML.

2.4 Freezing of Funds Used for Terrorist Financing (SR.III)

2.4.1 Description and analysis

Special Recommendation III (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

305. Poland was rated PC for Special Recommendation III based on the following factors:

- The definition of funds (deriving from the European Council Regulations) did not cover funds controlled by a designated person or persons acting on their behalf or at their direction (as it is required by UNSCR 1267 and UNSCR 1373).
- There was no 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.
- There was no publicly known and clearly defined procedure for de-listing of suspected terrorists listed by Poland.
- The legal basis for monitoring of compliance with some aspects of the AML/CFT Act dealing with terrorist financing issues was unclear.

Legal framework

306. Special Recommendation III is addressed in Poland in both domestic and EU-level legislation. Funds and assets of terrorists are thus to be frozen on the basis of EU regulations and complementary domestic legislation.

307. UN Security Council Resolutions 1267 (1999), 1390 (2002), and 1455 (2003) are implemented by Council Regulation No. 881/2002 of May 27, 2002, and the most part of S/RES 1373/2001, is implemented by Council Regulation No. 2580/2001 of December 27, 2001. The persons, groups and entities based or residents within the European Union, including Poland (referred to herein as EU-internals) do not fall within the scope of Council Regulation 2580/2001.

308. The *Common Position on the application of specific measures to combat terrorism* (2001/931/CFSP) contains a definition of the terms "terrorist act" and "terrorist group" as well as a list of persons, groups and entities suspected of having carried out terrorist activities. The European Community (EC) shall ensure the freezing of funds of such persons. The *Regulation on specific restrictive measures directed against certain persons and entities with a view to combating terrorism* ((EC) No. 2580/2001) is intended to implement the Common Position 2001/931/CFSP. However, the list annexed to the Regulation is not identical with the list attached to the Common Position. The reason given for this discrepancy is that the EC has no power to take unilateral measures against persons, groups and entities acting within the EU Member States, it only has the power to restrict payments and capital movements to third countries. Hence European organizations such as the *Basque Fatherland and Liberty* (E.T.A.), the *Real IRA* and the Greek *Revolutionary Organization 17 November* which are listed in the Common Position are absent from the list attached to the Regulation. However, it is worthwhile noting that whereas persons, groups and entities identified by the United Nations Security Council *may* be included in the list attached to the Common Position, the lists adopted by the Sanctions Committee against the Taliban and Al-Qaida are transposed automatically into Community legislation.

309. However, with regards to freezing measures within the competency of the EU (*i.e.* matters covered by EC Regulations), Member States may only adopt preliminary national measures, (*i.e.* the Member States may freeze only as long as the EU has not taken action). In this regard, and as complementary national legislation that is in line with the EC Treaty, Poland has enacted the Chapter 5a of the AML/CFT Act which supplements European regulations with procedures relating to application of restrictive measures as well as procedures on countering terrorism financing.

310. The Council Regulations are directly applicable law in Poland. Funds and assets are frozen directly and immediately by the Council Regulations.

311. As far as freezing mechanism is concerned all obligated institutions are advised that they should follow Official Journal of the EU as well as consolidated list publicly available on EEAS website in order to be provided with updated information on listed entities.

Freezing assets under S/Res/1267 (c.III.1) and under S/Res/1373 (c.III.2)

Freezing assets under UNSCR 1267 (1999)

312. On the basis of both, domestic and EU legislation, freezing would be automatically applied without any additional national measures.

313. As it was pointed out Poland implements sanctions regulations in accordance with the provisions which are adopted in the framework of the EU Common Foreign and Security Policy.

314. The EU has implemented UNSCR 1267 (1999) and its successor resolutions under EU Regulation 881/2002, which provides for measures against Al-Qaeda and the Taliban. The EU Regulations have direct effect and applicability in the jurisdiction of the EU. EU Regulation 881/2002 requires the freezing of funds and economic resources belonging to, owned, held or controlled by

listed individuals or entities and prohibits making available any funds or economic resources to, or for the benefit of listed individuals or entities. The lists (annexes) are updated regularly by the EU via Commission regulations.

315. The 3rd round MER identified that the "definition of funds (deriving from the European Council Regulations) does not cover funds controlled by a designated person or persons acting on their behalf or at their direction (as it is requires by UNSCR 1267 and UNSCR 1373)". At the time of evaluation Article 2 of Council Regulation (EC) No 881/2002 provided as follow:

> *"All funds and economic resources belonging to, or owned or held by, a natural or legal person, group or entity designated by the Sanctions Committee and listed in Annex I shall be frozen."*

316. The Council Regulation (EU) No 1286/2009 of 22 December 2009 amended regulation (EC) No 881/2002 and Article 2 was replaced by the following: *"All funds and economic resources belonging to, owned, held or controlled by a natural or legal person, entity, body or group listed in Annex I, shall be frozen"*. In this respect the deficiency relating to UNSCR 1267 seems to be partially covered.

317. There are also concerns whether the EC Regulation 881/2002 expressly covers funds derived from funds owned or controlled directly or indirectly by persons acting on their behalf or at their direction. Such reference is not provided for in the EC Regulation 1286/2009 or the EU Best Practices.

318. The European Union list of designated persons is the same as the United Nations list of persons and is draw up upon designations made by the United Nations Sanctions Committee. There is no time delay in Poland, once the European Union list is created as no further regulation is needed.

319. Although, due to procedural and translation requirements, the European Commission takes a certain amount of time to update Regulation 881/2002 after the UN Security Council Committee lists a person, entity or organization, in this respect the obligation in Poland to freeze terrorist funds without delay is questionable.

320. Additionally to the requirements of the EC Regulation, there is a separate chapter in the AML/CFT Act (Chapter 5a) providing for legal framework directly addressing fulfilment of obligations imposed by the European Union legislature or on the basis of regulations issued by the Minister competent for Financial Institutions in consultation with the Minister competent for Foreign Affairs. Most of the provisions with regard to freezing of assets are enshrined in the said Act and what follows this issue remains under remit of the General Inspector.

321. Article 20d of Chapter 5a of the AML/CFT Act deals with this issue and reads as follows:

Chapter 5a

Specific restrictive measures against persons, groups and entities

Article 20d.

1. *Any obligated institution shall perform freezing of the asset values with due diligence, with the exception of movable and immovable property, on the basis of:*
   1) *the European Union legislature imposing specific restrictive measures directed against certain persons, groups or entities, and*
   2) *regulations issued pursuant paragraph 4.*
2. *Any obligated institution, while performing such freezing, submits all the data in its possession and related to the freezing of asset values to the General Inspector, electronically or in paper form.*

322. As can be seen in the cited Article 20d, "movable and immovable property" is excluded from freezing actions taken by obligated institutions.

323. Article 2 § 3 of the AML/CFT Act provides the definition of "asset values" as follow: *"means of payment, financial instruments within the meaning of Article 2, item 1 of the Act of 29 July 2005 on trading in financial instruments, as well as other securities or foreign exchange, property rights, movable asset values and immovable estate".*

324. The stipulation of these exceptions seems to be a restrictive approach of the scope of the obligations imposed by EU Regulation No 881/2002 and implicitly of the effective implementation of the requirements set out by UNSCR S/RES/1267. Even if the EU Regulation No 881/2002 is directly applicable in its entirety because the domestic law cannot restrict the scope of its application, the provisions of the AML/CFT Act could produce confusions in practice.

325. The Polish authorities consider that in the context of the implementation of S/RES/1267(1999) Article 165a (terrorist financing offence) of the Polish Penal Code is relevant to freeze funds. This could be seen in connection with the procedure for transaction suspension and account blockage provided by Article 16 and following within Chapter 5 of the AML/CFT Act.

326. According with this procedure any obligated institution which received a disposition or an order of the transactions, or carried out such a transaction, or has any information about the intention to carry out such a transaction, for which there is a reasoned suspicion that it may be related to the criminal offense referred to in Article 165a of the Penal Code shall inform without delay and transmit the relevant data to the General Inspector. The General Inspector shall immediately confirm the reception of the above mentioned information. Within 24 hours from the reception of that information, the General Inspector may provide the obligated institution with a written request to suspend the transaction or block the account for no more than 72 hours from the date and time indicated on the confirmation of the reception. The transaction is suspended or the account blocked by the obligated institution immediately upon the receipt of that request. In the same time, the General Inspector shall notify the competent public prosecutor on a suspicion of crime that has allegedly been committed. Together with this notification, the General Inspector shall provide the prosecutor with any information and documents concerning the suspended transaction or the account blocked. The prosecutor may order to suspend this transaction or block the account for a definite period, but no longer than 3 months. The suspension or the blockage falls if before the expiry of 3 months period a decision on asset values freezing will not be issued.

327. Nonetheless, the procedure described by the Polish authorities to freeze funds is not in line with Special Recommendation III, since the requirement to freeze assets should apply indefinitely in time.

328. In conclusion, taken into consideration Article 20d paragraph 1, the freezing of the *movable and immovable property* of the listed persons on the basis of UNSCR 1267 seems to be possible only in the context of procedures described above not on the basis of the European Union legislature.

329. The evaluation team was advised that no freezing measure has been applied in Poland in the context of combating FT as no assets were identified as belonging to listed persons.

Freezing assets under UNSCR 1373 (2001)

330. The UNSCR 1373 provides a general obligation for states to freeze funds and economic resources of terrorists. The UNSCR 1373 itself is not a targeted financial sanction (no list is annexed), but it obliges states to adopt domestic targeted financial sanctions, or to have appropriate mechanisms for adopting such domestic targeted sanctions.

331. Under the relevant EU legislation, the obligation of UNSCR 1373 to freeze the assets of terrorists and terrorist entities is implemented jointly by Council Common Positions 2001/930/CFSP and 2001/931/CFSP, and EU Regulation 2580/2001. The EU Regulation 2580/2001 requires the freezing

of all funds and economic resources that belong to the listed terrorists and prohibits making available any funds or economic resources for listed individuals and entities. The definition of funds, financial assets and economic resources determined by directly applicable EU Regulation 2580/2001 is in compliance with the scope of UNSCR 1373. As it was underlined above "movable and immovable property" are exempt from freezing mechanism in accordance with Article 20d of the AML/CFT Act as long this mechanism is based on "*the European Union legislature imposing specific restrictive measures directed against certain persons, groups or entities".*

332. In addition, it should be mentioned that the EU Council has the authority for designating individuals or entities. Any member state may put forward names for the list and the Council ascertains amends and reviews this autonomous EU list. The list enclosed to EU Council Regulation 2580/2001 does not include persons, groups and entities having their roots, main activities and objectives within the EU (EU internals). In this respect domestic legislation is required to deal with the European Union internals.

EU internals

333. As noted above, the EU implemented UNSCR 1373 by establishing a list of persons and entities known or suspected to be involved in terrorist activities. With respect of non-EU internals the EU Regulation 2580/2001 requires the freezing of assets. The EU internals who are only covered by the extended list of Common position 2001/931/CFSP are marked with an asterisk indicating that they are not subject to freezing obligations under EU measures, but only by increased police and judicial co-operation between the member states. EU internals therefore have to be dealt with via domestic measures.

334. A Council decision dated 22 December 2009 abrogated Common Position 2009/468 with respect to persons, groups and entities to which Articles 2, 3 and 4 of Common Position 2001/931 applied (i.e. freezing measures and police and judicial cooperation referred to above) and includes an annex with the list of persons, groups and entities targeted by Articles 2, 3 and 4 of Common Position 2001/931. The Annex to the Council Decision no longer contains any terrorist or terrorist entity classified as "internal to the EU". The previous list appended to Common Position 2009/468/CFSP dated 15 June 2009 remained in effect with respect to persons and entities listed in the "internal" category on 31 March 2010. This situation is the result of a temporary arrangement implemented after the Lisbon Treaty came into force on 1 December 2009.

335. UNSCR 1373 requires the freezing of assets of all known or suspected terrorists. The EU lists clearly indicates the names of individuals and entities which are involved in terrorism (including EU internals) and therefore the Polish authorities consider that in Poland there is a legal obligation (Article 20d of the AML/CFT Act) to freeze the assets of the persons and entities on the EU list, including EU internals. Although the evaluation team does not fully support the Polish statement since the EU Council Regulation foresees measures to freeze funds only of non-EU Internals and Common Position 2001/931/CFSP in respect of EU Internals requires member-states to afford each other the widest possible assistance in preventing and combating terrorist acts though police and judicial cooperation.

336. Further to the above, the Polish authorities indicated that the freezing of terrorist assets as required under UNSCR 1373, particularly the assets of EU internals, can also be achieved by means of regulations issued under the amended AML/CFT Act (paragraph 4 of Article 20d). This could be done by issuing regulations which would include lists of EU internals identified as being related to terrorism. Penalties for breaches of freezing obligations can also be provided for in such regulations. Concerning any freezing of funds under the AML/CFT Act, the situation has changed since the 3rd round report. The above mentioned law would constitute the legal basis for freezing of assets without the need to apply for a court order. However, no EU internals have been so far the subject of issued regulations under the AML/CFT Act.

337. The Polish authorities also noted that the above-mentioned legal possibilities do not exclude the use of judicial procedures to freeze the assets of EU internals or any other person or entity should the Polish authorities have reason to believe that such EU internals, persons or entities are involved in any terrorist-related activities. The Polish authorities indicated that the identification by the EU or by the authorities of any State, of any person or entity as being involved in terrorist-related activities is enough to trigger the judicial procedure for freezing (see below).

Procedures

338. According to Article 20(d) of the AML/CFT Act all obligated financial institutions (e.g. banks, credit institutions, insurance companies, notaries, foundations, investment funds, currency exchange bureaus) shall freeze asset values mentioned in the relevant instruments of the European Union law or Polish national regulations. Obligated institutions that freeze assets shall transmit to the GIFI all relevant data concerning the frozen assets. It should be emphasised that obligated institutions are required by virtue of law to freeze assets of listed entities, no further confirmation of the General Inspector is therefore indispensable. The Inter-Ministerial Team of Financial Security has been established by the above mentioned Act. The Committee acts as a consultative and advisory body within the scope of application of specific restrictive measures against persons, groups and entities both in the context of prospective listing as well as releasing frozen assets.

339. Furthermore, the financial institution that processes the transaction or that possess information about the planned transaction shall inform without delay and transmit all relevant data to the General Inspector if there is a suspicion that such a transaction may be related to money laundering or terrorist financing. The General Inspector shall immediately confirm the reception of the above mentioned information. Within 24 hours from the reception of that information, the General Inspector may provide the obligated institution with a written request to suspend the transaction or block the account for no more than 72 hours from the date and time indicated on the confirmation of the reception. The transaction is suspended or the account blocked by the obligated institution immediately upon the receipt of that request.

340. At the same time, the General Inspector shall notify the competent public prosecutor on a suspicion of crime that has allegedly been committed. Together with this notification, the General Inspector shall provide the prosecutor with any information and documents concerning the suspended transaction or the account blocked.

341. The prosecutor may order to suspend this transaction or block the account for a definite period, but no longer than 3 months. The suspension or the blockage falls if before the expiry of 3 months period a decision on asset values freezing will not be issued.

Freezing actions taken by other countries (c.III.3)

At the EU level, the freezing mechanisms specified by Regulation 2580/2001 authorise freezing the assets of persons and entities from a non-member state, in particular an EU member state may request the listing of a person or entity from a non-member state. Any non-member state also has the possibility of presenting the Council with a listing request. This will be examined in the light of the requirements of Common Position 2001/931 and the aforementioned regulations; to be accepted it, must be the subject of a consensus decision by member states. Each member state of the EU may propose the listing of a person or entity to the Council, as may any non-EU State (through the President of the Council). Article 2.3 of Regulation 2580/2001 specifies that the Council, by unanimous decision, establishes, reviews and amends the list of persons, groups and entities to which this regulation applies. This possibility has been implemented by the EU Council.

342. At the national level, the Polish authorities consider that under Article 18a of the AML/CFT Act the GIFI is authorised to take discretionary decisions on actions instigated in other jurisdictions. The GIFI may submit a written request to the obligated institution to suspend a transaction or block the account up to 72 hours. Procedure on notification of public prosecutor applies accordingly. However,

it should be noted that this preventive measure depends on ability to instigate further criminal proceeding.

343. Nonetheless, the evaluators consider that the prescribed measures only partially cover criteria III.3. First of all, the GIFI is not explicitly designated as an authority to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. In practice, for other jurisdictions and internal authorities it would be difficult to identify in the absence of clear legal provisions that the GIFI as a competent authority to initiate a freezing action and the subsequent freezing of funds or other assets without delay.

344. Secondly, since the freezing mechanism should extend to funds and other assets, the scope of Article 18a of the AML/CFT Act is limited to transactions and bank accounts. Article 18a allows the GIFI to send a written request to obligated institutions to suspend a transaction or block an account if the information in its possession indicates that the conducted activity is aimed at ML or TF, this freezing mechanism stated by the Polish authorities is not in line with requirements of SR.III.

345. However, according to paragraph 4 of Article 20d the Minister competent for Financial Institutions in consultation with the Minister competent for Foreign Affairs may issue a regulation to initiate actions under the mechanisms of other jurisdictions. Although it is unclear whether the freezing actions will be initiated without delay. The Polish authorities informed the evaluators that the Minister competent for Financial Institutions has never issued any regulation according to Article 20d of the AML/CFT Act.

346. In practice, most EU member states would generally opt to propose a specific person or entity for EU wide designation through EU regulations, rather than propose a person or entity to Poland for designation. As noted above, Poland has the legal mechanisms to designate EU internals through the AML/CFT Act, but has not done so. Similarly, that Act could be used for non-EU residents not integrated onto the lists under the EU Regulations.

347. As also noted above, existing is the court-based mechanisms. The procedure applicable to requests to freeze assets of terrorists is the same as for any requests for mutual legal assistance request to freeze assets in Poland of an offender being proceeded against for criminal proceedings in third countries.

348. For persons and entities that do not appear on any EU list, but for which Poland receives a direct freezing request from other jurisdictions, Poland could also use a judicial-based mechanism for seizure and confiscation of terrorist funds, in such cases, seizure and confiscation of terrorist funds can be applied according to the criminal procedures as described under Recommendation 3, though this has not yet been tested in practice.

349. Consequently, applying judicial-based mechanisms, which depend on the ability to apply criminal procedures, in executing foreign requests of freezing the funds or economic resources of certain individuals or entities, which are either EU internals, or non-EU residents, but not listed by EU or UN, does not correspond with the FATF Interpretative Note to Special Recommendation III and in any event may be too slow.

Extension of c.III.3 to funds or assets controlled by designated persons (c.III.4)

350. The freezing mechanisms under the EU Regulations apply to a broad definition of financial assets and economic resources.

351. For the purposes of EU Regulation 881/2002: "funds" means "financial assets and economic benefits of every kind, including but not limited to cash, cheques, claims on money, drafts, money orders and other payment instruments; deposits with financial institutions or other entities, balances on accounts, debts and debt obligations; publicly and privately traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures, derivatives contracts; interest, dividends or other income on or value accruing from or generated by

assets; credit, right of set-off, guarantees, performance bonds or other financial commitments; letters of credit, bills of dating, bills of sale; any documents evidencing an interest in funds or financial resources, and any other instrument of export financing." The term "economic resources" refers to "assets of every kind, whether tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods or services".

352. Under S/RES/1267(1999), funds or other assets owned or controlled, directly or indirectly, by the listed persons or entities or by persons acting on their behalf or at their direction, must be frozen. Special Recommendation III speaks in this respect of "possession or control, directly or indirectly, wholly or jointly". Article 2 of Regulation 881/2002, as amended by Regulation 1286/2009, states that "All funds and economic resources belonging to, owned, held or controlled by a natural or legal person, entity, body or group listed in Annex I, shall be frozen". Annex I includes natural and legal persons, entities, bodies and groups designated by the UN Security Council or the Sanctions Committee as being associated with Osama bin Laden, the Al-Qaeda network or the Taliban. The definition of freezing introduced in Regulation 1286/2009 is understood very broadly and in a non-limitative manner, such that it covers without exception the hypotheses set out in SR.III (freezing of funds that are owned or controlled, whether wholly, jointly, directly or indirectly).

353. For the purposes of EU Regulation 2580/2001, the definition of "funds, other financial assets and economic resources" is defined as follows "assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers' cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit". "Freezing of funds, other financial assets and economic resources" means "the prevention of any movement, transfer, alteration, use of or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character, destination or other change that would enable the funds to be used, including portfolio management."

354. The definition of "funds" as defined in Regulation 2580/2001 covers all documents evidencing title to property. Article 1 of this regulation lists the financial services, the provision of which to listed persons or entities is prohibited. The definition of "funds" under Regulation 2580 is in line with the FATF interpretation.

355. However, EU Regulation 2580/2001 does not specify the freezing of funds and economic resources controlled indirectly by a listed person or entity or by a person acting on their behalf or at their direction. Nonetheless, Regulation 2580/2001 should be read in conjunction with Article 2 of Common Position 2001/931/CFSP of 27 December 2001, which specifies "that for the purposes of this common position, 'persons, groups and entities involved in acts of terrorism' means persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; entities owned or controlled directly or indirectly by such persons; and persons, groups and entities acting on behalf of, or at the direction of such persons and entities, including funds or derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons, groups and entities". It appears that Regulation 2580/2001 in conjunction with Common Position 2001/932/CFSP meets the requirement under criterion III.4.

Communication to the financial sector (c.III.5)

356. The Council and the European Commission make both decisions and regulations public through the Official Journal of the European Union, which can be accessed by anyone on the website of the European Union. Moreover, a consolidated list of entities subject to restrictive measures is always publicly available on the EEAS website and it is updated on a regular basis. The Polish authorities consider this to be sufficient notifications to all for whom the legislation creates obligations and rights.

357. Freezing actions taken under SR.III are being communicated to the Polish financial system by promulgation in the European Union Official Journal. As soon as the promulgation occurs, the text of

the respective Regulations is accessible on the official web page of the EU. Financial institutions are expected to be up to date with the newest legislation in this field, and this expectation is clearly communicated during both on-site visits, and trainings provided by the GIFI and the PFSA (regardless of the provision of the AML/CFT Act – Article 20(d) – which requires immediate freezing actions). Should Polish authorities wish to take freezing actions themselves, these means will also be promulgated, this time in the Polish Official Journal, which is also immediately accessible via web page. In addition, the Polish authorities make note that the majority of Polish financial institutions purchase commercial sanctions and PEP's lists which are integrated into their IT systems.

358. As the 3rd round evaluation also pointed out, it is still unclear whether there is any communication between the authorities and DNFBP, or other persons and the public at large, on their obligations in this area. Some of the categories of reporting entities met on the occasion of the on-site visit did not seem to be very clear on the obligations deriving from the legal provisions implementing the UNSCR resolutions, or the manner in which the lists could be consulted. Not all the reporting entities had instruments to verify all their clients against the lists in a timely manner.

Guidance to financial institutions and other persons or entities (c. III.6)

359. As mentioned above, the expectations regarding obligations of financial institutions in respect of targeted financial sanctions, are being communicated both during onsite visits (where this issue of financial institutions' compliance with international instruments of targeted financial sanctions is always verified), and during trainings.

360. It should be noted that obligated institutions are provided with relevant guidance on a regular basis. Moreover, in 2010 there was training aimed at providing obligated institutions with detailed information on sanction regime. This seminar was followed by Q&A session. In addition, obligated institutions are assisted either via phone or an e-mail in any case related to freezing mechanism as well as application of relevant domestic and international provisions. Furthermore, in order to meet financial sector demands GIFI issued a publication on counteracting money laundering addressed to entities required to implement obligations foreseen by law.

De-listing requests and unfreezing funds of de-listed persons (c.III.7)

361. As a member state of the EU Poland relies on the formal de-listing procedures which exist under the European Union mechanisms, both in relation to funds frozen under UNSCR 1267 and UNSCR 1373. EU Regulation 881/002 provides that the Commission may amend the list of persons on the basis of a determination by the United Nations Security Council or the Sanctions Committee (Article 7). EU Regulation 2580/2001 provides that the competent authorities of each member state may grant specific authorizations to unfreeze funds after consultations with other member states and the Commission (Article 6). In practice, therefore a person wishing to have funds unfrozen in Poland would have to take the matter up with the Polish competent authorities who, if satisfied, would take the case up with the Commission and/or the United Nations.

362. Relevant EU Regulations do not provide for a national autonomous decision for considering de-listing requests and unfreezing as a whole. As such, any freezing shall remain in effect until otherwise decided by the EU. Common Position 2001/931/CFSP of the European Union along with the EU Regulation 2580/2001 implements UNSCR 1373 (2001) and provides for a regular review of the sanctions list which it has established. Moreover, listed individuals and entities are informed about the listing, its reasons and legal consequences. If the EU maintains the person or entity on its list, the latter can lodge an appeal before the European Court of First Instance in order to contest the listing decision. Delisting from the EC Regulations may only be pursued before the EU courts.

363. According to section 20e of the AML/CFT Act when specific restrictive measures are adopted individually by Poland, the designated persons, groups and entities may step forward with a justified motion to the minister competent for financial institutions, for the removal from the sanctions list. Such a motion is subject to the opinion given at the immediate meeting of the Committee of Financial

Security. In case of freezing asset values based on the individual action of Poland, the General Inspector shall, if it is possible, immediately inform the person, the group or the entity whose asset values has been frozen on the fact. Such information should include justification of the act of freezing funds as well as an instruction on how to take further actions in order to be removed from the list, appeal or nullify freezing of asset values.

364. Moreover, the AML/CFT Act states that in the decision regarding the suspension of the transaction or the blockage of the account, the public prosecutor shall define the scope, manner and time-limits of the suspension or the blockage. The decision may be appealed to the court competent to hear the case.

365. The Polish authorities note that any obligated institution, at the request of the party ordering the transaction or of the account holder, can inform the party about the suspension of the transaction or the account blockage and indicate the authority which has requested for it. However there seems not to be a Polish authority responsible for advising individuals as to the procedures necessary for requesting delisting or related matters.

Unfreezing procedures of funds of persons inadvertently affected by freezing mechanisms (c.III.8)

366. Essential criterion III.8 requires that countries should have effective and publicly-known procedures for unfreezing, in a timely manner, the funds or other assets of persons or entities inadvertently affected by a freezing mechanism upon verification that the person or entity is not a designated person.

367. According to section 20e of the AML/CFT Act in the event of freezing asset values, any person, group or entity which is not mentioned in the acts of the European Union implementing specific restrictive measures or on the list of persons, groups or entities adopted individually by Poland, such a person, group or entity may request the General Inspector to be released from freezing of asset values. In this case the General Inspector shall decide on the release from freezing asset values ex officio. The decision on the release from freezing asset values shall be by decision of the General Inspector and this decision could be subject of an appeal within 14 days after the receipt of the notification about this decision. Further the Code of Administrative Procedure is applicable.

Access to frozen funds for expenses and other purposes (c.III.9)

368. With regard to releasing funds that are necessary for basic expenses (humanitarian exemptions), the UNSCR 1452 (2002) provides that the freezing measures under UNSCR 1267 do not apply to funds and economic resources that have been determined by the relevant state (Poland) necessary for basic expenses, including payments for foodstuff, rent, etc.

369. Neither EU Regulation 881/2002, nor the subsidiary regulation against Taliban provides specific provisions on humanitarian exemptions. There is a specific procedure in EU Regulation 2580/2001 for humanitarian exemptions and application must be made to the competent authority of the member state in whose territory the funds have been frozen. The competent authority in Poland is understood to be the Sanctions Monitoring Board (as notified by Poland to the European Commission).

370. The discussed procedures are contained in the measures adopted in the framework of the EU Common Foreign and Security Policy.

371. Article 20e of the AML/CFT Act covers this as well. In the event of the freezing of assets any person, group or entity is in difficult life or material situation may request the General Inspector to be released from freezing of asset values. In such case, the General Inspector may determine a total or a partial release from freezing asset values, if it is not contrary to the binding resolutions of international organisations.

Review of freezing decisions (c.III.10)

372. Relevant procedures, by which the freezing measure can be challenged with a view to having it reviewed by a court, are provided, first and foremost, at the European Union level. Freezing mechanisms envisaged by the relevant EU regulations can be challenged at the Courts of the European Union whereby any natural or legal person directly and individually affected by a restrictive regulation or decision can challenge it under the general principle established by Article 263 of the Treaty on the functioning of the European Union. The legality of freezing measure can also be challenged by bona fide third parties before the Courts of the European Union. Moreover, in accordance with Article 20e of the AML/CFT Act a person, body or entity whose assets have been frozen may submit relevant motion to General Inspector, who is the competent authority to make the decision on releasing frozen assets (either positive or negative). The appeal against the said decision should be filed to the minister competent for financial institutions within 14 days after the receipt of the notification about this decision and the proceeding is carried out in accordance with the Code of Administrative Procedure. The decision made by the minister competent for financial institutions may be then appealed at the administrative court.

Freezing, seizing and confiscation in other circumstances (applying c.3.1-3.4 and 3.6 in R.3, c.III.11)

373. Section 165a of the Criminal Code criminalizes terrorist financing and all measures applicable to the criminal offences (e.g. article 44 of the Penal Code) are applicable. If a person has been prosecuted for terrorist financing, the Polish authorities indicated that they would follow the provisions described earlier in respect of freezing, seizing and confiscating. In that case the same provisions of the General Part of the Criminal Code, addressing issues of forfeiture, reverse burden of proof and protection for the rights of bona fide third parties, are applicable.

374. Nevertheless the shortcomings mentioned above with regard to the scope of Section 165a of the Penal Code especially with regard to financing "lawful" segments of terrorist organizations activity, as of individual terrorists, are relevant in this context as well.

375. Polish law relating to confiscation and seizure are of general application; consequently, the measures in place pursuant to Recommendation 3 apply to funds or other assets relating to terrorism other than those targeted by Resolutions 1267 and 1373. Here to the shortcomings identified in Recommendation 3 therefore concern freezing, seizure and confiscation of funds or other assets relating to terrorism cascade on the application of Resolutions 1267 and 1373.

376. So far as confiscation / forfeiture is concerned, given that terrorist funds may be from a lawful origin, it is questionable whether the ability to confiscate "*items directly derived from an offence*" or "*served or were designed for committing the offence*" (Article 44 of the Criminal code) or "*any benefit from an offence*" (Article 45 of the Criminal Code) is sufficient when the funds were not "derived" from a crime or a "benefit".

Protection of rights of third parties (c.III.12)

377. It seems that third *bona fide* parties may exhaust the procedure set in section 20e of the AML/CFT Act which empowers the GIFI to release from freezing asset values *ex officio*, with possible appeal to the minister competent for financial institutions within 14 days after the receipt of the notification about this decision, all according to the provisions of the Code of Administrative Procedure, with a possible final appeal to the administrative court.

378. The Polish authorities additionally rely, in this context, on the criminal law and criminal proceedings which provide protections for the rights of *bona fide* third parties. Forfeiture of implements derived directly from the crime or implements that served the crime or were used to commit the crime cannot be forfeited if they are subject to the return to a wronged person or other authorized entity (Article 44 § 2 I 5 PC). Secondly, orders regarding search, seizure and concerning material evidence and other actions are subject to interlocutory appeal by persons whose rights have been violated; interlocutory appeal to an issued order or action performed in the preparatory

proceedings is examined by the district court where the proceedings are pending (Article 236 of the Penal Procedure Code).

Enforcing obligations under SR.III (c.III.13)

379. The GIFI is responsible for supervising the compliance with Special Recommendation III so far no sanctions have been imposed on financial institutions that failed to comply with the requirements of SR.III.

380. According to the Polish authorities adequate monitoring is in place to ensure compliance with relevant provisions referring to sanction regime. Moreover, obligated institutions are required to have in place internal procedures describing, inter alia, course of action in case of the suspension of transactions, account blocking and account's freezing. This aspect is always given thorough consideration during on-site inspection and what is more lack of the said procedure under the AML/CFT Act is subject to penalty of imprisonment up to 3 years. Pursuant penal provisions as stipulated in the AML/CFT Act it is also punishable when obligated institution contravenes obligation either to block an account or suspend transaction.

381. Furthermore, in accordance with Article 34b of the Act the obligated institution are subject to pecuniary penalty if they fails to comply with obligation to freeze the asset values of a person, group or entity or do not provide the General Inspector with all the data available to reasoning the freezing of asset values.

382. The Polish authorities additionally point to the Article 165a of the Polish Penal code states, which would apply, with regard to SRIII in cases when the obligated institution acts "with purpose to finance an offense of terrorist character".

Additional element – Implementation of measures in Best Practices Paper for SR.III (c.III.14) & Implementation of procedures to access frozen funds (c.III.15)

383. It appears that Poland has partially implemented the Best Practice Paper for SR.III by way of the EU and domestic legislation described earlier in this section.

384. In respect of the procedures to authorise access to funds and other assets that were frozen pursuant to UNSCR 1373 and that have been determined to be necessary for basic expenses, the payment , measures described in Article 20e of the AML/CFT Act under Criteria SR.III.9 are also applicable to and consistent with UNSCR 1373 and the spirit of UNSCR 1452

Recommendation 32 (terrorist financing freezing data)

385. According to the regulations of the AML/CFT Act (Chapter 5a) the obligated institutions – which freeze assets on the basis of the EU regulations – are obligated to submit all information related to the freezing of asset values to the GIFI, electronically or in paper form.

386. In the previous years there was no such information from the side of the obligated institutions.

Effectiveness and efficiency

387. As no information is available it is not possible to assess effectiveness

2.4.2 Recommendations and comments

388. UN Resolutions 1267 and 1373 (in respect of Non-European Union citizens) are legally implemented through EU mechanisms. Since the third round an amendment Article 20d of the AML/CFT Act has provided a clear legal mechanism, which would potentially cover designations in Poland in respect of EU citizens or named persons not covered by the EU clearing house list proposed by other countries, unfortunately the Polish authorities have chosen not to apply this mechanism yet.

389. A clear designating mechanism in such circumstances should be created. The US lists were automatically circulated. It appeared the obligated institutions sporadically check against the lists, but no terrorist accounts had been identified. Supervisors should check compliance with this obligation. The examiners were concerned that the law may not ensure adequate blocking of accounts under the lists in the absence of legal proceedings and this aspect should be urgently reviewed.

390. The Polish authorities may wish to consider, as they develop procedures and in the light of experience with the court based system, the merits of a more general administrative procedure for handling SR.III in its entirety, subject to proper safeguards (especially with regard to bona fide third parties).

391. Movable and immovable property should not be exempted from the freezing mechanism as there currently are pursuant to Article 20(d) of the AML/CFT Law.

392. The Polish authorities may consider amending its national legislation in order to cover deficiencies under the EU Regulations.

393. The Polish authorities should establish an effective system of communication with the DNFBP sector in respect of the obligations under SR.III.

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	**PC**	***Implementation of S/RES/1267*** • The EU or Polish Legislation do not cover the freezing of funds derived from funds owned or controlled directly or indirectly by persons acting on their behalf or at the direction of designated persons or entities; • The time taken to amend the EU regulations following amendments made to the list published by the 1267 Committee is relatively long; in this respect the obligation to freeze terrorist funds without delay is not observed; • The freezing mechanism under Article 20d of the AML/CFT Act excludes movable and immovable property, which restricts the scope of the obligations imposed by EU Council Regulation 881/2002; • Reliance on a criminal proceedings in order to freeze terrorists funds is not fully in line with the requirements of UNSCR 1267 since the requirement to freeze assets could be limited in time according to the Criminal Procedure Rules; ***Implementation of S/RES/1373*** • Poland has not yet taken specific measures to cover "EU internals"; • The freezing mechanism under Article 20d of the AML/CFT Act excludes movable and immovable property, which restricts the scope of the obligations imposed by EU Council Regulation 2580/2001; • Reliance on a criminal proceedings in order to freeze terrorists funds is not fully in line with the requirements of UNSCR 1373 since the requirement to freeze assets could be limited in time according to the Criminal Procedure Rules; *Other deficiencies:* • No communication system between the authorities and DNFBP;

		Effectiveness: • Concerns over the effectiveness due to conflicting provisions in the EU Regulations and Polish legislation.

2.5 The Financial Intelligence Unit and its functions (R.26)

2.5.1 Description and analysis

Recommendation 26 (rated C in the 3rd round report)

Summary of 2007 factors underlying the rating

394. Poland was rated "Compliant" in respect of Recommendation 26.

Legal framework

395. According to Article 3(1) of the AML/CFT Act, the competent government authorities responsible for combating money laundering and terrorist financing are:

a. the Minister competent for Financial Institutions as the supreme authority of financial information; and

b. the General Inspector of Financial Information, hereinafter referred to as the "General Inspector".

396. The General Inspector together with the Department of Financial Information constitute the FIU of Poland ("the GIFI").

397. The powers and functions of the GIFI are set out under Chapter 2 of the AML/CFT Act and include receiving, analysing and disseminating disclosures of STRs.

398. Additionally, the GIFI is authorised to supervise obligated entities in relation to their compliance with legal regulations on counteracting money laundering and terrorist financing and to impose penalties in line with the Act.

399. The following legislative acts regulate the Polish FIU's powers and functions:

a. The AML/CFT Act of 16th November 2000 on Anti-money Laundering and Combating the Financing of Terrorism (Journal of Laws 10.46.276 – consolidated text as amended);

b. Regulation of the Minister competent for Financial Institutions on determination of the sample register of transactions, the method of its maintenance and the mode of submitting the data from the register to the General Inspector of Financial Information dated 21 September 2001;

c. Regulation of the Minister competent for Financial Institutions on the form and mode of transfer by the Border Guard bodies and customs authorities information to the General Inspector of Financial Information dated 17 October 2010;

d. Council Decision of the European Union 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information;

e. Regulation of the Minister competent for Financial Institutions on the list of equivalent third countries dated 20 October 2009, which entered into force on 22 October, 2009. (OJ 2009 No 176, item 1364).

Establishment of an FIU as national centre (c.26.1)

400. According to Article 3(4) of the AML/CFT Act, the General Inspector performs his duties with the assistance and support the Department of Financial Information, which is situated within the structure of the Ministry of Finance. The General Inspector and the Department of Financial Information together form an administrative type of FIU. The Director and Deputy Directors of the Department are authorised by the General Inspector to perform all the functions attributed to the General Inspector by the AML/CFT Act, including gathering information, disseminating information and suspending transactions. In practice, the large majority of decisions related to the daily operations of the GIFI are taken by the Directors and the Deputy Directors rather than the General Inspector. However, this arrangement is not expressly regulated by the provisions of the Act, which can give rise to certain ambiguities.

401. Article 4(1) of the AML/CFT Act stipulates the General Inspector's duties, which involve acquiring, collecting, processing and analysing information in the manner prescribed by the law and undertaking actions aimed at counteracting money laundering and terrorism financing. In particular the General Inspector is responsible for the following duties:

1) the investigation of a transaction which has raised reasoned suspicions of the General Inspector;
2) suspending transactions or freezing accounts ;
3) adjudicating on the release of frozen asset values related to financial sanctions as provided for under domestic, EU and UN Regulations;
4) disclosing information on suspect transactions or requesting information on such transactions;
5) submitting documentation to appropriate bodies supporting a suspicion on the commission of a criminal offence;
6) initiating and undertaking other measures to counteract money laundering and financing terrorism, including training provided to the personnel of obligated institutions on the obligations which are applicable to these institutions;
7) monitoring of compliance with legal requirements on AML/CFT;
8) cooperating with foreign institutions and international organisations dealing with anti-money laundering or combating terrorist financing;
9) imposing penalties as referred to in the AML/CFT Act.

Guidance to financial institutions and other reporting parties on reporting STRs (c.26.2)

402. Pursuant to Article 13 of the AML/CFT Act the Minister Competent for Financial Institutions (which, together with the General Inspector, is the competent authority for AML/CFT), in consultation with the Minister Competent for Internal Affairs and the President of the National Bank of Poland, determines by regulation:

a. the form of the register referred to in Article 8 paragraph 4, the manner in which the register is to be operated and the procedure for the delivery of data from the register to the General Inspector;
b. the procedure for providing information on the transactions referred to in Article 8 paragraphs 1 and 3 to the General Inspector when using computerised data storage carriers.

403. As was mentioned in the 3rd round MER of Poland, in order to fulfil the requirement under Article 13 of the AML/CFT Act, on 21st September 2001 the Minister competent for Financial Institutions adopted the Regulation "on the determination of the sample register of transactions, the

method of its maintenance and the mode of submitting the data from the register to the General Inspector of Financial Information".

404. Paragraph 1 of this Regulation sets out detailed requirements on the content of the sample register of transactions, the manner in which the register is to be maintained and the mode of submitting the data from the register to the GIFI.

405. Paragraph 2 stipulates that the register of transactions should be kept by the obligated institutions in paper format or electronically. According to Article 8(4) of the AML/CFT Act, the register of transactions shall be stored for a period of 5 years, which shall commence on the first day of the year following the year when the transactions were recorded.

406. According to paragraph 3 of the Regulation the register in paper format shall be kept in a file format consisting of subsequently numbered transaction cards, drawn up and filled in separately for each registered transaction. The register kept in electronic format shall consist of records inserted separately for each transaction (Paragraph 4).

407. Annex 3 of the Regulation contains a sample reporting form.

408. It is worth mentioning that when an obligated institution identifies any errors in the information submitted to the GIFI, they are required to re-submit the accurate data to the GIFI within seven days. Although, the Polish authorities informed the evaluators that if such errors are minor, does not stop the GIFI from analysing such reports received from obligated institutions and implement this information to the data base of the GIFI. In case errors are substantive, the GIFI requires obligated institutions to correct and send a revised report back within 7 days. Additionally, the Polish authorities stated that if during the analysis analysts find an inconsistency between information provided by two or more different obligated institutions, a request is send to obligated institutions to correct the previously provided information within 7 days.

409. Although, the scope of application of this Regulation does not extend to terrorist financing, Annex 2 to the Regulation contains a requirement to provide information on transactions used for terrorist financing purposes within the form to be submitted to the GIFI. It is assumed that Annex 2 was updated when terrorist financing provisions were introduced within the AML/CFT Law.

410. Nevertheless, the Regulation does not make any reference to the reporting requirements under Articles 16 and 17 of the Act which were introduced in 2009. Therefore, the Regulation needs to be updated to be brought in line with the new AML/CFT Act. During the on-site visit the authorities (FIU) informed the evaluation team that the drafting of a new Regulation is already in progress.

411. In addition to the Regulation on the manner of reporting, the GIFI also assists obligated institutions with other issues such, as for instance, the software to be used while providing the GIFI with suitable data and the means of encrypting the transferred files. The GIFI publishes responses to the queries submitted by obligated institutions regarding the reporting process. The GIFI has also published a short Guide for obligated institutions on forwarding data to the GIFI in an electronic form on its website. Specimen transaction forms are also available on the GIFI's website.

412. Every month, information on transactions submitted incorrectly is analysed by the GIFI:

- the analysis focusses on the type of errors, the fields where such errors appear and the obligated institutions which repeatedly submit data incorrectly;
- a representative of the GIFI contacts the reporting institutions (by phone, by e-mail or by means of a letter) in order to draw their attention to the error(s) identified. The GIFI representative provides feedback and requests the reporting institution to rectify the error;
- meetings/consultations with representatives of the reporting institutions and associations of the reporting institutions are held; this includes targeted meetings to provide guidance on the

manner in which the most common transactions that are reported by a specific category are to be presented to the FIU.

413. Moreover, the GIFI also provides awareness-raising guidance notes[24] on reporting and registering obligations. These guidance notes are published on the website of the GIFI:

- Communication on registering transactions by leasing companies (referred to in art. 2 paragraph 1 letter b of AML/CFT Act);
- Communication of the GIFI on the obligation and method of registering of transactions on derivatives;
- Communication of the GIFI on transactions registered and forwarded to the GIFI by life insurance companies, including domestic ones, main branches of an insurer from a non-EU member state, branches of an insurer from a EU-member state and life insurance intermediaries, unless an insurer is responsible for their operations;
- Guidance on fulfilling duties by foundations;
- Guidance on registering transactions by notaries;
- Guidance on conducting activity of foreign currency exchange via Internet.

Access to information on timely basis by the FIU (c.26.3)

414. The Polish FIU has direct access to the following databases:

a. KCIK (National Centre of Criminal Information) - administered by the Police;

b. KEP (National Tax-payers Register) – gathers data of natural and legal persons; provides possibility to verify certain information by searching the usage of NIP number in business conduct. It has applications, e.g. to search links between entities, contacts to the persons analysed, identity documents, bank accounts, nationality, etc.;

c. KRS (National Court Register) – publicly-available database administered by the Ministry of Justice;

d. PESELnet - database gathering information on personal identification number assigned to Polish citizens;

e. CELINA (system of analysis of customs declarations) – one may search by: name, REGON (number assigned by National Register of Business Activity that is maintained by the Central Statistical Office), PESEL (personal identification number), and NIP (tax identification number). The results of the searches are SAD documents, which define country of destination, date, entity name (importer/exporter), identification data, description of goods, as well as the value;

f. VIES - database which gathers data on turnover of goods within the EU, such as quotas from customs declarations, dates and country of destination, data that may identify the orderer/foreign beneficiary (e.g. VAT-EU number, name, address);

g. REMdat - tax declarations register;

h. CERBER (bank accounts and accounts held by cooperative savings and credit unions, including deposits register) - this database enables a search by accounts owned by a particular person.

[24] http://www.mf.gov.pl/index.php?const=7&dzial=80&wysw=81&sub=sub3

415. One of the most important databases mentioned above is the KCIK, which facilitates cooperation between the GIFI and the Police. According to the National Centre for Criminal Information Act, KCIK is administered by the Police and is used as a conduit through which both the GIFI and the Police send requests for information to each other. The database enables the GIFI to determine whether the Police have conducted any investigation with respect to any person subject to a GIFI analysis. Similarly, the Police can refer to the database to confirm whether a person under investigation has been subject to an analysis by the GIFI. Since information in the database is not always immediately updated, the Police usually requests information directly from the GIFI in terms of Article 33 paragraph 1 point 1 of the AML/CFT Act.

416. The GIFI also maintains its own database, SIGIIF, which contains information on threshold transactions, STRs, data concerning analytical issues and information on cross-border cash declarations over €10,000. Since 2011 customs authorities have been inputting data on cross-border cash declarations directly into the SIGIIF.

417. In addition to the direct access to various databases, the General Inspector is empowered to request all government and local government authorities, other public organisational units, the National Bank of Poland, the Polish Financial Supervision Authority and the Supreme Chamber of Control to provide any information necessary to carry out the tasks assigned to the GIFI(Article 15 of the AML/CFT Act).

418. Although, there is no legal provision under the AML/CFT Act requiring the above-mentioned entities to provide information indirectly accessible by the GIFI on a timely basis, the Polish authorities informed the evaluation team that when a request is made to the governmental or supervisory authorities, it always indicates the timing of the response. This approach used by the GIFI shows that the governmental and supervisory authorities are provide information on a timely basis.

Additional information from reporting parties (c.26.4)

419. Pursuant to Article 13a of the AML/CFT Act, at the written request of the General Inspector, any obligated institution shall immediately disclose any information related to the transactions covered by the provisions of the AML/CFT Act. Such disclosure shall consist of information on the parties to a transaction, the content of documents relating to a transaction, and the balance and turnover of an account.

420. The Polish authorities remarked that Article 13a is a general provision which enables the FIU to request any information on transactions without any limitations. Additionally, the Polish authorities pointed out that even though Article 13a refers to transactions, the second part of this Article clearly refers to all information on the parties of a transaction, including information related to funds and beneficial owners. The evaluation team agreed with the explanation provided by the Polish delegation that Article 13a allows requesting all necessary information to fully fulfil the GIFI functions. Nonetheless, representatives of the GIFI informed the evaluation team that relevant statistics on requests made to obligated institutions according to Article 13a of the AML/CFT Act is not maintained.

Dissemination of information (c.26.5)

421. One of the duties of the General Inspector set out in Article 4(5) of the AML/CFT Act is to submit documentation supporting the suspicion of the commission of a criminal offence to appropriate bodies. The legal provisions on the dissemination of information, including the analytical reports, to the Public Prosecutor and other relevant bodies are set out in Chapter 4 of the AML/CFT Act.

422. Article 31 states that, where on the basis of the processing or analysis of information in its possession, the GIFI determines that there is a suspicion that a crime referred to in Article 165a and Article 299 of the Penal Code has been committed, the GIFI shall notify the public prosecutor of such suspicion and provide information supporting this suspicion.

423. Article 32 authorises the General Inspector to disclose any information collected in the performance of his functions to the courts and prosecutors, upon their written request, for the purpose of criminal proceedings. In order to verify the data contained in the notification made by the General Inspector, the prosecutor may request the General Inspector to provide information protected by law, including bank or insurance secrecy. Such information may also be requested in the course of the proceedings conducted pursuant to Article 307[25] of the Code of Criminal Procedure. If the information available to the General Inspector is not sufficient to enable the prosecutor to initiate preliminary ML/FT proceedings, the request can be directed to the obligated institution.

424. In addition to the dissemination of information to the Public Prosecutor, in terms of Article 33 of the AML/CFT Act, the General Inspector may disseminate information on suspicions of ML/FT to the following competent authorities:

- the Minister Competent for Internal Affairs;
- the Customs Service;
- the Internal Security Agency;
- the Intelligence Agency;
- the Military Counter-Intelligence Service;
- the Military Intelligence Service;
- the Fiscal Control Authority;
- the Central Anti-Corruption Bureau;
- the PFSA

425. The information referred to in Article 33, does not refer to disseminations of the analytical product produced by the GIFI (which is covered under Article 31). In fact, in terms of Article 33(1), the GIFI submits information to the above-mentioned competent authorities upon their written and reasoned request clearly indicating that this provision deals with the exchange of information. Additionally, Article 33(1) states that the competent authorities may only request information from the GIFI insofar as such a request is within their statutory powers. However, in practice, the GIFI appears to submit analytical reports to such entities on the basis of Article 33(3), even though this article only refers to the submission, at the initiative of the GIFI, of "*information on the transactions covered by the provisions of the Act"*, but not the analytical reports containing a reasonable suspicion of ML/FT. The evaluators consider the legal basis for such a procedure to be rather ambiguous.

426. In 2011, the number of disseminations by the FIU to other competent authorities exceeded the number of disseminations to the public prosecutor in a significant manner (refer to Table 16 below), notwithstanding the fact that the public prosecutor is formally the entity which is authorised by law to receive analytical reports.

427. Furthermore, it was noted that twenty-seven per cent of the total number of disseminations was sent to the investigative body of the Fiscal Control Authority, prompting the evaluators to conclude

[25] *Article 307. § 1. If necessary, it may be demanded that the data contained in the notice of the offence committed shall be completed within a specified time-limit, or a verification of the facts in the matter may be conducted. In that case the order instituting the investigation, or refusing the institution should be issued within thirty days of the day on which the notice was received.*

§ 2. In the verifying proceedings no evidence from an expert opinion or actions requiring records are undertaken, except for taking an oral notice of the offence or a motion for prosecution and the action specified in § 3.

§ 3. The data contained in the notice of offence may also be completed by examining the notifying person in the capacity of a witness.

§ 4. (abrogated).

§ 5. Provision of § 2 shall apply accordingly, in the event that a prosecution agency, prior to the issuance of the order to institute investigation, undertakes the verification of their own information leading them to suppose that an offence has been committed.

that a significant portion of FIU information is being utilised for the investigation of fiscal offences. The Polish authorities pointed out that the GIFI and the Fiscal Control Authority are focused on a common goal, which is the protection of the fiscal system of the State.

Table 16. Statistics on dissemination of information according to the Articles 31, Article 33(1) and 33(3) of the AML/CFT Act

	2007	2008	2009	2010	2011
Public prosecutor	190	246	180	120	130
Fiscal control offices	14	43	107	195	184
Internal Security Agency	22	26	73	89	156
Central Bureau of Investigation		13	38		
Police	n/a	n/a	n/a	122	172
Border Guards	n/a	n/a	1	7	14
Central Anticorruption Bureau	n/a	1	7	6	11
PFSA	1	1	-	-	2

Operational independence and autonomy (c.26.6)

428. The General Inspector together with the Department for Financial Information form the Polish FIU. The General Inspector is an Undersecretary of State within the Ministry of Finance, who is appointed and dismissed by the Prime Minister at the request of the Minister of Finance. Additionally, even though the General Inspector has other functions, in particular he serves as an Under Secretary for fiscal matters, the evaluators took the view that this supplementary function does not impact on the GIFI operational independence and autonomy. The Department is also situated within the structure of the Ministry of Finance. The Director and Deputy Directors of the Department are appointed and dismissed according to the Act of Civil Service (Journal of Laws No 227, item 1505). According to the Polish authorities the GIFI has full operational independence and autonomy and is not subject to any undue influence from the Minister of Finance.

429. The authority to receive and disseminate information, in particular analytical reports, is vested in the General Inspector pursuant to Articles 12(2), 16 and 31 of the AML/CFT Act. These provisions guarantee the independence and autonomy of the General Inspector insofar as receipt and dissemination of FIU information are concerned.

430. According to Articles 13a and 15 of the AML/CFT Act, the GIFI can request any information from the obligated institutions and cooperative units necessary to carry out his tasks in the field of combating ML and TF. These Articles contribute towards the FIU's operational independence and autonomy.

431. Although the GIFI does not have its own budget, it is authorised to reserve funds for its own expenditures in the central budget of the Ministry of Finance on an annual basis. The expenditures of the FIU include the purchase of software and hardware, maintenance of hardware, management of data security, training, international and internal relations and membership fees of international organisations. The salaries of the staff of the FIU, which consists of civil servants, are paid from the central budget of the Ministry of Finance.

432. The evaluators believe that the GIFI has sufficient operational independence and autonomy and is free from undue influence and interference.

Protection of information held by the FIU (c.26.7)

433. According to Art. 30 of the AML/CFT Act, any information which is received or provided by the GIFI is protected by separate laws governing the rules for their protection.

434. Article 30a requires the General Inspector and the staff of the Department of Financial Information to maintain confidential any information which came in their possession pursuant to the performance of their duties, in accordance with the principles and procedures specified in separate regulations. The requirement to maintain confidentiality shall apply to the staff of the Department even after the termination of their employment. There is no similar requirement with respect to the General Inspector.

435. On a practical level, the information held by the GIFI is physically protected through various measures. The GIFI network system is an isolated network and is never connected to the internet. All workstations having access to the GIFI system are located in a secure zone and access to the zone is monitored and locked. Access to the secure zone is limited to FIU employees who are required to have valid security clearance. Data transfers to and from the GIFI network is monitored. Users are accountable for all transfers. All activities within the system are subject to internal security regulations which are regularly revised.

436. The FIU premises are separated from the rest of the Ministry of Finance building and access is possible only upon production of a personalised card.

437. Dissemination of information by the GIFI may only take place in accordance with Article 31 and 33 (dissemination to competent authorities).

Publication of periodic reports (c.26.8)

438. According to Art. 4a of the AML/CFT Act, the GIFI is required to submit an annual report to the Prime Minister within three months of the end of the year under review. The report is then published on the website of the Ministry of Finance.

439. Every annual report should include the number of transactions reported by the obligated institutions, a description of the actions undertaken in response to such notifications, the number of cases resulting in judicial proceedings, the number of persons subject to the judicial proceedings and the amount of assets that were frozen, suspended, seized, confiscated or forfeited.

440. The annual reports[26] of 2007 – 2011 of the GIFI were provided to the evaluators. The annual reports contain various statistics on the number of STRs received, the cases opened by the GIFI, the cases disseminated to the law enforcement authorities, the on-site inspections carried out and the requests for exchange of information made and received. The annual reports also contain various detailed typologies and trends identified by the GIFI in the year under review.

[26] http://www.mf.gov.pl/en/ministry-of-finance/aml-CFT/publications

Membership of Egmont Group & Egmont Principles of Exchange of Information among FIUs (c.26.9 & 26.10)

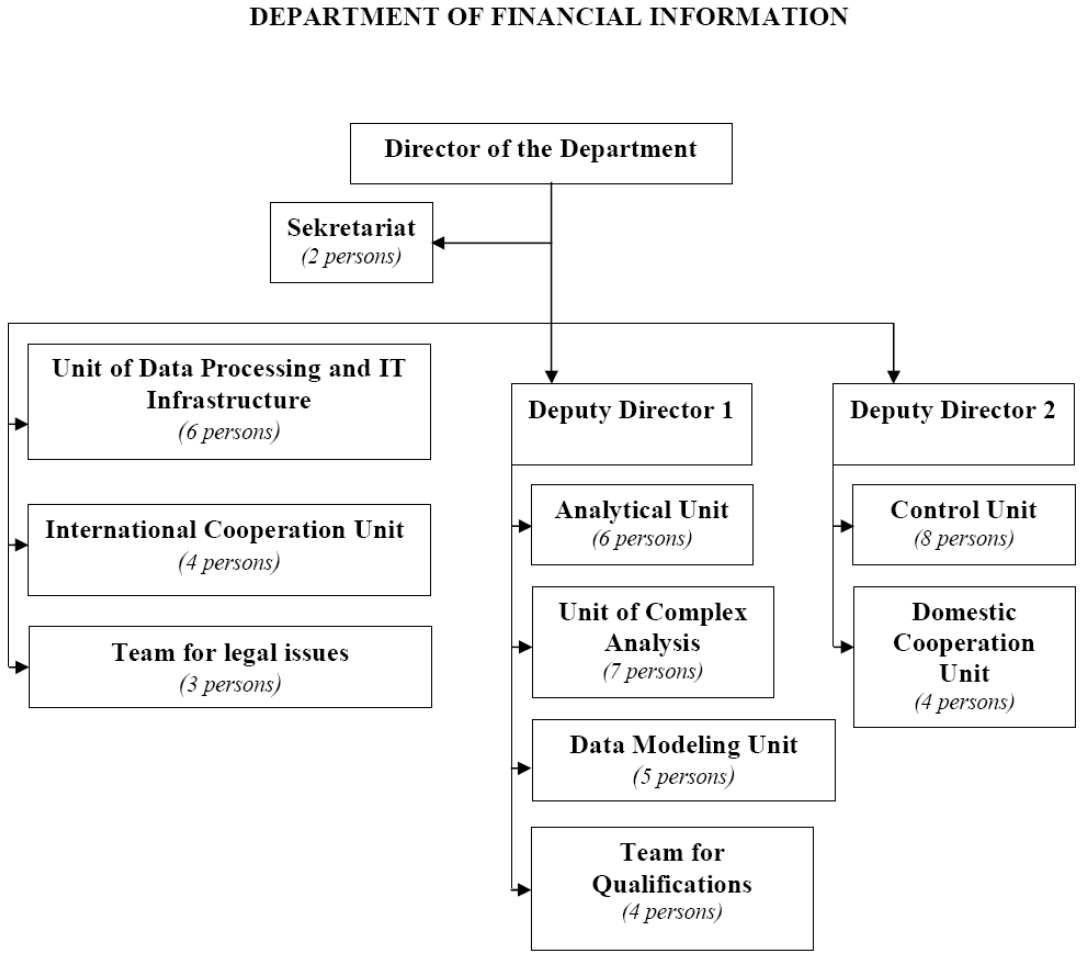
441. Poland has been a member of the Egmont Group for the past ten years. The GIFI is very active in its efforts to consolidate the exchange of information with foreign counterparts. Exchange of information with foreign counterparts is carried out through the Egmont Secure Web (ESW) and FIU.Net.

Recommendation 30 (FIU)

Adequacy of resources to FIU (c.30.1)

442. Since the 3rd round, the GIFI has gone through a restructuring process and has established various new units: a unit for domestic co-operation responsible for the effective exchange of information with cooperating units, a special unit for complex analysis, a unit entrusted with the function to carry out preliminary analysis of submitted STRs and other units for data modelling and data processing, including IT infrastructure. The below organogram was provided by the Polish Authorities.

Diagram 1: Structure of the Department of Financial Information



443. At the time of the on-site visit, the Department of Financial Information of the GIFI employed 52 officers, including the Director and two Deputy Directors. The evaluators are of the opinion that the Department is not adequately staffed, especially considering the large number of STRs received. The problem is particularly acute within the analysis section which is composed of 22 analysts. As was

stated at the on-site visit, the analysis of large cases generally drains significant resources of the analytical sections, often for long periods of time. As a result a backlog of cases is created causing difficulties in the effective analysis of less significant cases.

444. The analysts have at their disposal the following analytical software: a) Clementine, which is an analytical tool with graphical query editor and ability to run predefined queries, b) Business Object - a software for management of data and statistical purposes, c) Visual Links - an analytical tool for visualization of money flows and connections between entities, d) SI*GIIF - a custom built application used mainly for monitoring of reporting entity registration, data acquisition and data entry in case management. Supporting applications, such as in house built MS Access and MS Excel, to ease database handling is also available.

445. The funds that are provided to the GIFI for the purpose of purchasing software and hardware, maintaining hardware, data security, training, international and internal relations and membership fees could be considered as adequate.

446. The Ministry of Internal Affairs, Ministry of Defence and the Internal Security Agency, may second any of their employees or officers to the Department. Detailed terms and conditions, including scope of duties, responsibilities and access to the information are set out in various regulations. Seconded employees are required to report to the Director of the Department and are subject to the same confidentiality obligations applicable to the permanent staff of the Department.

Integrity of FIU authorities (c.30.2)

447. The staff of the Department of Financial Information is selected according to Article 4 of the Law on Civil Service which stipulates that a person to be employed by the civil service has to fulfil the following prerequisites: a) be a Polish citizen, b) be to exercise the full scope of civil rights, c) not be convicted of an intentionally committed criminal offence prosecuted upon public accusations or a fiscal offence d) holds qualifications required for civil service, and e) enjoys an impeccable reputation.

448. All the officers of the Department possess higher education qualifications, are skilled and highly motivated. All staff members must be subject to a security clearance process.

449. The confidentiality rules of the AML/CFT Act apply to the GIFI and the employees and officers of the Department of Financial Information.

Training of FIU staff (c.30.3)

450. The employees of the Department are trained on a regular basis. According to the Polish authorities, constant vocational training of the staff has become a common practice especially focussing on skills related to the use of IT tools in the analysis of information and security of processed information. In addition, regular training in the area of AML/CFT risks and vulnerabilities, legal awareness and financial law is provided.

Table 17: Trainings and workshops attended by the GIFI staff

Trainings/workshops/seminars	number of participants	year (2009 - VI.2012)	Duration/days
Asian crime workshop - organised by the Police HQ, Warsaw	1	2009	1
Administrative Proceedings workshop - internal training by the MoF	5	2009	1
FIU.NET Workshop - the Hague - organised by FIU.NET Bureau;20 - 21.01.2009	1	2009	2

FIU.NET Workshop - Malta - organised by FIU.NET Bureau; 24 - 25.11.2009	1	2009	2
I-link workshop - Lyon -organised by INTERPOL	1	2009	2
Bulk Cash Smuggling and Anti-Money Laundering Financial Training Course – Warsaw 18 - 19.05.2009; organised by the US Treasury Department in cooperation with the GIFI	20	2009	2
Seminar on "Derivatives transactions in the OTC market. Currency options" - Warsaw, organised by Bank BPH	1	2009	2
Murmańsk Conference on money laundering and offenses related to the exploitation of natural resources (mainly illegal fishing and illegal logging) in the Baltic Sea region in the examples of criminal proceedings in different countries - Russian Federation/ Murmansk 24- 25.11.2009/ organised by Council of Europe with ROSFINMONITORING	1	2009	2
Basic course on AML/CFT for the Internal Security Agency officers / Warsaw	2	2009	1
Legalization of proceeds of crime from the GIFI perspective - principles, methods, forms and the scope of the exchange of information between the Internal Security Agency and GIFI, in operational and investigative frames - October 2009, Warsaw	2	2009	1
Legalization of proceeds of crime from the GIFI perspective - principles, methods, forms and the scope of the exchange of information between the Internal Security Agency and GIFI, in operational and investigative frames - December 2009, Warsaw	2	2009	1
Regional Conference on combating ML and TF; Warsaw, 22 - 23 . 06. 2013, organised by the US Treasury Department and GIFI	20	2009	2
London FIU.NET Workshop - London/ organised by the FIU.NET Bureau/26 - 28.10.2010	2	2010	2
Training in economic crime - Police Academy in Pila	1	2010	2
Workshops - Cooperation between Police and the banking sector in the prevention, disclosure and combating crime associated with the functioning of the banks, organized for the representatives of the Police and representatives of the banking sector - Police Academy in Szczytno and the Criminal Bureau of the National Police Headquarters	2	2010	2
Workshop on fight against drug-related crime - Police Academy in Pila and the Criminal Bureau of the National Police Headquarters	3	2010	2
Conference on the securing of the property - representatives of the Police Headquarters and the Regional Police Headquarters - exchange of information between GIFI and law enforcement authorities as a basis for further action to secure the proceeds of crime - Police School in Katowice	2	2010	2
Internship „ Combating Organised Crime, Corruption and Money Laundering" – Washington (USA) State Department and FINCEN- 14 - 27 June 2010	1	2010	14
Using the VIES VAT number validation service - VAT Carousel Fraud Missing trader	4	2011	
Practical application of the provisions of the Criminal Code and money laundering predicate offences-training/organised by the Training Centre of the MoF, Warsaw, 3-4.10.2011	50	2011	2

Electronic Assets Recovery System (ESOM) - Police Academy in Szczytno	2	2011	12
Workshop on Hemolia project - Bran (Romania), organised by the Romanian FIU and Hemolia Project	1	2011	2
Fundamentals of Crime Analysis - Internal Security Agency Otwock/Poland, 16 - 20.05.2011	10	2011	5
Financial Analysis Training (FAT) - EUROPOL, Hague, 12-23.09.2011	1	2011	10
„Europol Roadshow" Conference - Police Academy in Slupsk and Europol /Poland/ 29 -30.03. 2011	2	2011	2
EU-USA Workshop on CFT - Budapest (Hungary)/ 6 - 7.06.2011, organised by Hungarian MoF and USA	3	2011	2
Workshop on CFT - Chisinau (Moldova)/27 - 29.09.2011/ organised by OSCE	1	2011	2
EU-GCC Workshop on Combating Terrorist Financing - Warsaw , 22-23.11.2011, organised by MoF in cooperation with EC and GCC	12	2011	2
The methodology and tactics of conducting investigations of crimes unjust VAT refund in scrap metal and fuel cases, with particular emphasis on the principles of cooperation with the tax control authorities during the proceedings/ organised by the Training Center of the MoF, Warsaw	5	2011	2
International expert workshops on Areas of cooperation between law enforcement agencies and the private sector in dealing with organized crime, mainly of an economic nature"	3	2011	2
VII Conference "Law enforcement and government agencies cooperation in the protection of economic and financial interests of the Republic of Poland and the EU in the field of trade in liquid fuels" - the Police Academy in Szczytno	2	2011	2
Workshops for asset recovery coordinators - The Central Bureau of Investigation of the National Police Headquarters	2	2011	2
4th High-level Pan-European Conference on Asset Recovery Offices "Successfully tracing and identifying the proceeds of crime in Europe"/ Warsaw/ by Police HQrs	2	2011	2
OSCE conference on combating corruption and money laundering - Kyiv (Ukraine), organised by OSCE, 28-30.06.2011	2	2011	3
Third edition of the workshops "Cooperation of the Police and the banking sector in the prevention, disclosure and combating crime associated with the functioning of the banks "- the Police Academy in Szczytno and the Criminal Bureau of the National Police Headquarters	2	2011	2
Training in the scope of Act on payment services of 19 August 2011, organised by MoF, 17.02.2012	50	2012	1
E-learning course in AML/CFT	1	2012	14
VIES application/organised by the Training Center of the MoF, Warsaw	30	2012	1
VAT Carousel Fraud - internal training, Warsaw	12	2012	1
VAT Carousel Fraud - external training, Warsaw	15	2012	1
FIU.NET Workshop - Levi (Finaland), 20-21.03. 2012, organised by	2	2012	2

FIU.NET Bureau			
Workshops for judges, prosecutors and representatives of GIFI on the use of electronic banking services to commit crimes (Miedzeszyn/Poland), organised by the Police HQrs and Polish Banking Association/10 -11.01.2012	12	2012	2
Training in Polish accounting law and its practical application/organised by the Training Center of the MoF, Warsaw, March 2012	1	2012	1
Moneypenny Workshop/ organised by Swedish National Police and the Institute for Security and Development Policy (ISDP)/ 9 - 10.02.2012	2	2012	2
EU - USA Workshop on CFT - Copenhagen, 11 - 12.06.2012	1	2012	2

Recommendation 32 (FIU)

451. The FIU maintains the following statistics:

- Number of descriptive reports received by GIFI
- Sources of descriptive reports
- Division of descriptive reports from obligated institutions according to the types of OI
- Sources of STRs
- Number of transactions provided to GIFI in each month
- Division of number of transactions provided to GIFI
- The result of the carried out analytical proceedings (reports to the Public Prosecutor's Office on suspicion of money laundering, blockage of accounts, forwarding information on GIFI's own initiative
- Statistics of feedback received in connection with reports provided by GIFI to Public Prosecutor's Offices (information on indictments, information on charges made, information on judgments' passed, information on initiation of proceedings, information on orders to initiate proceedings, information on combining conducted proceedings with other proceedings, information on refusal to initiate preparatory proceedings, information on discontinuance of proceedings, information on reinitiation of previously discontinued proceedings, information on completion of proceedings (in one case it was indicated that the part of materials was separated for separate proceedings).
- Statistics on controls carried out by GIFI and supervisory institutions
- Statistics on requests from fiscal control authorities and fiscal authorities (directors of fiscal control Office, Department for Fiscal Control of the Ministry of Finance, directors of fiscal chambers, heads of tax Office, the Department of Treasury Intelligence of the Ministry of Finance, the Department of Tax Administration of the Ministry of Finance)
- requests from authorized representatives of authorities reporting to the Minister of the Interior and Administration:
- Central Bureau of Investigation of the Police Headquarters (KGP), Division for Fighting Organized Economic Crime; Criminal Office of KGP Division for Fighting Economic Crimes; Criminal Office of KGP Division for Assets Recovery; National Border Guard Headquarters
- Requests from the Head of the Internal Security Agency (including the Counter-Terrorist Centre)

- Requests from the Head of the Central Anticorruption Bureau
- Requests from the Head of the National Criminal Information Centre (Inquiries from
- GIFI to KCIK; Registration of entities by GIFI in KCIK; Inquiries from KCIK to GIFI)

Effectiveness and efficiency

452. The vast array of databases directly available to the GIFI constitutes an effective mechanism for the collection of information for analytical purposes. This ensures that the analysis of a case is conducted rapidly and without any undue hindrances. The analysis is also enhanced through the use of different analytical software available to the analysts.

453. The number of cases opened by the GIFI appears to have remained largely constant between 2007 and 2012. This indicates that irrespective of the number of reports submitted by reporting entities, the working capacity of the analytical units of the GIFI remains the same. This therefore raises questions as to the ability of the analytical units, as they are currently structured and staffed, to effectively manage the relatively large number of reports received on an annual basis. Indeed, this conclusion is backed up by the fact that a marked discrepancy between the number of reports received and the number of cases opened exists.

454. On a positive note, the number of notifications sent to law enforcement authorities and prosecutors has steadily increased over the years. This suggests an improvement in the handling of cases by the analytical units.

Table 18: Statistics on STRs/SARs received, cases opened, notifications disseminated and judicial proceedings

	Receipt of STRs/SARs			Cases opened by FIU			notifications to law enforcement/prosecutors			Judicial proceedings			
							ML		FT	Indictments		Convictions	
	ML	TF	Total	ML	TF	total	LEA	Prosecutors		ML	TF	ML	TF
2007	25,424	229	25,653	1,351	7	1,358	14	190	14	35	0	13	0
2008	19,008	34	19,042	1,234	8	1,242	84	246	15	35	0	13	0
2009	12,699	67	12,766	1,262	11	1,273	246	180	21	31	0	11	0
2010	17,289	65	17,354	1,243	19	1,262	420	120	30	27	0	9	0
2011	26,880	55	26,935	1,505	15	1,520	539	130	19	26	0	4	0
2012	8,351	8	8,359	361	-	361	223	43	-	-	-	-	0

Table 19: Number of STRs and SARs received by the GIFI

	Receipt of STRs			Receipt of SARs		
	ML	**TF**	**Total**	**ML**	**TF**	**Total**
2007	23,534	199	23,733	1,890	30	1,920
2008	17,214	13	17,227	1,794	21	1,815
2009	10,864	40	10,904	1,835	27	1,862
2010	15,341	16	15,357	1,948	49	1,997
2011	24,382	26	24,408	2,498	29	2,527
2012[27]	7,769	0	7,769	582	8	590

455. With respect to the analytical process, information about suspicious transactions or suspicious report (STRs/SARs) is reported to the GIFI in electronic or paper way. If the information is submitted in paper, it is immediately manually integrated to the electronic registers of the GIFI's database without delay and this process has a high priority - this is the main task of dedicated staff in a dedicated unit. Once data from SARs/STRs appear in electronic system they are immediately available for analytical processes beginning with the classification of suspicious information. Some automatic analytical processes within database allow to link the data from SARs/STRs with other available data.

456. Each case is subject to a "qualification" process (i.e. "initial analysis") which comprises two main components: comparing information received form obligated institution or cooperating unit with data available to the GIFI (e.g. on transactions, criminal and tax data) and filling the special form in which the individual circumstances of the transactions are assigned to a certain number of points. If total sum of assigned points exceeds a threshold the case gets "active" status. Otherwise it gets "passive" status, which means there is no additional analysis done unless a new piece of information is received that is related to that case. The results of a case qualification may be changed if there are some special circumstances that justify it. Each qualification is approved by Director or his/her deputy.

457. Active cases are sent to analysts from the Analytical Units. He/she may gather additional information and conclude the case by preparing a notification to a law enforcement authority due to a suspicion that analysed transactions are related to money laundering, terrorist financing, other criminal or treasury penal offence. GIFI may also send information on transactions to other authorities – please see article 33 of the AML/CFT Act. Once the notification has been send the case receives status: "done" until the eventual receipt of additional information. If analyst considers that the collected material does not justify the suspicion that transactions may be connected with criminal

[27] First quarter of 2012

activity, he/she may propose to change the case status to "passive". The proposal is approved by his/her direct superior.

458. The analytical procedure usually takes 12- month in order to analyse a case and to conclude it, with the possibility to extend this period by further 6 months in particular cases.

459. There is a special procedure, as far as it concerns SARs that are sent on the basis of article 16 of the AML/CFT Act, which contain information about transaction that is going to be executed. The subjects involved in transactions described in a SAR are checked whether they are listed in any cases analysed by the GIFI. If the transactions are related to those, which were previously analysed, the SAR is added to the existed case, otherwise a new case is created. Afterwards the obligated institution is informed about the fact that the GIFI received a SAR and on the exact time of its reception. Since then obligated institution is not allowed to execute the notified transaction within next 24 hours and the GIFI is entitled to suspend it or to block the account/accounts involved. The GIFI may demand a suspension of the transaction or blockage of an account for the time that does not exceed 72 hours, counting from the moment of the receipt of such demand by the obligated institution. If such decision is made, the GIFI shall inform the public prosecutor's office about the offence referred to in Article 165a or 299 of the Penal Code and provide it with evidence supporting such suspicion.

460. During the conducted analysis, analysts create files with findings (incl. breakdown of suspicious/untypical transactions, visualisation of financial flows or additional information). On that basis the intelligence is created in a digital form and/or in a paper.

461. The main software tools allow to extract information on transactions from the GIFI's database to excel sheets or present them in a graph form (graph with predefined links between selected objects in database). This kind of software is used by each analyst in everyday work and helps to draw conclusions about money flows, as well as about the transactions. The analysts also use a tool that helps them to export account statements received from obligated institutions into the excel sheet, if they are recorded in other formats (i.e. txt). Some automatic analytical processes within the GIFI's database (linking data from different transactions, linking data from transaction records with other registers or queries submitted to the FIU and classifying them - including analysis of names and sequences of transactions) as well as some reports (generated on regular basis or ad-hoc) are built within the framework of software.

462. After the analysis, an analyst proposes the dissemination of analytical information. The proposal is accepted firstly by the direct superior (Head of the Analytical Unit) and then is forwarded to the Director of the Department of Financial Information who takes the decision.

463. Sometimes, the superior (Head of the Analytical Unit or the Director of the Department of Financial Information) – after familiarisation with the results of analysis – directly decides on the dissemination of analytical information to the competent authority.

464. After the report is disseminated to the public prosecutor, he informs the GIFI on a decision made in this regard. The GIFI analyses the justifications of such decisions. In the case of the refusal of initiating criminal proceeding, the GIFI is entitled to lodge a complaint on the prosecutor's decision to a competent court. If a prosecutor decides to discontinue the investigation and if the GIFI has doubts whether the public prosecutor performs all necessary actions the GIFI informs the Office of the General Prosecutor on such case. Last year the General Prosecutor – on the basis of the information received from the FIU – sent some guidelines to the regional public prosecutor's offices concerning conducting criminal proceeding on the basis of the reports received from the GIFI.

465. In case of the notifications sent to the Police or other LEAs the addressee often informs of its interest to cooperate with the GIFI by investigation in order to freeze money stemming from an illegal activity.

466. On regular basis statistical information from the Office of the General Prosecutor is provided to and analysed by the GIFI (information on numbers of investigation, prosecutions, convictions for

ML/TF etc.). Information from Public Prosecutor's Offices about results of single investigations is integrated to the FIU's database when available.

467. Based on the comments made to the evaluators by law enforcement authorities during the on-site visit, it appears that the analytical output of the GIFI is not routinely used as a basis for the initiation of an investigation. Law enforcement authorities perceive the GIFI mainly as a source of financial information, especially bank account information.

2.5.2 Recommendations and comments

Recommendation 26

468. The GIFI is encouraged to review the AML/CFT Act to address a number of remaining technical shortcomings related to Recommendation 26. In particular, the AML/CFT Act should clearly provide for the manner in which the functions and responsibilities of the General Inspector are to be delegated to the Department on Financial Information.

469. The Guidance on the manner of reporting should be brought in line with the amended AML/CFT Act. Among other things, the guidance should expressly include a reference to the reporting of FT transactions and reporting under Articles 16 and 17.

470. Although the GIFI regularly disseminates analytical reports to competent authorities (other than the public prosecutor), the legal basis for this procedure appears to be rather ambiguous. A clear provision dealing with this issue should be included in the AML/CFT Act.

471. The General Inspector should be required to maintain confidential any information received in the performance of his functions following the termination of his appointment.

Recommendation 30

472. The Polish authorities should consider allocating further resources to the analytical units of the Department of Financial Information of the GIFI.

Recommendation 32

473. The GIFI should maintain relevant statistics on requests made to obligated institutions according to Article 13a of the AML/CFT Act.

2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	**LC**	• Out-dated guidance on the manner of reporting; • There are no provisions to ensure that the General Inspector maintains confidential any information received in the performance of his functions following the termination of his appointment.

2.6 Law enforcement, prosecution and other competent authorities - the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27)

2.6.1 Description and analysis

Recommendation 27 (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

474. Poland was rated 'Partially Compliant' in respect of Recommendation 27 in the 3rd round evaluation report due to the fact that not enough emphasis was placed on police-generated money laundering cases and the proactive approach on investigations in major proceeds-generating cases was insufficient.

Establishment of designated law enforcement authorities responsible for ML and FT investigations (c.27.1)

475. In Poland the authority responsible for ensuring that ML and TF offences are properly investigated is the Department for Organised Crime and Corruption of the Office of the Prosecutor General. The Department monitors and supervises proceedings related to money laundering and terrorist financing. It also instructs the prosecutors on the direction of investigations, if necessary.

476. The LE bodies which are responsible for ML investigations within the Police are the Economic Crime Department of all regional (Voivodship) and Municipal headquarters, including the Central Bureau of Investigations and the Criminal Investigation Bureau. There is no specialised division within the Police which conducts ML investigations. However, financial investigations are an integral part of on-going police cases, in particular those concerning serious and organised crimes.

477. In addition, the Anti-corruption Bureau was created as a specialised authority to combat corruption in public and economic life, particularly in public and local government institutions, as well as to combat activities which are detrimental to the State's economic interests. The Anti-corruption Bureau is empowered to conduct ML/FT investigations which are related to corruption.

478. According to the Polish authorities the Border Guard is not directly empowered to investigate the ML cases. Nevertheless, ML falls under the scope of operational enquiries of the Border Guard and as a result it can open preparatory proceedings together with proceedings for the underlying offence, which falls within the competence of Border Guard. In September 2009, a concept note ("Pursuing operations with regard to defining the assets deriving from illegal or undisclosed resources by Border Guard officers") was issued by the Deputy Head of the Border Guard. This concept note provides guidance on gathering and completing operational documentation, which is used after validation, as procedural documentation, indicating the evidence of proceeds from crime, falling within the scope of statutory competences of Border Guard.

479. In all 17 regions (voidvodeship) Police Headquarters Asset Recovery Teams have been established. The head of the team is the regional asset recovery coordinator. Each team consists of 3-7 employees. Moreover, there is a coordinator in every division of the Central Bureau of investigation. The main task of these teams is tracing the assets in the most complex cases, assisting other financial investigators, supervising asset-tracing tasks performed in local police units, controlling the accuracy of statistics and delivering local training on asset recovery.

480. With respect to the Customs Service, there are separate investigation units in all customs offices and penal and fiscal units in all customs chambers, dealing mainly with financial crime and investigation in financial cases (penal and fiscal cases). The specialised personnel dealing with financial crime and investigation amounts to 474 officers.

481. The Fiscal authority receives numerous disseminations from the GIFI. According to the information provided by the Polish authorities the Fiscal authority sent to the public prosecutor 9

notifications in 2009, 8 in 2010 and 6 in 2011. It seems that only few cases are sent by the Fiscal authority to the criminal prosecutor on the basis of a dissemination from the GIFI considering a large number of reports sent to the Fiscal authorities by the GIFI.

TF investigations

482. Within the Police there are special organisational units that perform tasks with regard to identifying, counteracting and responding to terrorist crimes, such as, within Central Bureau of Investigation of the National Police Headquarters, Department of Terror Act responsible for terrorist crimes. Since 2008 police officers perform their tasks by working in the Counter-Terrorist Centre of the Internal Security Agency.

483. The Internal security agency carries out its tasks according to the Article 5 of The Internal Security Agency and Foreign Intelligence Agency Act of 24 May 2002) (an obligation to safeguard the internal security and constitutional order of the Republic of Poland). It fulfils the following functions: reporting-analysis, operational investigations, criminal investigations, as well as state protection.

Competent authorities investigating ML cases possibility to postpone or waive the arrest of suspected persons and/or the seizure of the money (c.27.2)

484. The Polish Penal Procedure Code does not contain any specific provisions on the postponement or waiver of the arrest of suspected persons. However, in the course of proceedings, an order for the arrest of a person is issued at the discretion of the prosecutor in charge of the case. If the prosecutor wishes to postpone or waive the arrest there is nothing which precludes him from doing so.

485. Measures for postponing or waiving the seizure of money for the purpose of identifying persons involved in such activities or for evidence gathering are covered by the Art 217[28] of the Code of Criminal procedure.

Additional elements (c.27.3)

486. Money laundering and terrorist financing offences are not on the list of offences for which special investigative techniques, such as wiretapping, surveillance and recording of the content of other conversations or information transmissions, can be applied in an investigation. Once an investigation commences, the court, acting in accordance with Article 237 § 1 of the Penal Procedure Code, upon a motion from the state prosecutor, may order the surveillance and recording of the content of telephone conversations in order to detect and obtain evidence for pending proceedings or to prevent a new offence from being committed. Telephone tapping, as well as surveillance and recording of the content of other conversations or information transmissions, including correspondence transmitted by electronic mail (Article 241) can be applied in an investigation that concerns one of the listed offences (Article 237 § 3).

[28]Article 217 § 1. Objects which may serve as evidence, or be subject to seizure in order to secure penalties regarding property, penal measures involving property or claims to redress damage, should be surrendered when so required by the court, the state prosecutor, and in cases not amenable to delay, by the Police or other authorised agency.

§ 2. A person holding the objects subject to surrender shall be called upon to release them voluntarily.

§ 3. In the event of a seizure of objects, provision of Article 228 shall apply accordingly. A record need not be written if the object is appended to the files of the case.

§ 4. If the surrender is demanded by the Police or any other authorised agency acting within its scope of competence, the person surrendering the objects has the right to file a motion without delay for the drawing up and serving him an order of the court or of the state prosecutor authorising the action. The person surrendering the objects shall be instructed about this right. The person shall be served, within 14 days of the seizure of the objects, an order of the court or the state prosecutor authorising the action.

§ 5. In the event of refusal of a voluntary surrender of objects, a seizure may be effected. Provisions of Article 220 § 3 and Article 229 shall apply accordingly.

487. According to Article 237 § 3 the surveillance and recording of the content of telephone conversations is allowed only when proceedings are pending or a justified concern exists about the possibility of a new offence being committed regarding:

(1) homicide,

(2) being a danger to the public or causing a catastrophe,

(3) trade in humans or white slavery,

(4) the abduction of a person,

(5) the demanding of a ransom,

(6) the hijacking of an aircraft or a vessel,

(7) robbery, robbery with violence, or extortion with violence.

(8) an attempt against the sovereignty or independence of the State,

(9) an attempt against the constitutional order of the State or on its supreme agencies, or against a unit of the Armed Forces of the Republic of Poland,

(10) spying or disclosing a State secret,

(11) amassing weapons, explosives or radioactive materials,

(12) the forging of money, or effecting of transactions involving counterfeit money, including the means or instruments of payment, or transferable documents which entitle one to obtain an amount of money, goods, consignment or a material object, or such documents containing the obligation to pay in capital, interest, a share in profits or that contain a declaration of participation in profit,

(13) producing, processing, effecting transactions, or smuggling narcotic drugs, substitutes thereof, or psychotropic substances,

(14) organised crime group,

(15) property of significant value,

(16) the use of violence or unlawful threats in connection with criminal proceedings,

(17) bribery and influence trading,

(18) pandering or obtaining profits from facilitating and protecting prostitution

488. A variety of special investigation techniques can be used with regards to ML in the course of a preliminary investigation. With respect to TF, the only body that is authorised to use special investigation techniques in preliminary investigations is the Internal Security Agency.

489. The CBA and the Internal Security Agency are authorised to use special investigative techniques according to their sectoral laws. Nevertheless, there is a provision in CBA Act that limits the use of special investigative techniques for ML to those cases where prosecuted offences are connected to corruption or an offence against State Treasury exceeding 200,000PLN (€50,000). According to the Polish authorities, the Police can use special techniques pursuant to Article 19 of the Police Act. In addition, pursuant to Article 20 of the Act on Police, in money laundering cases the police has access to information covered by bank and insurance secrecy. All mentioned methods and techniques from Articles 19 and 20 may be used only with consent and control of the district court.

490. Lack of access to fiscal and tax secrecy in the intelligence phase is a problem according to the police authorities. According to the Police authorities, amendments to the Act on Police that would

enable the Police to have access to banking and insurance data were not resumed by the new elected Parliament. Additionally, the Police is not granted access to the registry of central bank accounts[29].

Additional elements (c.27.4)

491. In proceedings concerning money laundering the most common special technique is telephone tapping.

492. Police can use special techniques pursuant to the Act on Police such as wiretapping, control of correspondence, controlled purchase, controlled delivery, undercover operations, and controlled payment of bribes in the case of money laundering offenses.

493. The Central Anti-Corruption Bureau (CBA) applies special investigative techniques mentioned *inter alia* in article 50 of the UN Convention against corruption (UNCAC) or in Article 20 of the UN Convention against transnational organised crime. These techniques are applied for the purpose of identifying, preventing and detecting criminal offences, and also for evidence-gathering and preserving in crimes:

a) ML - based on Article 17Law on the CBA (Dz.U.2006.104.708), CBA applies operational control, in order to identify, prevent and detect offences in the field of Article 299 PPC (Polish Penal Code - money laundering);

b) ML - based on Article 19Law on the CBA, the CBA applies controlled delivery mentioned in Article 2 (i) UNCAC, and also applies controlled active and passive bribery, in order to verify the previously obtained information and to investigate and detect perpetrators and evidence-gathering.

c) FT - in extent referred to Article 165a PPC (FT) – CBA bases upon Article 13 and Article 14 Law on the CBA, the service takes all other means: operational, investigational techniques and analytical, information techniques as well, including observing and registering public places using technical support to collect picture and sound accompanying the criminal events.

494. These activities may take place with the participation of CBA officer, and/or person giving CBA help (participating) upon Article 25 Law on the CBA.

495. The use of special investigative techniques by the CBA in the ML is allowed, if prosecuted offences remain in connection with corruption or action against of the State-Treasury sized over 200.000 PLN – about 50.000 Euro (Article 2.1.(b)Law on the CBA).

496. In accordance with Article 2.3.Law on the CBA, the service may conduct investigations including all criminal acts disclosed during its course, if are connecting as subject matter or object matter with the act which constitutes the basis for initiation of investigation - therefore the acts constituting offences underlying of ML and FT offences.

Additional elements (c.27.5)

497. Although permanent or temporary groups specialized in investigating the proceeds of crime do not exist, for the purpose of disclosure the proceeds of crime and subsequent seizure thereof, Prosecutor's Offices as well as the Police co-operate with Revenue Services. Furthermore, when there is a need of cooperation between several institutions (Internal Security Agency, Central Anticorruption Bureau, Border Guard, Customs) coordination teams are appointed by the chiefs of these services. Also, the Commander-in-chief, the Regional Police Chief Inspector or the Head of the Central Bureau of Investigation, appoint an investigation team consisting in police officers from different units.

[29] According to Police authorities, there is work in progress on establishing register of central bank accounts.

498. According to the Police authorities they have satisfactory cooperation with other law enforcement bodies such as the FIU and the Tax Office.

499. Regarding co-operative investigation with appropriate competent authorities in other countries the Penal Procedure Code in part concerning judicial co-operation has been supplemented with provisions addressing Joint Investigative teams. In accordance with Polish law, the prosecutor is responsible to appoint a joint investigative team.

Additional elements (c.27.6)

500. In accordance with Polish law, the GIFI analyses ML/FT trends. For the purpose of producing its annual report, the GIFI uses information received from the Police. Additionally, analysis is conducted by the Criminal Intelligence Bureau of National Police Headquarters. This analysis is limited mainly to statistics and description of particular cases.

Recommendation 30 (law enforcement)

Adequacy of resources to law enforcement and prosecution (c.30.1)

501. Law enforcement bodies and prosecution authorities appear to have adequate human and technical resources. There are approximately 100,000 police officers in Poland, including 32,500 in criminal service, of whom 3,500 deal with economic crime within separate structures of the Economic Crime Departments (including the Central Bureau of Investigation). The Central Bureau of Investigation (CBI) of the National Police Headquarters in Warsaw is a specialised police unit dedicated to combating organised crime and employs approximately 2,050 officers, 300 of whom are directly involved in combating only economic serious and organized crimes. The Police has been experiencing problems with maintaining experienced and specially-trained officers on board since they often seek better positions within the private sector.

502. In the Economic Crime Departments of the 17 Regional (voivodeship) Police Headquarters approximately, 800 police officers deal with serious economic crimes. Other officers (2,400) in the District Police Headquarters are involved in less complex cases.

503. The National ARO was established within the National Police Headquarters in 2008. This is complemented by asset recovery teams in all Police Headquarters situated in the 17 regions. The head of the team is the regional asset recovery coordinator. The team generally consists of 3-7 officers. Moreover, a coordinator is appointed in every division of the Central Bureau of Investigation. The main task of these teams is to trace assets in the most complex cases, assisting other financial investigators, supervising asset tracing tasks performed in local police units, controlling the accuracy of statistics and delivering training on asset recovery.

504. According to the Annual Report of the Prosecutor General for 2011, there are 6,295 prosecutors in service. Since no specialised units exist within the prosecution service, all the prosecutors conduct ML/FT investigations.

Integrity of law enforcement authorities (c.30.2)

505. The officers of competent authorities maintain high professional standards, including standards concerning confidentiality and integrity. They are appropriately skilled. Integrity standards to be followed are set out in sectoral laws prescribing legal conditions for employment.

506. High professional standards for prosecutors are guaranteed by the provisions of an Act of 20 June 1985 on Prosecution Service. Pursuant to Article 14 § 1 of the Act, *for the post of a public prosecutor can be appointed only a person who:*

- *is of a Polish nationality and enjoys full civil and citizen rights*
- *has an impeccable character*
- *graduated from law studies at a university level in Poland and obtained Master's Degree or from foreign studies recognized in Poland*

- *is able, considering his health, to fulfil duties of public prosecutor*
- *is above 26 years old*
- *passed a prosecutor's or judge's exam*
- *worked as an assistant prosecutor or an assistant judge at least for one year, or served in military organizational entities of public prosecutor's office a military service term foreseen in the regulations on a military service of professional soldiers.*

507. The issue of confidentiality is addressed by Article 48 of the Act on Prosecution:

> *Article 48.1.Prosecutor is obliged to keep secret case circumstances, which he got to know due to his official post in the course of investigation and also beyond the open court case.*
>
> *2. The obligation to keep secret lasts even after the official employment relationship ceased.*
>
> *3. The obligation to keep secret ceases, when prosecutor testifies in preparatory proceedings or before the court, unless the disclosure of a secret threatens the State or such important private interest, which is not contradictory to the aims of administration of justice. In such cases, Prosecutor General may exempt prosecutor from keeping a secret.*

508. According to the Act on the Police there are several obligations that each police officer dealing with ML and FT has to fulfil e.g. have full public rights, not have received a conviction and have appropriate education, among others.

509. The Central Anti-Corruption Bureau (CBA): High standards are ensured, inter alia, by Article 48 Law on the CBA, which requires officers:

- to have full public rights;
- show unblemished moral, civic and patriotic attitude;
- not be convicted of intentionally committed criminal offence prosecuted upon public accusations or criminal tax;
- provide a warrant of secrecy pursuant to the requirements laid down in the provisions of Law of Poland on the protection of classified information;
- have at least secondary education and professional competence, physical and psychological ability to serve;
- not have worked and not have been co-workers in organs of State security, listed in the Law on the Institute of National Remembrance -Commission for prosecution of crimes against the Polish nation (IPN).

510. The CBA primarily appoints citizens experienced in other State bodies, such as the Agency of Internal Security, Police or Border Guard officers.

511. In addition, officers of the CBA serve under an oath of faith to the state, the constitutional authorities of the Polish Republic, undertake to comply with the law, diligent performance of their duties, even with risk of life, guard of honour, dignity, good name of service, discipline and professional ethics.

512. Officers must obtain security clearance for access to classified information under Article 48 of the Law of the CBA.

513. According to the Internal Security Agency and Foreign Intelligence Agency Act, only a Polish citizen enjoying full public rights may serve in the ABW. Such a person has to be characterized by flawless moral, ethical and patriotic conduct.

Training of law enforcement staff (c.30.3)

514. The representatives of the GIFI as trainers participate every year in seminars, trainings and meetings organised by the law enforcement agencies dedicated to counteracting and fighting against financial crimes (inter alia ML and TF). In 2011, seminars, trainings and meetings were related to the

following areas: cooperation of the Police and financial institutions in the field of prevention, detection and combating crimes related to the banking, cooperation of the Police and the FIU by the asset recovery, cooperation of the Border Guards and the FIU in the field of combating criminality, cooperation of the Police and the FIU in the fight against financial crime to the detriment of the State Treasury or the EU, combating crimes committed by the Asian organised groups.

515. The National School of Judiciary and Public Prosecution, which was established on the basis of the Act of 23 January 2009, is the central institution responsible for providing the initial and continuous training for the officials of the common courts of law and the public prosecutor's office in Poland.

516. Issues of ML and FT are addressed in the course of training for prosecutors. From 2009 to 2011 a number of trainings for prosecutors and judges took place and encompassed a variety of topics linked with predicate offences for ML, seizure of property, etc.:

2009:

- Methodology of conducting investigation concerning economic crime. (60 prosecutors attended the training)
- Stock market criminality - methodology of conducting investigation. (60 prosecutors attended the training)
- Offences committed by means of computer systems - methodology of conducting investigation (60 prosecutors attended the training)
- Practical aspects of seizure and forfeiture of property. (120 prosecutors attended the training)
- Specialized training on money laundering investigation (latest typology, autonomous prosecution, seizure of property) for prosecutors dealing with organized crime (100 prosecutors attended the training)

2010:

- Practical aspects of seizure and forfeiture of property (50 prosecutors attended the training)
- Offences committed by means of computer systems - methodology of conducting investigation (50 prosecutors attended the training)
- Forensic software – electronic evidence in criminal investigation. (50 prosecutors attended the training)
- Forensic analysis in criminal investigation. (50 prosecutors attended the training)
- International co-operation in criminal investigation, European Arrest Warrant and Schengen Information System (50 prosecutors attended the training)
- Fiscal offences - methodology of conducting investigations. (50 prosecutors attended the training)
- Amendments to the penal code and penal procedure code (including amendment of the ML offence and introduction of the terrorist financing offence) (100 prosecutors attended the training)

2011:

- Economic crime – selected topics (50 prosecutors attended the training)

517. In 2009-2010 the Prosecutor General's Office also cooperated with Warsaw School of Economics and organized seminars on money laundering (including issues of autonomous prosecution, latest typology and seizure of property) within the framework of post-graduate studies for judges and prosecutors.

518. According to the Polish authorities police officers and civilians working in departments and units dedicated to economic and financial crime within Police structures, undergo various specialised training according to the assigned tasks to extend their competences in area of money laundering, economic fraud, tax and customs crimes etc. There is constant participation in courses of

representatives from other LEA Border Guard, internal Security Agency, Customs Service, Tax Service, Central Anti-corruption Bureau, Prosecutors and Polish FIU. During trainings performed by ARO at a local level in 2009- 600 police officers were trained, in 2010-700 officers, in 2011-1000 officers were trained. In 2012, only 200 officers were trained due to Euro 2012 Tournament.

519. Since the 3rd round, there seems to have been more activities with regard to training law enforcement bodies, in particular Police. As per prosecution it seems from the available information on training that significant portion of prosecutors is not educated in the area of ML/TF. Also, it is unclear what portion of employees of other LEA benefited from trainings.

Effectiveness and efficiency

520. Since the 3rd round mutual evaluation, the Police, including the Central Bureau of Investigation, have taken further steps to initiate more ML investigations in major proceeds-generating cases. The Police keep statistics on initiated cases in accordance with Art 299 of the Penal code and on cases forwarded to the prosecutors' office. Statistics on the breakdown of predicate offences are not kept by the Police. Also, there is no evidence of 3rd party/autonomous ML cases being generated on the initiative of the police.

521. The Police was the only LEA authority that made available statistics with regard to ML investigations. This raises concern in relation to ML investigations carried out by other LEAs, in particular insofar as the fiscal authority is concerned, since it receives a significant amount of notifications from the GIFI. Since the 3rd round, the police authorities have increased their efforts in generating ML investigations and conduct parallel financial investigations.

Table 20. Statistics on initiated cases of money laundering resulting in prosecutions:

Year	Total number of initiated cases of ML	On own initiative	Resulting in prosecution
2009	164	13	54
2010	133	8	89
2011	134	12	67

522. According to the above Table, in 2009 the Police initiated 164 cases of ML, 33 % of which resulted in prosecution. In 2010, almost 67% of initiated cases resulted in prosecution. In 2011, the figures were slightly lower, where every other case of ML resulted in prosecution. ML cases initiated on the initiative of the police amounts to less than 10% of the overall number of ML investigations.

Table 21. Identified ML offences – number of persons:

Year	No. of identified ML offences (persons)
2009	284
2010	311
2011	339

523. With regard to number of persons in cases of ML investigated by Police, steady growth is observed from 2009 to 2011.

Table 22. Overall statistics on investigations, prosecutions and convictions for ML

Year	Investigations Number of all on - going investigations		Investigations commenced in a given year (these numbers are included in the total number of investigations and persons in the columns on the left		Prosecutions		Convictions	
	Cases	Persons	Cases	Persons	cases	Persons	Cases	Persons
2007	645	1436	296	Data not collected in 2007	82	288	36	55
2008	741	1626	284	254	74	324	27	53
2009	796	1753	235	192	65	360	18	41
2010	866	1726	223	154	74	308	21	45
2011	754	1968	192	254	71	290	19	47

524. From 2007 to 2011, a negative trend has been observed in the number of cases that were investigated (new cases commenced), prosecuted and convicted. On the other hand, the number of investigated persons raised from 154 in 2010 to 254 in 2011. Number of prosecuted persons is slightly declining, but, in general, number of convicted persons remains approximately the same.

525. Apart from the Police and the GIFI, other law enforcement bodies, seem not to keep detailed statistics related to ML/FT, such as statistics on predicate offences, on parallel ML investigation etc.

2.6.2 Recommendations and comments

526. At the time of the third round evaluation, the evaluators concluded that the pro-active approach by law enforcement authorities to ML/FT investigations was limited. During the fourth round the evaluators noted that the situation did not improve significantly, as is demonstrated by the statistics provided by the authorities. Since no indication was provided on the extent of proceeds-generating crime investigations, the evaluators were not in a position to conclude whether the police are proactively conducting financial investigations in relation to such crimes.

Recommendation 27

527. More emphasis should be placed on ML investigations by LEA in major proceeds-generating cases.

528. ML and TF offences should be on the list of offences for which special investigative techniques can be applied in the investigation.

529. LEA should be sufficiently proactive in ML investigations.

Recommendation 30

530. More continuous specialised training for law enforcement bodies and prosecution authorities in the area of combating ML/FT should be provided.

Recommendation 32

531. More detailed statistics are required to demonstrate the effectiveness of the AML/CFT regime overall.

2.6.3 Compliance with Recommendation 27

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	**PC**	**Effectiveness:** • Over focus on fiscal ML cases; • Low number of ML investigations by LEA in major proceeds-generating cases; • Insufficiently proactive approach by LEA in ML investigations; • Insufficient utilisation of FIU information by LEAs.

3. PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

Legal framework and developments since the third evaluation

532. Since the adoption of the third mutual evaluation report in June 2007, Poland has taken several legislative and regulatory measures in order to address the main deficiencies identified in the third round evaluation. These developments are set out in detail under the description of each of the relevant recommendations.

Law, regulations and other enforceable means

533. Poland has a broadly sound legal structure for the preventive standards. As indicated earlier, the main relevant texts are the AML/CFT Act (2000 and 2010), which applies to any person or entity subject to the AML/CFT requirements, the Banking Act (1997 and 2011), Act on Insurance Activity, Act on Trading in Financial Instruments, Act on Financial Market Supervision, Act on Investment Funds and Act on Payment Services. A more detailed description of the legal framework is set out in Section 1.1 above.

Scope

534. Pursuant to Article 2 (1) of the AML/CFT Act, obligated institutions include:

a) branches of a credit institution;
b) any financial institution having its registered office in the territory of Poland and branches of financial institutions not having their registered office in Poland;
c) national banks and branches of foreign banks;
d) the National Bank of Poland - relating to the maintenance of bank accounts for legal entities, sale of coins, banknotes and numismatic items for collection and other purposes, gold buying and exchange of damaged legal tender;
e) electronic money institutions, branches of foreign electronic money institutions and any clearing agent operating under the Act of 12 September 2002 on electronic payment instruments;
f) investment companies, custodian banks;
g) foreign legal entities carrying out brokerage activities and commodity brokerage houses in the territory of Poland;
h) the National Depository for Securities S.A. – in so far as the maintenance of securities accounts or omnibus accounts is concerned;
i) insurance companies carrying on life insurance;
j) investment funds, investment fund management companies;
k) cooperative savings and credit unions;
l) the Polish Post;
m) entities providing currency exchange operations;
n) payment institutions, branches of EU payment institutions, agencies of payment institutions and their agents.

535. Accordingly, the AML/CFT Act applies to all activities and operations defined in the Glossary to the FATF Methodology in relation to financial institutions.

Customer Due Diligence and Record Keeping

3.1 Risk of money laundering / financing of terrorism

536. The Act of 25 June 2009, which amends the AML/CFT Act, was enacted to transpose the Third AML Directive (Directive 2005/60/EC) and the Implementation Directive (Directive 2005/70/EC) into Polish legislation and to address a number of recommendations made in the 3rd Mutual Evaluation Report.

537. The exceptions for simplified CDD reproduce the provisions laid down in the 3rd AML Directive. The AML/CFT Act states that reduced CDD measures may be applied, *inter alia*, to clients and institutions from the EU or equivalent countries. The list of equivalent third countries was established in a regulation issued by the Minister competent for Financial Institutions on 20 October 2009. The AML/CFT Act provides an exhaustive list of situations where reduced CDD measures may be applied.

538. The AML/CFT Act also provides a list of categories of clients and transactions in relation to which certain high-risk measures must be applied. Financial institutions may expand this list on the basis of their own risk-management policies and procedures.

539. Furthermore, since the 3rd round evaluation, the risk-based approach has been introduced within the Polish AML/CFT regime. This means that financial institutions may allocate resources and calibrate the application of customer due diligence measures in accordance with the ML/FT risks posed by a particular transaction or client.

540. Limited information was provided on the ML/FT risks in Poland since no formal risk assessment was carried out by the Polish authorities. During the on-site visit, it was pointed out that the threat of terrorism is low in Poland since there have been no terrorist attacks in recent history. Nonetheless, the number of TF STRs received by the GIFI is relatively high. Since 2007 60 TF reports were submitted to the Internal Security Agency. The Polish authorities informed the evaluation team that there were no indictments or convictions because the Internal Security Agency probably didn't confirm that the received TF transactions were actually related to TF.

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to R.8)

3.2.1 Description and analysis

Recommendation 5 (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

541. In the 3rd round evaluation, Poland received a 'Non-Compliant' rating for Recommendation 5. The rating was based on the following deficiencies:

(a) the absence of the requirement to identify a customer when establishing a business relationship, when carrying out wire transfers that fall within the definition of an occasional transaction (Interpretative Note to SR VII), when the financial institution has doubts about the veracity or adequacy of previously obtained identification data and in the case of threshold transactions of electronic money institutions' customers;

(b) the absence of the requirement for the identification of the ultimate beneficiary owner;

(c) the absence of the requirement to conduct on-going monitoring and enhanced CDD;

(d) the absence of the requirement to obtain information on the purpose and nature of a business relationship;

(e) the absence of the requirement not to open accounts when satisfactory CDD cannot be completed and to terminate the relationship when the financial institution is unable to comply with CDD obligations.

542. Most of these issues were addressed to some extent with the enactment of the AML/CFT Act of 2009.

Anonymous accounts and accounts in fictitious names (c.5.1)

543. Article 19 of the Act of 25 June 2009 contains the following provision:

" 1. Any contracts allowing anonymous accounts to be kept shall be deemed null and void by law after 12 months of this act entering into force.

2. The obliged institutions shall immediately take actions to identify such account holders and to inform them of the provisions of paragraph 1.

3. In cases stated in paragraph 1, the funds shall be deposited in a separate non-interest account."

544. The Polish authorities informed the evaluators that any funds deposited in the separate non-interest account referred to in Article 19(3) can only be withdrawn after full CDD measures are conducted on the account holder. However, this is not expressly stated in the law. Furthermore, although Article 19 covers anonymous accounts which existed prior to the coming into force of the Act of 25 June 2009, it is debatable whether the provisions of this article also extend to the opening of new anonymous accounts.

545. The Polish authorities consider this last issue to be covered by Article 8b paragraphs (1) and (3) of the AML/CFT Act, which require financial institutions to apply financial security measures to their clients, consisting of, inter alia, client identification and verification of identity on the basis of documents or information publicly available.

546. Furthermore, according to Article 9g of the AML/CFT Act,

Any obligated institutions shall apply appropriate measures of financial security in order to prevent money laundering or terrorist financing, which may arise from products or transactions allowing to maintain anonymity.

547. Polish legislation does not make explicit reference to accounts in fictitious names. However, according to the Polish authorities, the provisions contained in the AML/CFT Act do not allow financial institutions to provide services and products without verifying the identity of the clients.

548. The Polish authorities informed the evaluators that, prior to the coming into force of the Act of 25 June 2009, there were 3225 anonymous accounts with a total value of approximately €4.5 million. Currently there are no new anonymous accounts in Poland. This was confirmed in the course of AML/CFT inspections carried out by the supervisory authorities.

Customer due diligence

When CDD is required (c.5.2)*

549. CDD requirements are governed by Article 8b (4) of the AML/CFT Act which requires financial institutions to conduct CDD, in particular, when:

- *concluding*[30] *a contract with a client;*
- *carrying out transactions with a client with whom the obligated institution has not previously concluded any agreements of the equivalent of more than EUR 15,000, regardless of whether the transaction is carried out as a single operation or as several operations if the circumstances indicate that they are linked;*
- *there is a suspicion of money laundering or terrorist financing regardless of the value of such a transaction, its organisational form and the type of a client;*
- *there are doubts raised that the previously received data referred to in Article 9 are authentic and complete.*

[30] In the view of the Polish authorities concluding a contract should be understood as establishing a business relationship.

550. The Polish authorities consider that signing a contract with a client is mandatory for establishing a business relationship. Therefore, although there is no definition of "contract" in the AML/CFT Act, the evaluators concluded that CDD is to be carried out whenever a business relationship is established in line with criterion 5.2.

551. In addition, one of the requirements, when the CDD measures should be conducted, *there are doubts raised that the previously received data referred to in Article 9 are authentic and complete* raised some concerns. In this respect, the Polish authorities additionally informed the evaluation team that if data gathered during the identification process are not authentic and complete there are naturally doubts to the veracity and adequacy of that data. Not authentic and not complete data are either incorrect or inadequate. In this respect one phrase does not exclude the other, and this is merely the issue of understanding and implementing the standard. The evaluators agreed with the argumentation provided by the Polish authorities.

552. The AML/CFT Act does not require financial institutions to apply CDD measures in relation to wire transfers amounting to €1, 000 or more, as referred to under Special Recommendation VII. Nevertheless, financial institutions in Poland are subject to the provisions of Regulation 1781/2006 of the European Parliament and of the Council of 15 November 2006, on information on the payer accompanying transfers of funds, which is directly applicable in Poland subject to the derogation in Article 10c of the AML/CFT Act. Thus, although there is no requirement to conduct full CDD in relation to wire transfers equal to or exceeding €1,000, the identification and verification of identity of a client are required in terms of Regulation 1781/2006.

Identification measures and verification sources (c.5.3)*

553. As mentioned above, in terms of paragraphs (1) and (3) of Article 8b, financial institutions are required to identify their clients and verify their identity on the basis of publicly-available documents or information. The requirement to verify identity on the basis of documents or information which are publicly available falls short of the requirement under criterion 5.3 which refers to reliable, independent source documents, data or information. On the basis of the current provision, financial institutions may verify the identity of a customer by using publicly-available information which is not obtained from a reliable and independent source.

554. However the Polish authorities believe that the information obtained from "publicly available sources" does not exclude this information being reliable. The idea behind stating in the legislation that the verification of identification should be done from "publicly available sources" was that FI's can find in the public domain also the polish court register, which is reliable information. Nonetheless the evaluation team did not except the Polish argumentation, since it is not supported by any other legislation or other enforceable means.

555. Article 9 (1) of the AML/CFT Act clearly specifies the identification data that should be collected for clients. In particular Article 9(1) states the following:

a) *in case of natural persons and their representatives: determination and recording of the features of such a document confirming on the basis of separate provisions the identity of the person: the first and last name, nationality and address of the person performing the transaction; furthermore, his/her PESEL[31]; or, if the person has no PESEL number, his/her date of birth or the number of an identity document confirming the identity of an alien, or a country code if it was a passport presented;*

b) *in case of a legal entity: recording of current data from the extract of the Court Register or another document indicating the (company's) name and organisational form of such a legal entity, its registered office and address, its tax identification number along with the*

[31] PESEL (Polish Universal Electronic System for Registration of the Population) is the national identification number used in Poland since 1979.

first and last name and the PESEL number of the person representing this legal entity - or in the case of a person with no PESEL number, his/her date of birth;

c) *in case of organisational units without legal status: recording of current data from a document indicating the name, the organisational form, the registered office and address, tax identification number along with the first name, the last name and the PESEL number of the person representing this unit - or in the case of a person with no PESEL number, his/her date of birth*.

556. Article 9a of the AML/CFT Act defines verification as *"verifying and confirming data referred to in Article 9"*.

Identification of legal persons or other arrangements (c.5.4)

557. According to Article 9 of the AML/CFT Act, for customers that are legal persons or legal arrangements, financial institutions are required to obtain:

- The first and last name and the PESEL number (or date of birth in the case of a person with no PESEL) of the person representing the customer.
- The extract of the National Court Register or another document which contains a reference to the date of establishment of the customer, the customer's name, the organisational form, the registered office and address and the tax identification number.

558. In addition, the Polish authorities informed the evaluation team that the Polish Civil Code (article 96 in conjunction with article 6) states that if a person is acting as a proxy he/she must prove it. The civil law doctrine states that anyone doing in the name of other person is effective only if the person acts strictly on behalf of such person, and from his doings it must be clear that he acts as a proxy. Therefore the proxy each time must state clearly that he acts on behalf of another person, and point out directly the person on whose behalf he's acting. From the Polish authorities perspective it is counterintuitive to assume that there must be a legal provision stating directly that a FI must always check if the proxy is genuine.

559. Also the Polish authorities pointed out that the data of persons who are authorised to represent legal persons can be verified through the National Court Register. The register, which is publicly available, online and free of charge, provides a description of the manner in which a legal person may be represented. Every person is entitled to receive authenticated copies, excerpts and certificates of data contained in the Register (Law on the National Court Register, 20 August 1997). It should be noted that the Register effectively records company officials (e.g. directors, etc.), however this Register does not include persons acting under a power of attorney (e.g. agents, independent lawyers)

560. Nonetheless the evaluators noted that Article 9 and provisions from the Civil Code do not explicitly require financial institutions to verify that any person purporting to act on behalf of the customer is so authorised.

Identification of beneficial owner (c.5.5, c.5.5.1* & c.5.5.2)*

561. Article 8b (3), point 2, requires financial institutions to make "*attempts, with due diligence, in order to identify a beneficial owner and apply verification measures to identify the identity of, dependent on appropriate risk assessment, in order to provide the obligated institution with data required on the actual identity of a beneficial owner, including the determination of the ownership structure and dependence of the client"*.

562. Article 9 (3) of the AML/CFT Act specifies that the above identification includes the determination and recording of the first and last name and address, along with other identifiers to the extent to which financial institutions are able to determine it.

563. While criterion 5.5 requires financial institutions to identify the beneficial owner, Article 8b (3), point 2 merely requires financial institutions to make "*attempts*" to identify the beneficial owner.

Pursuant to this provision, financial institutions may enter into a business relationship without having identified the beneficial owner, as long as an attempt to identify the beneficial owner was made. In fact, during the on-site visit, financial institutions explained that in practice an attempt to identify the beneficial owner is always made. However, when it is impossible or difficult to identify a beneficial owner, the business relationship is still established and the customer is simply classified as high risk. Therefore, the evaluators concluded that there is no express requirement in the law which requires financial institutions to always identify the beneficial owners, where applicable, before establishing a business relationship or conducting an occasional transaction.

564. In relation to this issue, the Polish authorities indicated that on 13 February 2012 the Warsaw Voivodship Administrative Court issued a decision which supported the position of General Inspector of Financial Information who sanctioned a notary for failure to identify the beneficiary owner. In the decision the Court inter alia stated the following:

> *"Determining the real beneficial owner is therefore a basic financial security measure that is applied always, regardless of the awarded level of risk assessment."*

565. Although this court decision supports the requirement to identify the beneficiary owner, it does not set a precedent nor does it create a mandatory legal obligation for financial institutions. Therefore, it may not be accepted as a 'law, regulation or enforceable mean' for the purposes of criterion 5.5.

566. With respect to criterion 5.5.1 and 5.5.2, the Polish authorities pointed to the definition of a beneficial owner under Article 2(1a) of the AML/CFT Act, which reads as follows:

- *a natural person or natural persons, who are owners of a legal entity or exercise control over a client or have an impact on a natural person, on whose behalf a transaction or activity is being conducted,*
- *a natural person or natural persons who are stakeholders or shareholders or have the voting right at shareholders meetings at the level of above 25% within such a legal entity, therein by means of block of registered shares, with the exception of companies whose securities are traded within the organised trading, and are subject to or apply the provisions of the European Union laws on disclosure of information, and any entities providing financial services in the territory of an EU-Member State or an equivalent state in the case of legal entities,*
- *a natural person or natural persons who exercises control over at least 25% of the asset values - in the case of entities entrusted with the administration of asset values and the distribution of, with the exception of the entities carrying out activities referred to in Article 69 item 2 point 4 of the Act of 29 July 2005 on trading in financial instruments.*

567. With respect to legal persons, the beneficial owner is a natural person who owns or exercises control over the entity or has voting rights over 25% at the shareholders meeting of the entity.

568. Article 9d (2) of the AML/CFT Act provides for a derogation for listed companies and allows financial institutions, taking into account the reduced risk of money laundering and terrorist financing, not to identify and verify the beneficial owners of the company whose securities are admitted to public trading on a regulated market in at least one European Union member state or in an equivalent country.

Information on purpose and nature of business relationship (c.5.6)

569. Article 8b (3), point 3, of the AML/CFT Act requires financial institutions to obtain information regarding the purpose and the intended nature of a business relationship.

On-going due diligence on business relationship (c.5.7, 5.7.1 & 5.7.2)*

570. Financial institutions are required to conduct on-going due diligence on the business relationship pursuant to Article 8b(3), point 4, which states that financial institutions should *conduct constant*

monitoring of current economic relationships with a client, therein surveying transactions carried out to ensure that transactions are in accordance with the knowledge of the obligated institution on the client and the business profile of his operations and with the risk; and, if possible, surveying the origins of assets and constant update of documents and information in possession. However, it appears that Article 8b(3) is not fully in line with the requirement, since reporting institutions are obliged to survey the origins of assets, if possible but not where necessary.

571. On-going due diligence includes scrutiny of transactions throughout the course of the relationship with the client to ensure that they are consistent with the institution's knowledge of the client and his business and risk profile.

572. According to the above provision, financial institutions should also ensure that the CDD information obtained is kept up-to-date.

573. The representatives of financial institutions met during the on-site visit indicated that the identification data of a client is updated either when the client requests new financial products or otherwise on an annual basis.

Risk – enhanced due diligence for higher risk customers (c.5.8)

574. In terms of Article 8b (1) of the AML/CFT Act, financial institutions are required to apply CDD measures on the basis of an assessment of ML/FT risks, taking into account, in particular, the type of client, economic relationships, products or transactions.

575. Article 9e of the AML/CFT Act provides for the application of enhanced CDD for higher-risk customers. The Act also sets out three specific situations where, regardless of their own risk assessments, financial institutions are required to undertake enhanced CDD measures. These specific situations are the following:

- Non face-to-face business relations;
- Cross-border correspondent relations; and
- Politically Exposed Persons.

576. According to Article 9e, entities are required to undertake the following enhanced CDD measures in order to manage the ML/FT risk.

577. With respect to non face-to-face business relations, at least one of the following additional measures is to be applied:

1) *establishment of the identity of the client on the basis of additional documents or information;*
2) *additional verification of the authenticity of the documents or attestation of their compliance with the original copies by a notary public, a government body, a local government authority or an entity providing financial services;*
3) *ascertainment of the fact that the first transaction was conducted via the client's account in the entity providing financial services.*

578. The measures to be applied with respect to PEPs and correspondent relationships are dealt with in detail under Recommendations 6 and 7 respectively.

579. Transactions involving non-resident customers, private banking, legal persons or arrangements such as trusts that are personal assets holding vehicles or companies with nominee shareholders or bearer shares are not specifically covered. However, these types of business relationships would fall within the scope of Article 9e (1) which requires the application of enhanced CDD in relation to higher-risk situations.

580. The evaluators noted that no guidance was issued by the Polish authorities to assist financial institutions in determining who is a higher-risk customer and the type of enhanced CDD measures to be applied.

Risk – application of simplified/reduced CDD measures when appropriate (c.5.9)

581. Article 9d (1) of the AML/CFT Act sets out an exhaustive list of low-risk categories of customers in relation to which a financial institution may determine not to apply CDD measures (identification, verification, identification of the beneficial owner, and obtaining information about the purpose and nature of the business relationship). The categories are the following:

- Financial institutions situated in an EU Member State or equivalent country;
- Government and local authorities;
- Life insurance policies with an annual premium not exceeding €1,000 or with a single premium not exceeding €2,500.
- Insurance policies for pension schemes without a surrender clause and without the possibility of being used as collateral.
- Electronic money if the maximum amount does not exceed €150 (not rechargeable device) or €2,500 (per calendar year for rechargeable device).

582. Since Article 9d(1) completely exempts financial institutions from carrying out CDD measures with respect to the above categories of clients and products, it falls short of meeting the requirements under criterion 5.9, which states that measures may be reduced or simplified but not completely waived. The Polish authorities argued that although Article 9d(1) permits financial institutions to waive CDD measures completely, this can only be done after taking into account the ML/FT risk. Where there is information which suggests that the ML/FT risk is not low, financial institutions may not apply simplified CDD.

583. The representatives of financial institutions interviewed during the on-site visit indicated that they identify low-risk clients when a business relationship is established. However, they pointed out that no regulations or other enforceable means on the manner in which reduced/simplified CDD measures are to be implemented in practice are available.

584. In terms of Article 9d paragraph 2 of the AML/CFT Act, financial institutions may conduct simplified identification and verification measures in relation to a customer that is a listed company situated in the EU or equivalent country when establishing a business relationship and when there is a suspicion of ML/FT. This provision is not in line with criterion 5.11 which states that simplified CDD shall not apply when there is a suspicion of ML/FT. Although Article 9d (5) allows the Minister competent for Financial Institutions to extend the list of low-risk categories of clients for which simplified due diligence may apply, the list has never been extended in practice.

Risk – simplification/ reduction of CDD measures relating to overseas residents (c.5.10)

585. Article 9d paragraphs (1) and (2) of the AML/CFT Act permit the application of simplified due diligence to customers resident in an EU Member State or an equivalent country. An equivalent country is defined in the AML/CFT Act as a country that applies provisions on ML/FT in line with European Union AML/CFT Law. In practice reference is made to the EU Common Understanding on Third Country Equivalence to determine whether a country has equivalent AML/CFT laws.

Risk – simplified/ reduced CDD measures not to apply when suspicions of ML/FT or other risk scenarios exist (c.5.11)

586. There is no requirement in the law which prohibits the application of simplified CDD when there is a suspicion of ML/FT or specific higher risk scenarios apply. Furthermore, in terms of Article 9d paragraph 2, financial institutions may conduct simplified identification and verification measures

in relation to a customer that is a listed company situated in the EU or equivalent country when there is a suspicion of ML/FT.

Risk Based application of CDD to be consistent with guidelines (c.5.12)

587. At the time of the on-site visit, the Polish authorities had not issued any guidelines for the application of the risk-based approach. However, the Polish FSA provides on-going training, feedback and written interpretations on the risk-based approach.

Timing of verification of identity – general rule (c.5.13)

588. Article 9a (1) of the AML/CFT Act states that the verification of the identity of the customer and the beneficial owner is to be performed before entering into a contract with a client or prior to conducting a transaction.

Timing of verification of identity – treatment of exceptional circumstances (c.5.14 & 5.14.1)

589. Article 9a paragraphs (2) and (3) and Article 9b of the AML/CFT Act provide for exceptions in relation to timing of verification of identity within the context of a business relationship. Article 9a (2) states that the verification of identity of a customer may be completed after the establishment of a business relationship if it is necessary to ensure the normal conduct of business operations and where there is a low risk of money laundering or terrorist financing. This provision does not include one of the elements under criterion 5.14, which requires financial institutions to complete the verification of identity as soon as reasonably practicable after the establishment of the business relationship.

590. Article 9a (3) states that in the case of life insurance operations, the verification of identity of a policy's beneficiary or a policy's holder may be performed at the time of payout, prior to effecting the payout or when a beneficiary or a policyholder intends to exercise rights under such an insurance policy.

591. Furthermore, Article 9b of the AML/CFT Act permits obligated institutions to open an account without performing any CDD measures in certain justified cases. There is no explanation as to what constitutes a justified case. The provision further states that a financial institution may only carry out transactions after signing the opening-of-account contract. This provision is not entirely in line with criterion 5.14 since it permits financial institutions to not carry out any CDD measures before opening the account, whereas the Standards only refer to the postponement of verification of identity. However, Article 9b does not go beyond the requirements under criterion 5.14.1, since financial institutions are not permitted to utilise the account prior to carrying out full CDD measures.

592. During the on-site visit the representatives of financial institutions, the FIU and supervisor authorities indicated that Article 9b is intended to be applied when opening accounts without the presence of the client. However, transactions through such accounts may only be conducted after all CDD measures have been carried out.

Failure to satisfactorily complete CDD before commencing the business relationship (c.5.15) and after commencing the business relationship (c.5.16)

593. Polish law requires financial institutions to comply with CDD measures and where they are unable to do so, Article 8b (5) of the AML/CFT Act prescribes that financial institutions shall not carry out a transaction, shall not sign a contract with the customer or shall terminate any previously signed contracts. In addition, financial institutions are required to submit to the FIU information about such client, along with information on the specific transaction, where appropriate, taking into account the risk of money laundering and terrorist financing.

594. During the on-site visit, the representatives of financial institutions explained that in those cases where they are unable to identify the ultimate beneficial owner of a legal entity, rather than terminating the business relationship they raise the risk level of the customer. This goes beyond what is required under criterion 5.15.

Existing customers – (c.5.17 & 5.18)

595. The general requirement to apply CDD measures to existing customers is stated in Article 17 of the Act of 25 June 2009 that requires obligated institutions to apply CDD measures on the basis of risk analysis.

Article 17. Not later than in 12 months from the moment this Act enters into force, all obliged institutions shall perform the risk analysis of their existing customers, as referred to in Article 8b paragraph 1 of the AML/CFT Act.

Effectiveness and efficiency

596. The evaluators noted that financial institutions in Poland are generally aware of the CDD requirements as a result of the significant efforts invested in outreach to the financial sector by the GIFI and the PFSA. Such outreach generally takes the form of training programmes and clarification notes published on the websites of the GIFI and the PFSA. In addition, a guide entitled "Counteracting money laundering and terrorism financing" was issued by the GIFI to assist financial institutions and other reporting entities in the practical application of their AML/CFT requirements. Nevertheless, the guide is not publicly available but directly distributed by the GIFI to financial institutions and other reporting entities. The current (3rd) edition of the Guide has been issued in 2009 after the amendment of the AML/CFT Act. The evaluators were not in a position to assess the content of the guide since a translated copy was not made available to them.

597. The Bankers Association also issued recommendations on the application of the risk-based approach within AML/CFT, which recommendations were not officially endorsed by the authorities.

598. The representatives of the financial institutions met during the on-site visit confirmed that the GIFI is prompt in responding to queries made by financial institutions in order to clarify issues related to the implementation of CDD measures. However, the clarifications provided by the GIFI are not binding and simply serve as a guideline on the interpretation of the AML/CFT requirements. The evaluators were informed that in 2010 the GIFI responded to 315 inquiries submitted by obligated entities.

599. The major concern of the evaluators with respect to CDD measures is the identification of the beneficial owners. The interviewed representatives of reporting entities confirmed that in those situations where it is impossible to determine who the ultimate beneficial owner is, rather than terminating the business relationship, refraining from establishing the business relationship or rejecting the transaction, as the case may be, the financial institution simply revises the risk profile of the customer and proceeds with the business relationship or transaction. The evaluators believe that this practice is a direct result of the rather ambiguous wording of relevant provision in the AML/CFT Act, the absence of further clarification on this issue in secondary legislation and the unclear position of the state agencies themselves on this matter.

600. The issues identified under Recommendation 33 in relation to the lack of transparency concerning beneficial ownership and control of legal person may potentially have a negative impact on the effectiveness of the application of the requirements under Criteria 5.5, 5.5.1 and 5.5.2.

Recommendation 6 (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

601. Poland received a Non-Compliant rating for Recommendation 6 in the 3rd round MER since no enforceable AML/CFT measures had been in place concerning politically exposed persons.

Risk management systems, senior management approval, requirement to determine source of wealth and funds and on-going monitoring (c. 6.1- c. 6.4)

602. Politically exposed persons are defined in Article 2 (1f) of the AML/CFT Act as natural persons having their domicile outside the territory of the Republic of Poland and holding the following public functions:

- *Heads of state, heads of government, ministers, deputy ministers or assistant ministers, members of parliament,*
- *judges of supreme courts, constitutional tribunals and other judicial bodies whose decisions are not subject to further appeal with the exception of extraordinary measures,*
- *members of the court of auditors,*
- *members of central bank management boards,*
- *ambassadors, chargés d'affairs and senior officers of armed forces,*
- *members of management or supervisory bodies of state-owned enterprises.*

603. The natural persons holding any of the above-mentioned public functions retain their PEP status for a period of one year from the date on which they cease to hold such functions. The definition of PEPs in the AML/CFT Act also extends to the family members of PEPs including their spouses or persons cohabiting with them, parents and children and the spouses of those parents and children or other persons cohabiting with such persons.

604. The AML/CFT Act also covers persons in close professional or business cooperation with PEPs, those who co-own legal entities with PEPs and those who are entitled to assets of legal entities if they have been established for the benefit of PEPs.

605. The PEP definition is largely in line with the definition of PEPs in the Glossary to the FATF Methodology. However, the Polish PEP definition refers to persons residing in a foreign state whereas the standard refers to persons entrusted with prominent public functions in a foreign country irrespective of their residence. As a result, the Polish PEP definition excludes persons residing in Poland who are entrusted with prominent public functions in a foreign jurisdiction.

606. In terms of Article 9e 1, financial institutions are required to apply enhanced CDD measures when the customer is a PEP. This requirement does not extend to beneficial owners who are PEPs as required by criterion 6.1.

607. According to Article 9e 4. (1) of the AML/CFT Act, financial institutions are required to implement risk-based procedures to determine whether a customer is a PEP

608. Additionally, before establishing a business relationship with a PEP, financial institutions are required to obtain the consent of senior management (the board, the designated member of the management board, a person designated by the board or a person responsible for the activities of the financial institution). Senior management approval is not required to proceed with a business relationship where the customer or the beneficial owner becomes or is found to be a PEP after having been accepted as a customer.

609. Financial institutions are also required to take adequate measures to establish the source of asset values used by the customer in the business relationship. According to the Polish authorities explanation, the requirement to establish the source of asset values of a PEP covers both the source of wealth and the source of funds as required by criteria 6.3.

610. In addition, financial institutions must maintain constant monitoring of transactions conducted by PEPs. This requirement is not entirely in line with criterion 6.4 which refers to the enhanced on-going monitoring of a business relationship and not just transactions.

Additional elements

Domestic PEP-s – Requirements

611. The AML/CFT Act does not extend the requirement to apply enhanced due diligence measures to PEPs who hold prominent public functions domestically.

Ratification of the Merida Convention

612. The 2003 United Nations Convention against Corruption was ratified by Poland on 15 September 2006.

Effectiveness and efficiency

613. Financial institutions demonstrated a satisfactory level of awareness of the PEP requirements during the on-site visit. Some of the representatives of financial institutions (*i.a.* large banks) indicated that they use public sources or commercial databases (*e.g.* WorldCheck) for the detection of PEPs and their family members and associates.

614. Several representatives of small institutions indicated that they limit their efforts to detect PEPs through the collection of written declarations by the client, subject to penal liability for false declarations. Such option is envisaged under Article 9e (5) of the AML/CFT Act.

615. Although there is no formal requirement in the AML/CFT Act to obtain senior management approval in order to proceed with a business relationship with an existing client who is found to be or becomes a PEP, the Polish authorities and the financial institutions indicated that in practice such approval is sought as part of the risk management procedures.

Recommendation 7 (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

616. Poland received a 'Non-Compliant' rating in the 3rd round report as no enforceable AML/CFT measures had been in place concerning the establishment of cross-border correspondent banking relationships.

Require to obtain information on respondent institution & Assessment of AML/CFT controls in Respondent institutions (c. 7.1 & 7.2)

617. Financial institutions that maintain a cross-border correspondent banking relationship with foreign financial institutions located in countries other than the EU member States and equivalent countries are required to apply enhanced CDD measures according to Article 9e (3) of the AML/CFT Act. Since, this provision does not apply to institutions located within the EU or an equivalent country, it falls short of meeting the requirements under Recommendation 7 which refers to all type of cross-border relationships even if they are established with a respondent institution that is located in a state imposing equivalent obligations.

618. Article 9e (3) points 1 and 2 require financial institutions to collect sufficient information to determine the scope of operations of the respondent institution and to ascertain whether a provider of financial services is supervised by the state in which it is established. There is no explicit obligation to determine the reputation of the respondent institution and whether it has been subject to a ML or TF investigation or regulatory action.

619. Pursuant to Article 9e (3) point 2, financial institutions are also required to assess the measures implemented by the respondent institution in so far as counteracting money laundering and terrorist financing are concerned. However, there is no requirement to ascertain that the AML/CFT measures implemented by the respondent institution are adequate and effective.

Approval of establishing correspondent relationships (c.7.3)

620. According to Article 9e (3) point 5 of the AML/CFT Act, financial institutions are required to obtain a prior approval of a board of directors or a designated person before establishing new correspondent relationships.

Documentation of AML/CFT responsibilities for each institution (c.7.4)

621. Article 9e (5) point 3 of the AML/CFT Act requires financial institutions to prepare documentation defining the scope of responsibilities of each institution.

Payable through Accounts (c.7.5)

622. According to paragraph 3 of Article 9e point 4 of the AML/CFT Act, with respect to payable-through accounts, financial institutions are required to ascertain that the respondent institution conducts CDD measures in relation to clients having direct access to the respondent's accounts and that it is able to provide any relevant customer identification data upon request to the correspondent financial institution.

Effectiveness and efficiency

623. At the time of the on-site visit, the bankers demonstrated a satisfactory level of awareness and understanding of the enhanced CDD measures which are required when establishing correspondent relationships. The PFSA and the FIU pointed out that they had never identified any major issues with respect to the enhanced CDD measures examined in the course of on-site inspections.

Recommendation 8 (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

624. Poland received a Partially Compliant rating in the 3rd round MER since financial institutions were not subject to a direct requirement to have policies in place to prevent the misuse of technological developments in ML and TF schemes.

Misuse of new technology for ML/FT (c.8.1)

625. Financial institutions are not required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in ML/FT schemes.

626. The Polish authorities indicated that although no express provision exists in the law, guidance on this matter was provided to financial institutions on an individual basis. Additionally, a paper issued by the Wolfsberg Group on pre-paid and stored value cards was translated into Polish and placed on the website of the PFSA.

Risk of non-face-to-face business relationships (c8.2 & c8.2.1)

627. Financial institutions are required to apply enhanced CDD measures when the customer is not physically present for the establishment of a business relationship or the carrying out of a transaction. In such cases, according to Article 9e (2) of the AML/CFT Act, financial institutions shall apply at least one of the following measures in order to reduce the risk:

i) *establishment of the identity of the client on the basis of additional documents or information;*

ii) *additional verification of the authenticity of the documents or attestation of their compliance with the original copies by a notary public, a government body, a local government authority or an entity providing financial services;*

iii) *ascertainment of the fact that the first transaction was conducted via the client's account in the entity providing financial services.*

628. The evaluators noted that financial institutions are not required to have policies and procedures to address the specific risks associated with non face-to-face business relationships when conducting on-going due diligence.

Effectiveness and efficiency

629. The effectiveness of criterion 8.1 could not be demonstrated since there is no requirement in the law to prevent the misuse of new technologies.

630. During the on-site visit financial institutions explained that non face-to-face relationships are invariably categorised as higher risk relationships and enhanced due diligence measures are applied. This position was corroborated by the authorities, who stated that no deficiencies were identified in relation to this requirement in the course of on-site visits.

3.2.2 Recommendations and comments

631. The following actions are recommended to be taken to ensure an adequate implementation of Recommendations 5, 6, 7 and 8.

Recommendation 5

632. Notwithstanding the fact that most of the CDD deficiencies identified in the third round were broadly addressed through the enactment of the AML/CFT Act, the evaluators noted that the legislative provisions dealing with CDD requirements are still not entirely in line with the FATF Standards. Moreover, since a translated copy of the guide issued by the FIU was not made available to the evaluators, it was not possible to conclude with certainty whether such guidance provides adequate assistance to financial institutions on the practical implementation of the legislative requirements.

633. A provision should be included in the AML/CFT Act expressly requiring financial institutions to carry out customer due diligence measures when carrying out occasional transactions that qualify as a wire transfer amounting to or exceeding €1,000.

634. Financial institutions should be required to verify customer identity on the basis of document, data or information obtained from a reliable and independent source.

635. Financial institutions should be required to identify the beneficial owner, where applicable, and not simply attempt to identify the beneficial owner. Additionally, there should be a clear provision to explicitly prohibit financial institutions from establishing (or continuing) a business relationship with a customer in those instances where the ultimate beneficiary owner cannot be determined.

636. Financial institutions should be required to ensure that a person acting on behalf of a legal person is so authorised.

637. Obligated institutions should be required when conducting on-going due diligence on the business relationship to establish, where necessary, the source of funds.

638. Financial institutions should not be permitted to waive the application of CDD measures entirely when dealing with low risk customers and products. Additionally, the application of simplified CDD should not be accepted whenever there is a suspicion of ML/FT.

639. Financial institutions should be required to complete the verification of identity as soon as reasonably practicable in those cases where verification is not carried out before the establishment of a business relationship. Additionally, financial institutions should not be permitted to open an account without performing full CDD measures, since the relevant criterion merely refers to the postponement of verification and not full CDD.

640. Polish authorities should consider issuing a specific guidance to assist financial institutions in implementing the requirements of the AML/CFT Act.

Recommendation 6

641. The PEP definition should be extended to cover important political party officials and persons entrusted with prominent public functions in a foreign country irrespective of their residence.

642. Financial institutions should be required to apply enhanced CDD measures when the beneficial owner is a PEP.

643. Financial institutions should be required to obtain senior management approval to continue the business relationship where the customer or beneficial owner subsequently becomes or is found to be a PEP after having been accepted as a client.

644. Financial institutions should be required to conduct enhanced on-going monitoring on the entire business relationship and not just transactions.

Recommendation 7

645. According to the FATF Standards, the requirements regarding correspondent banking relationships have to be applied irrespective of whether the respondent institution is located in a state imposing equivalent obligations. Therefore, Article 9e (3) of the AML/CFT Act should apply to respondent institutions located in any foreign jurisdictions.

646. Financial institutions should be required to determine the reputation of the respondent institution and whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

647. Financial institutions should be required to ascertain that the AML/CFT measures implemented by a respondent institution are adequate and effective.

Recommendation 8

648. A requirement to have policies and measures to prevent the misuse of technological developments in ML/FT schemes should be introduced.

649. Financial institutions should be required to have policies and procedures to address the specific risks associated with non face-to-face business relationships when conducting on-going due diligence.

3.2.3 Compliance with Recommendations 5, 6, 7 and 8

	Rating	Summary of factors underlying rating
R.5	**PC**	• The legislation does not cover full CDD requirements when carrying out occasional transactions that are wire transfers equal to or exceeding €1,000;[32] • Financial institutions are required to verify the customer identity on the basis of documents and information from a public source, but not specifically from reliable and independent sources; • There is no clear requirement to identify the beneficial owner, since financial institutions are only required to attempt to identify the beneficial owner; • There is no requirement to verify whether any person purporting to act on behalf of a legal person is so authorised; • When conducting on-going due diligence on the business relationship there is no requirement to establish, where necessary, the source of funds;

[32] The obligation to carry out full CDD only applies to wire transfers exceeding 15,000 EUR.

		• The provisions dealing with simplified CDD permit financial institutions to waive all CDD measures, except for on-going monitoring; • There is no prohibition against applying simplified CDD when there is a suspicion of ML/FT; • There is no requirement to complete verification of identity as soon as reasonably practicable in those cases where verification is not carried out before the establishment of a business relationship; • Article 9b permits financial institutions to open an account without performing full CDD; **Effectiveness:** • Some financial institutions met on-site maintain a business relationship despite the fact that the ultimate beneficial owner is unknown.
R.6	**LC**	• The PEP definition does not cover important political party officials and persons entrusted with a prominent public function by a foreign jurisdiction who are resident in Poland; • No requirement to apply enhanced CDD if the beneficial owner is a PEP; • No specific requirement to obtain senior management approval to continue a business relationship where the customer subsequently is found to be or becomes PEP; • There is no requirement to conduct enhanced on-going monitoring on the entire business relationship with a PEP.
R.7	**LC**	• The requirements regarding correspondent banking relationships are limited to respondent institutions located in a state not imposing equivalent AML/CFT obligations; • No requirement to establish the reputation of the respondent and to determine whether it has been subject to a ML/FT investigation or regulatory action; • No requirement to ascertain that the AML/CFT measures implemented by a respondent institution are adequate and effective.
R.8	**PC**	• No requirement to have policies and procedures in place to prevent the misuse of technological developments in ML/FT schemes; • No requirement to have policies and procedures to address the specific risks associated with non face-to-face business relationships when conducting on-going due diligence.

3.3 Third Parties and Introduced Business (R.9)

3.3.1 Description and analysis

Recommendation 9 (rated N/A in the 3rd round report)

Summary of 2007 factors underlying the rating

650. Poland received a 'Not Applicable' rating in the 3rd MER.

651. Following the adoption of amendments to the AML/CFT Act in 2010, Article 9h and 9i introduced provisions providing for reliance on other entities for the application of CDD measures. In this respect, the evaluators have considered it necessary to assess this Recommendation under the fourth assessment.

652. Article 9h of the AML/CFT Act states the following:

> *Each obligated institutions may rely on other entities in so far as the implementation of the obligations set out in Article 8b (3) points 1-3. The responsibility for such an implementation shall remain with the obligated institution.*

653. In addition, Article 9i of the AML/CFT Act provides for reliance by a financial institution situated in Poland on another financial institution situated in an EU member state or equivalent country, when the financial institution situated in Poland is requested to conduct a transaction on behalf of a customer of the financial institution situated outside Poland. In such cases reliance may take place provided that the financial institution in Poland has ensured that the financial institution outside Poland will provide copies of CDD documentation whenever it is so requested. Furthermore, the financial institution outside Poland should be required by the financial institution in Poland to make copies of CDD documentation immediately accessible.

Requirement to immediately obtain certain CDD elements from third parties; availability of identification data from third parties (c.9.1 & 9.2)

654. As stated above, Articles 9h and 9i of the AML/CFT Act establish the possibility for obligated institutions to rely on third parties to perform CDD measures. In particular, Article 9h refers to general requirement and Article 9i specifically deals with third parties from EU member-states or equivalent country.

655. Criterion 9.1 requires financial institutions relying upon a third party to immediately obtain from the third party the necessary information concerning certain elements of the CDD process. This requirement does not feature in Article 9h, however Article 9i(1) foresees such a requirement.

656. Criterion 9.2 requires financial institutions to take adequate steps to satisfy themselves that copies of CDD documentation will be made available from the third party upon request without delay. This requirement only features under Article 9i(1).

Regulation and supervision of third party & adequacy of application of FATF Recommendations (c.9.3 & 9.4)

657. There is no requirement in Article 9h for financial institutions to satisfy themselves that the third party is regulated and supervised (in accordance with Recommendation 23, 24 and 29), and has measures in place to comply with the CDD and record-keeping requirements. Article 9i(1) permits financial institutions in Poland to rely on financial institutions in an EU member state or equivalent country. Therefore, to some extent criterion 9.3 is covered under this article.

658. With respect to criterion 9.4, Article 9i states that financial institutions may only rely on other financial institutions situated in an EU or equivalent countries. Therefore, this criterion is covered. However, Article 9h does not impose any limitations with respect to the country where the third party can be based.

Ultimate responsibility (c.9.5)

659. According to Article 9h of the AML/CFT Act, the ultimate responsibility for meeting customer due diligence requirements remains with the reporting entity that relies on the third party. Article 9i 1 is silent on this matter.

Effectiveness and efficiency

660. Financial institutions representatives interviewed during the on-site visit did not indicate that reliance on the third parties is widely applied. Polish authorities are of the opinion that Article 9h is applicable only for the outsourcing or agency relationships although this is not confirmed by law or secondary legislation.

3.3.2 Recommendations and comments

661. Although the AML/CFT Act provides for reliance on third parties a number of significant gaps exist in the legislation. The provisions on reliance should therefore be entirely amended to be brought in line with the different criteria set out under Recommendation 9. In particular, the following requirements should be provided for:

- Immediately obtain from the third party the necessary information concerning certain elements of the CDD process (Criteria 5.3 to 5.6);
- Take adequate steps to ensure that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;
- Satisfy themselves that the third party is regulated and supervised and has measures in place to comply with the CDD requirements.

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	**PC**	• Partial requirement to immediately obtain from a third party the necessary information concerning certain elements of the CDD process; • Partial requirement to take adequate steps to ensure that that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay; • No clear requirement to ensure that the third party is regulated and supervised and has measures in place to comply with the CDD requirements; • No measures to determine under Article 9h of the AML/CFT Act whether the country in which the third party is based adequately applies the FATF Recommendations.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and analysis

Recommendation 4 (rated C in the 3rd round report)

Summary of 2007 factors underlying the rating

662. Recommendation 4 was rated Compliant in the 3rd round MER of Poland.

Ability of competent authorities to access information they require to properly perform their functions in combating ML or FT

663. Criterion 4.1 requires that no financial institution secrecy law inhibits the implementation of the FATF Recommendations particularly as regards the ability of competent authorities to access information they require to properly perform their functions in combating ML or FT; the sharing of information between competent authorities, either domestically or internationally; and the sharing of information between financial institutions.

664. According to Article 29 of the AML/CFT Act in order to disclose any information in the manner and extent prescribed by the Act to the GIFI, regulations restricting the disclosure of confidential information shall not apply, except for classified information.

665. Article 15 of the AML/CFT Act authorises the GIFI to request any governmental and local authorities and other public organisational units, as well as the National Bank of Poland, the Polish Financial Supervision Authority and the Supreme Chamber of Control (see Article 2 § 8 of the AML/CFT Act) to make available information and copies of documents.

666. Pursuant to Article 13a of the AML/CFT Act, obligated institutions shall make available the information concerning transactions subject to the AML/CFT Act upon written request by the GIFI.

667. The current provisions of the AML/CFT Act are worded in fairly broad terms and the evaluation team was not informed about any practical impediments to obtaining information from obligated institutions.

Banking secrecy:

668. Article 105 paragraph 1 point 2 of the Banking Act requires banks to disclose information that is subject to the obligation of banking secrecy amongst others at the request of:

- the Banking Supervision Commission,
- GIFI (in cases provided for in separate legislation),
- the Police, when this is necessary for effective crime prevention or detection,
- a court or public prosecutor in connection with legal proceedings under way in cases involving criminal or fiscal offences:
    a) against a natural person where such person is party to an agreement with the bank, with the scope of information being that related to that natural person,
    b) committed with respect to the activity of a juridical person or organisation not possessed of personality at law, with the scope of information being that related to that juridical person or organisation,
- a court or public prosecutor in connection with the performance of a request for legal assistance from a foreign country which, on the basis of a ratified international agreement binding on the Republic of Poland, has the right to request information that is subject to the obligation of banking secrecy,

- a court in connection with legal proceedings under way in cases involving inheritance or the division of the joint property of husband and wife, and also legal proceedings under way against a natural person in cases involving maintenance or continuous financial provisions related to maintenance, where the said person is party to an agreement with the bank.

Capital market secrecy

669. Pursuant to paragraph 1(3) of Article 150 of the Act on Trading in Financial Instruments the professional secrecy obligation shall not be deemed breached by disclosure of information covered by professional secrecy to the GIFI to the extent and on the terms specified in the AML/CFT Act.

670. Similar provisions can be found in the Act on Investment Funds of 29 July 2005 (Articles 281 and 282), the Tax Ordinance Act of 29 August 1997 and the Tax Investigation Act of 28 August 1991 (Article 33).

Insurance secrecy

671. Article 19 of the Act on Insurance Activities states: *"Insurance undertaking and persons employed therewith or the persons and entities with the help of which insurance undertaking performs insurance operations shall be obligated to maintain secrecy concerning individual insurance contracts".*

672. According to paragraph 2 of Article 19 of the Act *"The interdiction referred to in paragraph 1 does not concern information given at the request of the GIFI, with respect to his performance of the tasks specified in the AML/CFT Act".*

Sharing of information between competent authorities, either domestically or internationally

673. As was previously mentioned the GIFI is also empowered (see Article 33 AML/CFT Act) to share information with some other authorities as already noted under Recommendation 26 (Section 2.5 of this report).

674. Furthermore, according to paragraph 2 of Article 17 of the Act on Financial Market Supervision the PFSA and the National Bank of Poland may enter into an agreement on cooperation and information exchange between the FSA and the National Bank of Poland. Such an agreement was signed on 14 December 2007.

675. In addition, Article 17a of the Act allows the PFSA to provide the Minister of Finance and the National Bank of Poland with information acquired by the PFSA, including information protected under separate laws, necessary to pursue the objective of activity and tasks of the Polish Financial Stability Committee.

676. Article 17 (3 and 4) also allows the PFSA to exchange information with the European Central Bank, the Bank Guarantee Fund and the Insurance Guarantee Fund.

677. In respect of sharing information between international competent authorities, pursuant to Article 78 of the Act on Financial Market Supervision, the Financial Supervision Authority shall exchange information to the extent necessary to exercise supervision over the particular sectors of the financial market and over financial conglomerates, as well as in connection with cooperation with foreign regulatory authorities.

678. Also according to Article 131 of the Banking Act the Polish Financial Supervision Authority may provide information concerning a bank to the banking supervision agency of another country, where:

1) this will not prejudice the economic interests of the Republic of Poland,
2) it is ensured that the information provided will be utilised solely for the purposes of banking supervision,

3) it is guaranteed that the information provided may be transmitted to parties outside the agency of banking supervision solely with the prior consent of the Polish Financial Supervision Authority.

Sharing of information between financial institutions where this is required by R.7, R.9 or SR. VII

679. The obligations stipulated by paragraph 4 of Article 9e point 4 of the AML/CFT Act (see also analysis of Recommendation 7 under Section 3.2) in the area of correspondent banking relationships provide the ability of financial institutions to share information for the purpose of Recommendation 7.

680. However, given the lack of provisions concerning reliance on third parties (see analysis of Recommendation 9), it is unclear if financial institutions could provide information on their customers in the absence of a specific provision in this sense.

681. In the case of the information related to the wire transfer payer that has to accompany through the payment chain this obligation is set forth in Regulation (EC) No 1781/2006 of the European Parliament and the Council, which is directly applicable for the country members (see analysis of Special Recommendation VII).

Effectiveness and efficiency

682. The information presented to the evaluation team by the Polish authorities and the private sector did not reveal any instances where professional secrecy provisions limited the information exchange in practice.

3.4.2 Recommendations and comments

683. In Poland no financial institution secrecy law inhibits the implementation of the FATF Recommendations.

684. Polish authorities should take necessary steps to introduce provisions in the AML/CFT Act to cover reliance on third parties, specifically with respect to obtaining information from them.

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	**LC**	• No specific provision on third parties reliance to allow financial institutions to obtain necessary information on their customers.

3.5 Record Keeping and Wire Transfer Rules (R.10 and SR. VII)

3.5.1 Description and analysis

Recommendation 10 (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

685. Poland received a Partially Compliant rating for Recommendation 10 in the third round evaluation. The evaluation report noted that there were no requirements in law or regulation to require financial institutions to keep identification data, account files and business correspondence for at least five years after the closure of the account or termination of the business relationship. The absence of a provision in law or regulation requiring financial institutions to ensure that customer and transaction records and information are available on a timely basis to the competent authorities was also criticised.

Record keeping & Reconstruction of Transaction Records (c.10.1 and 10.1.1)

686. Article 8 (4a) of the AML/CFT Act prescribes that *any information on the transactions carried out by the obligated institution and documents related to such a transaction are stored for a period of 5 years calculating from the first day of the year in which the last record associated with the transaction took place.*

687. There is no provision in the AML/CFT Act or other law or regulation that empowers competent authorities to request a financial institution to extend the record-keeping period beyond five years with respect to transactions.

688. Although there is no specific requirement in the law which states that transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity, the Polish authorities are of the opinion that the requirement under Article 8(4a) to maintain any information on transactions is sufficient to cover criterion 10.1.1.

Record keeping of identification data, files and correspondence (c.10.2)

689. Article 9k requires financial institutions to store all CDD and enhanced CDD documentation for a period of five years. The five-year period commences on the first day of the year following the year in which the transaction was carried out for the customer.

690. The record-keeping period does not commence on the date of termination of an account or a business relationship as required under criterion 10.2. Furthermore, competent authorities are not explicitly empowered to extend such period. Nonetheless, in practice obligated institutions do maintain all necessary documents for more than 5 years after the date of termination of an account or a business relationship.

691. Article 74.1.4 of the Accounting Act requires all entities to keep the accounting documents which are related to business contracts for 5 years from the beginning of the year which follows the financial year in which operations, transactions and proceedings were have been completed, paid, settled or expired. According to the Art.20.1 of the Accounting Act refers to the accounting documents as to the documents based on which the entries in the books of account are based. Therefore Accounting Act recordkeeping requirements may cover account files from c.10.2 but not business correspondence. As the generally accepted definition of accounting documents is "Original records which evidence a financial transaction, such as debit/credit memos, invoices, receipts, orders, vouchers" it is unclear whether this covers account opening documentation including identification data.

692. There is also no specific requirement to keep business correspondence.

Availability of Records to competent authorities in a timely manner (c.10.3)

693. Sectoral laws, namely Article 105 paragraph 1 point 2 of the Banking Act, Article 88 of the Act on Trading in Financial Documents, Article 225 paragraph 2 of Act on Investment Funds, Article 19 of the Act on Insurance Activities provide for that the supervisory authorities should be provided upon a request any necessary information from obligated institutions.

Effectiveness and efficiency

694. Although the GIFI, other competent authorities and financial institutions did not refer to any issues with respect to the record-keeping requirements, the various technical shortcomings identified by the evaluators could have a serious impact on the effectiveness of Recommendation 10.

Special Recommendation VII (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

695. Poland was rated 'Non-Compliant' with respect to SRVII, since the requirements under SRVII on wire-transfers were not directly covered by law or regulation. Furthermore, it was also noted that in the Polish legal framework there was no obligation to identify a customer who transfers money (except for transactions exceeding €15,000 or suspicious transactions). With respect to domestic banking wire transfers between account holders, financial institutions are required to include the originators account number and his/her name and address within the message or payment form. This is based on Standards issued by the Polish Banking Association in cooperation with the National Clearing House. These Standards were followed by all banks but they were not binding.

696. Regulation 1781/2006 of the European Parliament and of the Council, of 15 November 2006, provides rules on transactions related to domestic or cross-border money transfers or remittances in amounts of €1,000 or more. This Regulation is mandatory and binding on all EU Member States and is directly applicable in Poland as a member of the European Union.

Obtain Originator Information for Wire Transfers (c.VII.1)

697. According to the FATF methodology, transfers between Poland and other EU member countries are considered as domestic for the purposes of the assessment of SRVII, while wire transfers between Poland and non-EU member states are considered as cross-border.

698. Article 4 of the Regulation defines complete information on the payer as that information relating to the name, address and account number – the latter to be replaced by a unique identifier where a payer does not hold an account.

699. Moreover, Article 5 of the Regulation requires that for payments not effected through an existing account, originator information should be verified only where the amount exceeds €1,000 whether carried out in one operation or in several operations that appear to be linked. Verification of identification data is to be carried out on the basis of documents, data or information obtained from a reliable and independent source.

700. According to Article 10c (1) of the AML/CFT Act, the provisions of the Regulation do not apply where a payment service provider of the payee is able by means of a unique reference number to trace back all the transfers of funds to the payer, who has concluded a contract for the supply of goods and services with the payee, even if amount of such transaction does not exceed the equivalent of €1,000.

701. According to Article 10c (2) of the AML/CFT Act the provisions of the Regulation do not apply to a payment service provider having its legal address in the territory of Poland in relation to transfers of funds to non-profit organisations, exercising charitable, religious, cultural, educational, social, scientific activities, if the transfer of funds does not exceed the equivalent of €150 and takes place only in the territory of Poland.

Inclusion of Originator Information in Cross-Border Wire Transfers (c. VII.2); Inclusion of Originator Information in Domestic Wire Transfers (c. VII.3); Maintenance of Originator Information (c.VII.4)

702. According to Article 7(1) of the Regulation, cross-border wire transfers shall be accompanied by complete information on the payer. Article 7(2) states that a batch file transfer from a single payer to different payees need not be accompanied by complete information on the payer, provided that the batch file contains that information and the individual transfers carry the account number of the payer or a unique identifier.

703. Under Article 6 of the Regulation, domestic wire transfers of funds shall only be required to be accompanied by the account number of the payer or a unique identifier where both payer and payee payment services providers are situated within the European Union allowing the transaction to be

traced back to the payer. However, if so requested by the payment service provider of the payee, the payment service provider of the payer shall make available to the payment service provider of the payee complete information on the payer within three working days of receiving that request.

704. Article 12 of the Regulation stipulates that intermediary payment service providers shall ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer.

705. According to Article 14 of the Regulation, payment service providers shall respond fully and without delay to enquiries from the competent authorities concerning the information on the payer accompanying transfers of funds and corresponding records, in accordance with the procedural requirements established in the national law of the Member State in which they are situated. For the purpose of the EU Regulation, the competent authority in Poland is the FIU in full cooperation with the PFSA.

706. In cases of technical limitations to a payment system, an intermediary payment service provider situated within the EU must keep records of all information received for five years (Article 13 (5) of the Regulation).

707. According to Article 8 (4) of the AML/CFT Act, the register of transactions shall be stored for a period of five years, which commences on the first day of the year following the year in which transactions were recorded. In accordance with Article 12, information on transactions shall include the trade date, the identification data of the parties and the numbers of the accounts used to conduct the transactions.

Risk Based Procedures for Transfers Not Accompanied by Originator Information (c. VII.5)

708. As stipulated in Article 8 of the Regulation, the payment service provider of the payee shall detect whether, in the messaging or payment and settlement system used to effect a transfer of funds, the fields relating to the information on the payer have been completed. Providers shall have effective procedures in place in order to detect whether the following information on the payer is missing:

- for transfers of funds where the payment service provider of the payer is situated in the EU, the information required under Article 6 of the regulation;
- for transfers of funds where the payment service provider of the payer is situated outside the Community, complete information on the payer, or where applicable, the information required under Article 13; and
- for batch file transfers where the payment service provider of the payer is situated outside the Community, complete information on the payer in the batch file transfer only, but not in the individual transfers bundled therein.

709. If the payment service provider of the payee becomes aware, when receiving transfers of funds, that information on the payer required under this Regulation is missing or incomplete, it shall either reject the transfer or ask for complete information on the payer. Where a payment service provider regularly fails to supply the required information on the payer, the payment service provider of the payee shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider or deciding whether or not to restrict or terminate its business relationship with that payment service provider. The payment service provider of the payee shall report that fact to the authorities responsible for combating money laundering or terrorist financing, which is the GIFI (Article 9 of the Regulation).

710. According to Article 10 of the Regulation, the payment service provider of the payee shall consider missing or incomplete information on the payer as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether it must be reported, in accordance with

the reporting obligations set out in the 3rd EU Directive, to the authorities responsible for combating money laundering or terrorist financing.

711. During the interviews, the representatives of banks and the Banking Association confirmed that they have adopted internal procedures concerning AML/CFT risks and that the PFSA examines those procedures during on-site inspections. The monitoring of compliance with the requirements of Regulation 1781/2006 is a fairly detailed part of the inspection manual of the PFSA.

Monitoring of Implementation (c. VII.6) and Application of Sanctions (c. VII.7: applying c.17.1 – 17.4)

712. According to Article 21 (3a) of the AML/CFT Act, the GIFI is the designated authority to impose penalties in cases of breaches of the provisions of the AML Law. Breaches of the Regulation are also stipulated in the AML/CFT Act under Article 34b, which reads as follows:

> 1. Any obligated institution which is in breach of the following provisions of Regulation No 1781/2006:
>
> 1) Articles 5-7, does not ensure that the transfer of funds is accompanied by complete information on the payer,
>
> 2) Article 8, does not have effective procedures in place to detect the absence of information on the payer,
>
> 3) Article 9, does not inform the General Inspector about the payment service providers of the payer, which regularly fail to provide relevant information on the payer,
>
> 4) Article 12, when acting as an intermediary payment service provider, does not keep all the information on the payer accompanying transfers of funds,
>
> 5) Article 14, does not provide a full response on the request of the General Inspector about the information on the payer accompanying transfers of funds, and does not provide the General Inspector with the requested relevant documents.
>
> - shall be subject to financial sanctions.

713. According to Article 34c of the AML/CFT Act the sanctions may not be higher than PLN 750,000 (approx. €180,000).

Additional elements – Elimination of thresholds (c. VII.8 and c. VII.9)

714. For transfers of funds where the payment service provider of the payer is situated outside the EU (incoming cross-border wire transfers), the payment service provider of the payee shall have effective procedures in place in order to detect whether the complete information on the payer as referred to in Article 4 (complete information on the payer) is missing (Article 8 (b) of the Regulation). If this is not the case, the payment service provider has to follow the procedures described above, regardless of any threshold.

715. For transfers of funds where the payment service provider of the payee is situated outside the area of the EU (outgoing cross-border wire transfers), the transfer shall always be accompanied by complete information on the payer, regardless of the threshold. (Article 7 of the Regulation; exemptions in the context of batch file transfers are elaborated above).

Effectiveness and efficiency

716. In October 2007 discussions were held between the GIFI, the General Inspector of Banking Supervision and Polish Bank Association to exchange opinions on the difficulties encountered when dealing with issues of European regulations implementing FATF Special Recommendation VII and the situation regarding the application of the Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds. According to the opinion of the Polish Bank Association, the

transfers of funds with incomplete or meaningless information on the payer do not exceed 10% of the total number of transfers that are conducted. The findings of inspections carried out by the supervisory authorities indicated that in all those instances where transfers are received with incomplete information, banks initiate an examination and seek to obtain complete information on the payer.

717. Following the meeting between the GIFI, the Banking Supervision and the Bank Association in 2007, the supervisory authorities did not conduct any assessment on the problems identified by payment service providers. Additionally, no reporting system was introduced on payment service providers which regularly fail to provide the required information as recommended in Para 4.3 of the Common Understanding (CESR/ CEBS/ CEIOPS) on Regulation 1781/2006.

718. During the on-site visit, the representatives of banks confirmed that they have not identified regular and serious problems regarding the information on the payer in the case of cross-border wire transfers.

3.5.2 Recommendation and comments

Recommendation 10

719. The Polish legislation should explicitly empower competent authorities to request financial institutions to extend the record-keeping period beyond five years.

720. The requirement for the record-keeping period for identification data under the AML/CFT Act should be amended to commence on the date of the termination of an account or a business relationship. Additionally, financial institutions should be required to maintain records of business correspondence.

Special Recommendation VII

721. The requirements for SR.VII seem to be comprehensively and adequately covered by EU Regulation 1781/2006 which is mandatory for the Member States of the EU and therefore directly applicable in Poland.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**LC**	• There is no requirement empowering competent authorities to request financial institutions to extend the record-keeping period beyond 5 years; • The commencement of the record-keeping period under the AML/CFT Act in relation to customer data is not linked to the date of the termination of an account or a business relationship; • No requirement to retain business correspondence.
SR.VII	**C**	

Unusual and Suspicious transactions

3.6 Monitoring of Transactions and Relationship Reporting (R. 11 and R. 21)

3.6.1 Description and analysis[33]

Recommendation 11 (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

722. As a result of the assessment of compliance with Recommendation 11 under the Third-Round Evaluation, Poland was rated 'Partially Compliant' in view of the fact that it did not have in place adequate provisions requiring financial institutions to pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose, nor to examine as far as possible the background and purpose of unusual transactions, to set forth findings in writing and keep such findings available for competent authorities or auditors for at least five years.

Special attention to complex, unusual large transactions (c. 11.1)

723. The AML/CFT Act does not contain a direct reference to the obligation to pay special attention to complex and unusually large transactions, as well as to unusual patterns of transactions, which have no apparent or visible economic or lawful purpose. The Polish authorities explained that criterion 11.1 is covered through a combined application of Article 8b 3 point 4 and Article 8a paragraph 1. Article 8b paragraph 3 point 4, which is the provision dealing with on-going monitoring, requires financial institutions to constantly monitor the on-going economic relationships with a client. This includes monitoring all the transactions carried out to ensure that those transactions are consistent with the financial institution's knowledge of the customer and the business and risk profile of the customer's operations and, if possible, examining the origin of the assets. Financial institutions are also required to keep documents and information on their client constantly updated.

724. In addition, Article 8a paragraph 1 requires financial institutions to carry out on-going analysis of the transactions carried out. This provision appears to require the analysis of all transactions carried out by a financial institution. It is unclear how this requirement could be achieved in practice.

725. The evaluators are of the opinion that since Article 8a paragraph 1 is couched in very wide terms, it technically covers the requirement under criterion 11.1. Nevertheless, this article could potentially cause effectiveness issues, since it would appear to be physically impossible for a financial institution to analyse every single transaction carried out by a customer and record the findings in writing. Additionally, the manner in which Article 8a paragraph 1 is drafted could potentially detract the focus from complex, unusual large transactions or unusual patterns of transactions, which is the primary purpose of Recommendation 11.

Examination of complex and unusual transactions (c. 11.2)

726. As already stated Article 8a paragraph 1 requires financial institutions to analyse all transactions. This would technically cover the requirement to examine as far as possible the background and purpose of such transactions. Additionally, financial institutions are required to document in paper or electronic format the results of the analysis of all transactions.

Record-keeping of finding of examination (c. 11.3)

727. Article 8a paragraph 2 requires financial institutions to keep a record of the analysis of all transactions for a period of five years, which period commences on the first day of the year following

[33] The description of the system for reporting suspicious transactions in s.3.7 is integrally linked with the description of the FIU in s.2.5, and the two texts need to be complementary and not duplicative.

the year in which the transactions were conducted. There is no specific requirement to make such records available to auditors.

Effectiveness and efficiency

728. During the on-site visit, the evaluators noted that, even in the absence of a specific requirement to pay special attention to unusual transactions, to some extent several financial institutions appeared to conduct an analysis of such transactions.

729. As stated in the analysis above, the manner in which Article 8a paragraph 1 is drafted could potentially detract the focus from complex, unusual large transactions or unusual patterns of transactions, which is the primary purpose of Recommendation 11.

730. The evaluators were informed that the FIU issued specific guidance on this matter to assist financial institutions in the effective application of this requirement. However, the evaluators were not in a position to assess the quality of such guidance since it was not made available to the evaluators.

Recommendation 21 (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

731. In the 3rd round evaluation, Poland was rated 'Non-Compliant' with respect to Recommendation 21 since none of the criteria under the standard had been implemented.

Special attention to countries not sufficiently applying FATF Recommendations (c. 21.1 & 21.1.1),

732. There is no express requirement for reporting entities to pay special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF recommendations.

733. The Polish authorities indicated that Article 10a (3) of the AML/CFT Act requires financial institutions to consider the geographical risk in the course of their risk analysis when establishing a business relationship or carrying out a transaction. However, the evaluators do not consider this article to cover the requirements under Recommendation 21 directly.

734. Nevertheless, Article 8a paragraph 1 partially covers criterion 21.1, since it requires financial institutions to carry out on-going analysis of all transactions. Therefore, in terms of this article, the evaluators believe that financial institutions are required to analyse transactions with persons from or in countries which do not or insufficiently apply the FATF recommendations. However, the requirement does not extend to business relationships.

735. With respect to criterion 21.1.1 the Polish authorities pointed out that the FATF public documents are published on the website of the PFSA and the GIFI and are therefore publicly-available. However, the evaluators noted that although the website of the PFSA contains a reference to the FATF public documents, the relevant link to the FATF website does not function properly. Additionally, the FATF public documents issued in 2012 were not available on the website of the GIFI.

Examination of transactions with no apparent economic or visible lawful purpose from countries not sufficiently applying FATF Recommendations (c 21.2)

736. Article 8a paragraph 1 requires financial institutions to analyse all transactions. Therefore, financial institutions are technically required to examine as far as possible the background and purpose of transactions which have no apparent economic or visible lawful purpose from countries that do not apply or insufficiently apply the FATF Recommendations. Additionally, financial institutions are required to document in paper or electronic format the results of the analysis of all transactions.

737. There is no specific requirement to make the written findings available to auditors.

Ability to apply counter measures with regard to countries not sufficiently applying FATF Recommendations (c 21.3)

738. There is no specific provision which empowers competent authorities to apply appropriate counter-measures where a country continues not to apply or insufficiently applies the FATF recommendations. Nevertheless the PFSA remarked that it may issue recommendations to the financial market or send letters of advice in order to apply such counter-measures.

Effectiveness and efficiency

739. Meetings with the representatives of financial institutions demonstrated an adequate level of understanding on the manner in which customers from or in countries included in the FATF public documents are to be treated.

740. Notwithstanding the adequate level of understanding by financial institutions with regard to the requirements under Recommendation 21, the evaluators noted that insufficient guidance is provided by the PFSA and the GIFI regarding the FATF public documents.

3.6.2 Recommendations and comments

Recommendation 11

741. The Polish authorities should consider introducing a specific requirement to pay special attention to all complex or unusual transactions and unusual patterns of transactions.

742. Moreover, a requirement to make transaction records available to auditors should also be included in the law.

Recommendation 21

743. The Polish authorities should revise the entire provisions dealing with Recommendation 21. In particular, a specific requirement to give special attention to business relationships with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be introduced.

744. The written findings in relation to the analysis of transactions that have no apparent economic or visible lawful purpose should be available to assist auditors.

745. Competent authorities should be empowered to apply appropriate counter-measures.

746. The PFSA and GIFI should provide further assistance to financial institutions regarding the practical implementation of the requirements under Recommendation 21.

3.6.3 Compliance with Recommendations 11 and 21

	Rating	Summary of factors underlying rating
R.11	**LC**	• There is no specific requirement to make transaction records available to auditors; **Effectiveness:** • The manner in which Article 8a paragraph 1 is drafted could potentially detract the focus from complex, unusual large transactions or unusual patterns of transactions.
R.21	**PC**	• There is no requirement to give special attention to business relationships with persons from or in countries which do not or

		insufficiently apply the FATF Recommendations; • There is no requirement to make written findings available to assist auditors; • There is no requirement to apply appropriate counter-measures; **Effectiveness:** • The effectiveness of the measures which are in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries is debatable.

3.7 Suspicious Transaction Reports and Other Reporting (R. 13 and SR.IV)

3.7.1 Description and analysis[34]

Recommendation 13 (rated PC in the 3rd round report) & Special Recommendation IV (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

747. Recommendation 13 was rated 'Partially Compliant' in the third evaluation round based on the following factors:

- Attempted transactions were not covered;
- Financing of terrorism was only partially covered;
- Low number of reports outside the banking sector raised issues of effectiveness of implementation.

748. Special Recommendation IV was rated 'Partially Compliant' based on the fact that the reporting obligation in respect of financing of terrorism was insufficiently wide.

749. Following the third evaluation round, the AML/CFT Act was amended to address some of these deficiencies.

Requirement to Make STRs on ML/FT to FIU (c. 13.1, c.13.2 & IV.1)

750. According to the AML/CFT Act, obligated institutions are required to report suspicious transactions to the GIFI under Article 11 paragraph 1 of Chapter 4 (which deals with the provision of information to the GIFI) and Article 16 paragraph 1 of Chapter 5 (which deals with the suspension of suspicious transactions and freezing of accounts).

751. Article 8 paragraph 3 of the AML/CFT Act requires any obligated institution conducting a transaction to register such transaction when circumstances may suggest that it is related to money laundering or terrorist financing, regardless of its value and character. After the transaction is registered, paragraph 1 of Article 11 requires obligated institution to submit this information to the GIFI. Article 12 paragraph 1 defines what specific documents should be stored under Article 8 paragraph 3. Article 12 paragraph 2 requires obligated institutions to forward information on transactions registered in accordance with Article 8 paragraph 3 to the GIFI immediately (i.e. when the circumstances may suggest that the transaction is relation to ML/TF).

752. The other reporting requirement is found under paragraph 1 of Article 16. According to this article, any obligated institution which is requested to carry out a transaction, or has carried out a

[34] The description of the system for reporting suspicious transactions in s.3.7 is integrally linked with the description of the FIU in s.2.5, and the two texts need to be complementary and not duplicative.

transaction, or is aware that a customer intends to carry out a transaction suspected to be related to ML/TF, the obligated institution is obliged to report to the GIFI. Obligated institutions are required to indicate whether the transaction is to be suspended or the account blocked.

753. The representatives of the GIFI confirmed that Article 16 paragraph 1 deals with *ex-ante* reporting. They indicated that this provision requires obligated institutions to report imminent suspicious transactions before they are carried out. It is to be noted, however, that there is no specific preceding requirement on obligated institutions to refrain from carrying out a transaction before informing the GIFI. Obligated institutions are only prohibited from carrying out the suspicious transaction after a report is submitted to the GIFI (in terms of Article 16(4)).

754. On the other hand, according to the Polish authorities, Article 11 paragraph 1 deals with *ex-post* reporting. The representatives of GIFI explained that this requirement covers reporting of suspicions that are formed after a transaction has been carried out. For instance, they referred to a situation where a suspicion is formed by the obligated institution on a particular customer following the emergence of reports in the media indicating that the customer had been involved in criminal activities. At that point, the obligated institution scrutinises the transactions of the customer in the light of the media reports and identifies a number of transactions that may possibly have been related to ML/FT. The obligated institution then proceeds to submit such information to the GIFI. The representatives of the GIFI indicated that under Article 11 paragraph 1, obligated institutions either report a single transaction or else a cluster of suspicious transactions which are referred to as suspicious activity reports (SAR) in table provided under the part *Effectiveness*.

755. Notwithstanding the explanations provided by the authorities, the evaluators noted that a combined reading of Articles 8 paragraph 3 and Article 11 paragraph 1 contains a requirement which is very similar to that found under Article 16 paragraph 1. Whereas Article 8 paragraph 3 refers to an obligated institution 'conducting a transaction', Article 16 paragraph 1 refers to an obligated institution which has received a request to carry out a transaction. The distinction between the two requirements is therefore not very clear. In fact, the authorities themselves appeared to be hesitant when requested to clearly distinguish between the different provisions. Additionally, the legal basis for the reporting of transactions in relation to which a suspicion was identified after the event (*ex-post*) and the reporting of SARs under Article 11 paragraph 1 is very tenuous. The authorities did not provide statistics clearly distinguishing between the reports submitted to the GIFI under Article 11 paragraph 1 and Article 16 paragraph 1.

756. The reporting requirements under Article 11 and Article 16 only refer to transactions suspected of ML/TF and not to funds that are the proceeds of a criminal activity. Therefore, the reporting obligation is narrower than the requirement under criterion 13.1. From information gathered by during the on-site visit, the evaluation team concluded that in practice financial institutions submit reports to the GIFI when a transaction is suspected to be related to criminal activity, even though this is not prescribed by AML/CFT Act.

757. As to reporting of TF suspicions (c.13.2*, IV.1), both Article 11 paragraph 1 and Article 16 paragraph 1 also refer to 'terrorism financing'. Nevertheless, as mentioned above, the reporting requirement only refers to transactions and not to the suspicion that funds are linked or related, or to be used, for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism. Furthermore, the shortcomings identified in relation to Article 165a on the criminalisation of terrorist financing restrict the scope of the TF reporting requirement.

No Reporting Threshold for STRs (c. 13.3 & c. SR.IV.2)

758. The reporting requirements under Articles 11 and 16 are not subject to any threshold limitations.

759. Article 16 paragraph 1 covers attempted transactions, since it requires obligated institutions to report when they are in possession of information indicating that a customer intends to carry out a suspicious transaction. However, no similar requirement is found under Article 11 paragraph 1. The

Polish authorities informed the evaluation team that obligated institutions sent 72 STRs related to attempted transactions under Article 16 of the AML/CFT Act.

Making of ML/FT STRs regardless of Possible Involvement of Tax Matters (c. 13.4, c. IV.2)

760. Reporting entities are required to report suspicions of ML/FT irrespective of the nature of the underlying activity.

Additional Elements – Reporting of All Criminal Acts (c. 13.5)

761. According to Article 111 paragraph 1 of the Criminal Code of Poland the liability for an act committed abroad is subject to the condition that liability for such an act is likewise recognised as an offence, by a law in force in the place of its commission. In view of this requirement this additional element is not covered.

Effectiveness and efficiency R.13

762. The reporting entities which the evaluators met with during the on-site visit demonstrated a high-level of awareness of the suspicious transaction reporting requirements and appreciated the FIU Reporting Guide. Additionally, despite of some technical deficiencies in the reporting requirement under R.13, the evaluation team acknowledges that in practice the STR regime in Poland is comprehensively and accurately established and that financial institutions submit reports to the GIFI when a transaction is suspected to be related to a criminal activity, even though this is not prescribed by the AML/CFT Act.

763. As indicated in the table below, in 2007 the GIFI received 25,372 ML reports from financial institutions. The figures decreased in 2008 and 2009 (18,967 and 12,693 respectively) as a result of an improved internal-filtering process of suspicious transactions following an increase in awareness-raising and training programmes organised by the GIFI. According to the Polish authorities, although the numbers were lower in 2008 and 2009, the quality of the STRs was considerably higher and produced more effective results. Indeed, in 2009 the largest number of cases was opened compared to the number of reports received (see Table 18 under Recommendation 26). Following 2010, a steep rise of received STRs was again noted, culminating in 2011 with 26,817 ML reports submitted by financial institutions. The reason for this significant increase may be attributed to an increase in SARs, which may consist of several reported transactions. Additionally, the changes relating to the reporting regime as a result of the AML/CFT Act and continuous outreach to reporting entities may have also been a contributing factor.

764. The highest number of ML reports was filed by banks. In fact, banks have submitted 87% of the total number of reports received by the GIFI. The other significant contributors were investment funds, cooperative units, brokerage houses and insurance companies. However, the evaluators noted with concern that the number of reports submitted by investment funds and insurance companies has been declining. The reporting pattern of investment funds appears to be rather unusual. For instance, in 2007 only 3 reports were submitted followed by 2,875 in 2008. By 2010 the number of reports dwindled to a mere 169. No clear explanation was provided in relation to this reporting pattern. On the whole, it appears that all financial institutions, bar currency exchange offices, are active in submitting reports to the GIFI.

765. As noted under Recommendation 26, the number of ML cases opened by the GIFI on the basis of STRs/SARs is on average 1,300. Although the discrepancy between the number of submitted reports and the number of opened cases is significant, the evaluators believe that the quality of reports submitted by financial institutions is adequate.

Table 23: Number of ML STRs/SARs by category of financial institutions

Reporting Entities	2007	2008	2009	2010	2011	01.01.2012-31.03.2012	Total
Banks, foreign banks branches, branches of credit institutions	23,484	14,307	10,458	15,572	24,658	7,147	**95,626**
Investment funds, investment funds societies	3	2,875	1,062	169	78	22	**4,209**
Leasing or factoring activity	8	4	14	29	123	15	**193**
Co-operative savings and credit banks	135	421	291	96	152	25	**1,120**
Insurance companies	969	591	215	209	149	38	**2,171**
Brokerage houses or other entities engaged in brokerage activities	84	234	146	559	1,041	483	**2,547**
Joint Stock Company National Depositary for Securities	0	0	0	0	0	0	**0**
Post office	0	0	6	6	3	0	**15**
Currency exchange	13	7	1	5	69	22	**117**
Cooperative units	676	528	500	535	523	590	**3,352**
Other financial institutions	0	0	0	13	21	0	**34**
Total	**25,372**	**18,967**	**12,693**	**17,193**	**26,817**	**8,342**	**109,384**

Table 24: Number of TF STRs/SARs by category of financial institutions

Reporting Entities	2007	2008	2009	2010	2011	01.01.2012-31.03.2012	Total
Banks, foreign banks branches, branches of credit institutions	194	15	47	8	19	-	**283**

Investment funds, investment funds societies	-	-	-	-	-	-	-
Leasing or factoring activity	-	-	-	4	-	-	**4**
Co-operative savings and credit banks	-	-	-	1	-	-	**1**
Insurance companies	1	1	1	1	-	-	**4**
Brokerage houses or other entities engaged in brokerage activities	-	-	-	-	-	-	-
Joint Stock Company National Depositary for Securities	-	-	-	-	-	-	-
Post office	-	-	1	1	2	-	**4**
Currency exchange	-	-	-	-	1	-	**1**
Cooperative units	-	-	-	-	-	-	
Other financial institutions	-	-	-	-	-	-	**1**
Total	**195**	**16**	**49**	**15**	**22**	**-**	**298**

766. In total 298 reports of TF suspicions were reported. As in the case of ML reports, the highest number of TF reports was submitted by banks (95%). Very few other entities submitted a TF report. It is interesting to note that the Post Office, as a MVTS, submitted 4 TF reports. The other entities that submitted a TF report were leasing companies (4), cooperative savings and credit banks (1), insurance companies (4), currency exchange (1) and other financial institutions (1). The GIFI opened 60 TF cases in total. Nevertheless, the number of notifications sent to the Intelligence Services Agency was 99. The notifications forwarded to the ISA did not lead to any indictments or convictions.

3.7.2 Recommendations and comments

Recommendation 13 and Special Recommendation IV

767. The scope of the ML reporting requirement should be extended to the reporting of "funds" suspected to be the proceeds of a criminal activity.

768. The FT reporting obligation should be extended to "funds" as required under Criterion 13.2.

769. The reporting requirement under Article 11 paragraph 1 should expressly provide for attempted transactions.

770. The Polish authorities should revise the legal text of the entire reporting regime to remove any overlaps between the requirements under Article 11 and 16, to provide for a clear legal basis for the reporting of suspicious activity reports.

3.7.3 Compliance with Recommendation 13 and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13	**PC**	• The scope of the reporting requirement is only linked to transactions related to ML/TF and does not extend to the reporting of "*funds"* suspected to be the proceeds of a criminal activity; • The FT reporting obligation is limited to *"transactions"* related to FT and does not extend to *"funds"*; • The deficiencies identified with respect to Recommendation 1 and Special Recommendation II restrict the scope of the reporting requirement; • Possible confusion between reporting obligations under Articles 8.3, 11.1 and 16 (e.g. attempted transactions are not covered under Article 11.1).
SR.IV	**PC**	• The FT reporting obligation is limited to *"transactions"* related to FT and does not extend to *"funds"*; • The deficiencies identified with respect to Special Recommendation II restrict the scope of the reporting requirement; • Possible confusion between reporting obligations under Articles 8.3, 11.1 and 16 (e.g. attempted transactions are not covered under Article 11.1).

3.8 Foreign Branches (R.22)

3.8.1 Description and analysis

Recommendation 22 (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

771. In the 3rd round evaluation Poland was rated 'Non-Compliant' with respect to Recommendation 22. It was noted that there was no provision in the law dealing with the requirement for financial institutions to ensure that their branches and subsidiaries situated in a foreign jurisdiction apply AML/CFT procedures consistent with the home-country requirements.

772. Pursuant to the amended AML/CFT Act, financial institutions are now required to ensure that branches located in non-EU member states comply with measures that are consistent with the AML/CFT Act. The Polish authorities informed the evaluators that all the branches/subsidiaries of Polish financial institutions are situated within EU member states, with one exception (a subsidiary situated in Ukraine).

Consistency of the AML/CFT measures with home country requirements and the FATF recommendations (c. 22.1 & 22.2)

773. According to Article 9j (1) of the AML/CFT Act, financial institutions are required to apply the requirements set out in the AML/CFT Act in their branches and subsidiaries situated in countries outside the EU.

774. The scope of the requirement does not extend to branches and subsidiaries of the institutions located in EU Member States. Nevertheless, it is presumed that AML/CFT obligations in EU Member States are equivalent to those existing in Poland due to the fact that all EU Member States are obliged to implement the 3rd EU AML/CFT Directive. Hence, foreign branches and subsidiaries of Polish institutions are considered to be obliged entities under the relevant AML/CFT legislation of other EU Member States.

775. Pursuant to Article 9j (2) where it is impossible to comply with the obligations set out in the AML/CFT Act, financial institutions are required to carry out all necessary measures in order to effectively prevent money laundering and financing of terrorism. In terms of Article 9j(3) financial institutions are required to inform their subsidiaries and affiliates of the AML/CFT policies and internal procedures implemented within the financial institution.

776. The AML/CFT does not provide for those situations where the minimum AML/CFT requirements of the host and home countries differ. There is therefore no requirement for financial institutions to apply the higher standard of AML/CFT measures in such circumstances. The requirement to inform the home country supervisor where the application of equivalent AML/CFT measures is impossible is not reflected in Polish legislation.

Additional elements (c. 22.3)

777. According to Article 9j of the AML/CFT Act, any obligated institution with its branches and subsidiaries in the territory of non-EU member-states shall apply the CDD measures defined in the Act in those branches and subsidiaries. The Polish authorities explained that this is a general requirement and in this respect financial institutions subject to the Basel Core Principles are required to apply a consolidated CDD measures at the group level.

Effectiveness and efficiency

778. As mentioned above, with the exception of one subsidiary operating in Ukraine, all the branches/subsidiaries of Polish financial institutions are situated within EU member states. Therefore, it is presumed that all such branches and subsidiaries are subject to AML/CFT measures which are equivalent to those in Poland.

3.8.2 Recommendation and comments

Recommendation 22

779. Poland has to some extent implemented the Recommendation 22 in its legislative acts as recommended in the 3rd round evaluation report.

780. However, the Polish authorities should take further steps to completely align their legislative provisions with the requirements under Recommendation 22. In particular, a requirement should be introduced for foreign branches and subsidiaries of Polish financial institutions to apply higher standards when the AML/CFT requirements of home and host countries differ.

781. Additionally, financial institutions should be required to inform the home country supervisor where it is impossible to apply AML/CFT measures which are at least equivalent to those in force in Poland.

3.8.3 Compliance with Recommendation 22

	Rating	Summary of factors underlying rating
R.22	**LC**	• There is no explicit obligation for branches and subsidiaries of Polish financial institutions established in a foreign jurisdiction to apply higher standards when the AML/CFT requirements of home and host

		countries differ; • There is no requirement to inform the home country supervisor where it is impossible to apply AML/CFT measures which are at least equivalent to those in force in Poland.

3.9 Shell Banks (R.18)

3.9.1 Description and analysis

Recommendation 18 (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

782. In the third round evaluation, Poland was rated 'Partially Compliant' with respect to Recommendation 18 as the legal framework did not prohibit financial institutions from entering into, or continuing, correspondent banking relationships with shell banks, nor required them to satisfy themselves that respondent institutions in a foreign country do not permit accounts to be used by shell banks.

Prohibition of establishment of shell banks (c. 18.1)

783. As it was noted in the 3rd round evaluation report, the establishment of a bank is subject to licensing by the PFSA according to Article 30 of the Banking Act (which, among other criteria, requires banks to have premises equipped with technical facilities). Therefore, the establishment of shell banks is not permitted in terms of Polish legislation.

784. Article 2 (1c) of the amended AML/CFT Act introduced a new definition of shell banks which slightly falls short of the one provided in the Glossary of the FATF Methodology insofar as it does not specify that the financial group of which the bank forms part of should be subject to effective consolidated supervision.

Prohibition of correspondent banking with shell banks (c. 18.2)

785. Pursuant to Article 9f of AML/CFT Act, obligated entities are not permitted to enter into, or continue, correspondent banking relationships with a shell bank or a bank that holds accounts for a shell bank. This prohibition was introduced to implement the recommendations provided in the 3rd evaluation report.

786. According to Article 34a (7) of the AML/CFT Act, an obligated institution which establishes and maintains cooperation with a shell bank shall be subject to a financial sanction.

Requirement to satisfy respondent financial institutions of use of accounts by shell banks (c. 18.3)

787. Article 9f (2) of the AML/CFT Act prohibits financial institutions from establishing and maintaining a correspondent banking relationship with a respondent institution which enters into arrangements and contracts with shell banks.

788. The GIFI published guidance which contains reference to the treatment of shell banks and provides an e-learning platform for obligated institutions and cooperating entities regarding the implementation of this requirement. Furthermore, the PFSA provides on-going training for financial institutions on the requirements relating to the establishment and maintenance of correspondent banking relationships.

Effectiveness and efficiency

789. During the on-site visit the evaluators were not aware of any shell banks operating in Poland or any banks which had corresponding relations with shell banks or those banks that allowed shell banks

to use its accounts. Representatives of financial institutions demonstrated that they apply proper risk policies when establishing a business relationship *inter alia* before establishing correspondent banking relationship.

3.9.2 Recommendation and comments

790. Poland has implemented most of the recommendations made in the 3rd round report in relation to Recommendation 18 within its legislative framework. However, it is recommended that the definition of a "shell bank" be amended to specify that a shell bank will qualify as such if, *inter alia*, it is not part of a financial group which is subject to effective consolidated supervision.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	**C**	

Regulation, supervision, guidance, monitoring and sanctions

3.10 The Supervisory and Oversight System - Competent Authorities and SROs / Role, Functions, Duties and Powers (Including Sanctions) (R. 23, 29 and 17)

3.10.1 Description and analysis

Authorities/SROs roles and duties & Structure and resources

Recommendation 23 (23.1, 23.2) (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

791. In the Third Round Evaluation, Poland was rated 'Partially Compliant' with respect to Recommendation 23. The main concerns of the evaluators were the lack of sector-specific regulations issued by financial supervisors and the explicit unwillingness of certain supervisors to be involved in training and in issuing regulations/guidelines to assist obligated entities.

Regulation and Supervision of Financial Institutions (c. 23.1)

792. All financial institutions are subject to the AML/CFT Act and are therefore subject to the supervision of the GIFI and other supervisory authorities, including the PFSA, the NBP and the NSCCU[35]. Further provisions on the regulation and supervision of financial institutions are found in the sector-specific laws and in GIFI guidelines.

Designation of Competent Authority (c. 23.2)

793. Pursuant to Article 21 (1) of the AML/CFT Act, the monitoring of compliance by obligated institutions with AML/CFT requirements – except for the NBP – is exercised by the GIFI.

794. The supervisory powers of the GIFI are set out under Article 4 paragraph 1 of the AML/CFT Act, which states that the GIFI shall be responsible for monitoring compliance with AML/CFT requirements and initiating/undertaking other measures to counteract ML/FT, including training provided to the personnel of the obligated institutions within the responsibilities imposed on these institutions.

[35] Since 27 October 2012 the PFSA is responsible for the supervision over co-operative savings and credit unions and the National Association of Co-operative Savings and Credit Unions. Nonetheless the NCCSU can also supervise savings unions.

795. According to Article 21 (3), monitoring of compliance may also be carried out by the PFSA, NBP and NSCCU within their supervisory competences. The PFSA is responsible for the supervision of all financial institutions in Poland except for foreign exchange offices and savings and credit unions, which are supervised by the NBP and the NSCCU respectively.

796. In terms of Article 21 paragraph 3b, the PFSA, the NBP and the NSCCU are required to submit their on-site compliance schedule to the GIFI within two weeks of the completion of the plan. The purpose of this submission is to inform the GIFI in order to avoid duplication and prepare the final version taking into account the recommendations of the GIFI. The plan includes the number and type of institutions to be inspected. Nonetheless, there is no specific date in the AML/CFT Act or other legislation for completion of the on-site visit plan.

797. The Department of National Operations of NBP provides the on-site inspection plan to the GIFI biannually. These plans originate in the Voivodship offices of the NBP. The plans forwarded in an electronic form (Excel format) according to the specimen proposed by the GIFI. The GIFI is immediately notified in the event of any changes to the plan.

798. The GIFI and the financial supervisors carry out on-site inspections independently of each other. During the on-site visit planning process the supervisory authorities are informed about the GIFI's examination plan. The GIFI co-ordinates the planning process.

Recommendation 30 (all supervisory authorities) (rated LC in the 3rd round report)

799. In the 3rd round evaluation the number of AML/CFT experts within the Polish supervisory authorities was deemed to be insufficient, especially within the PSEC. Furthermore, the evaluators determined that CFT training was needed for financial supervisors. Most of these shortcomings have been addressed by the PFSA.

800. The Act on Financial Market Supervision provides for the independence of the PFSA from the government and for its independent funding. The Act also sets out provisions to ensure that the employees of the PFSA display high integrity in the fulfilment of their functions. Employees are required to undergo a clearance procedure when applying for a position within the PFSA.

Adequately structured (including operational independence), staffed and funded and provided with sufficient technical and other resources (c. 30.1)

GIFI

801. For a detailed explanation on the structure, operational independence, funding and technical and other resources of the GIFI, reference may be made to Section 2.5 of the report. According to an organisational chart of the GIFI, the compliance monitoring function of the GIFI is carried out by the Control Unit of the Department of Financial Information which consists of eight officers.

PFSA

802. The provisions governing the establishment, funding and independence of the PFSA are set out in the Act on Financial Market Supervision.

803. According to Article 5 of the Act on Financial Market Supervision, the FSA is to be composed of a Chairperson, two Vice-Chairpersons and four members.

804. According to Article 7, the Chairperson of the FSA is appointed by the President of the Polish Council of Ministers for a five-year term. Pursuant to Article 8, the Chairperson cannot be dismissed without a sufficient cause:

> *1. The President of the Polish Council of Ministers shall dismiss the FSA's Chairperson before the expiry of his (her) term of office only if the Chairperson:*
>
> *1) has been convicted of an intentional offence or a fiscal offence by way a final and binding judicial decision, or*

2) has resigned from the position, or

3) has lost Polish citizenship, or

4) has lost the ability to perform his (her) duties as a result of a prolonged illness, lasting more than three months.

2. The term of office of the FSA's Chairperson shall expire upon the Chairperson's death or dismissal.

805. The PFSA is serviced by the Office of the PFSA, whose work is supervised by the Chairperson and Vice-Chairpersons. The organisational rules are established by an order of the Prime Minister. The unit within the PFSA which is in charge of AML/CFT supervision of financial institutions is situated within the Banking and Payment Institutions' Inspections Department[36]. The unit is composed of six officers.

806. The financing of the PFSA and the remuneration of the Chairperson, the Vice-Chairpersons and the employees is provided for under Articles 19 and 20 of the Act:

Art. 19

The expenses representing costs of the operations of the FSA and the FSA Office, in the amount specified in the budget act, including remuneration and bonus awards payable to the FSA's Chairperson and Vice-Chairpersons and the employees of the FSA Office shall be financed from the fees paid by the regulated entities, in the amount and on terms stipulated in the Acts referred to in Art. 1 (2).

Art. 20

1. Remuneration and bonus awards payable to the FSA's Chairperson and Vice-Chairpersons and the employees of the FSA Office should be established at a level ensuring efficient exercise of supervision over the financial market and the accomplishment of the purpose specified in Art. 2.

2. The President of the Polish Council of Ministers shall define, by way of a regulation, the manner of establishing the amount of funds to be appropriated for payment of remuneration and bonus awards to the FSA's Chairperson and Vice-Chairpersons, and determining the amount of such remuneration and bonus awards, as well as the manner of establishing the amount of funds to be appropriated for payment of remuneration and bonus awards to employees of the FSA Office, taking into account the organisation of the FSA and the FSA Office, within the scope of exercised supervision and the level of salaries in the regulated institutions.

NBP and NSCCU

807. The only information provided by the NBP regarding this criterion was the number of inspectors who conduct inspections on foreign exchange offices. The evaluators were informed that there are 121 inspectors. However, the inspectors do not exclusively conduct AML/CFT inspections. No information was provided by the NSCCU.

Professional Standards and Integrity (c. 30.2)

GIFI

808. For a detailed explanation on the structure, operational independence, funding and technical and other resources of the GIFI, reference may be made to Section 2.5 of the report.

[36] Since October 2012 the name has changed to Banking, Payment Institutions and Cooperative Savings and Credit Unions Inspections' Department.

PFSA

809. The Chairperson, the Vice-Chairpersons, the members of the FSA and the employees of the Office are required to observe a code of ethics which details the obligations of the employees in relation to their functions. Additionally, a number of internal regulations have been issued to govern the functioning of PFSA activities (including public speaking of employees). Furthermore, Article 15 of the Act on Financial Market Supervision states that officers of the PFSA may not hold certain equity interests in entities which are subject to the FSA's supervision, may not be members of such entities' governing bodies or be employed at such entities and may not perform any other actions which would be in conflict with their duties or which could give rise to a suspicion of partiality or self-interest.

810. According to Article 16 of the Act on Financial Market Supervision, officers of the PFSA have an obligation to maintain secrecy even after their employment has been terminated.

NBP and NSCCU

811. No information was provided by the NBP and the NSCCU.

Adequate Training (c. 30.3)

812. The Polish authorities informed the evaluation team that the inspectors of all financial supervisors participate in an annual E-learning course provided by the GIFI. The inspectors of the PFSA who conduct AML/CFT monitoring also participate in international training (such as 3L3 training organised by BAFIN).

813. The PFSA delivers anti-money laundering and terrorism financing training to its inspectors on a regular basis. According to the information provided by the Polish authorities, representatives of the PFSA, who participate in different international forums, seminars, trainings, are providing training to other inspectors of the PFSA. Furthermore, the authorities pointed out that handbooks were drawn up internally, which contain detailed rules of conduct for the inspectors.

814. The PFSA provides training both for financial institutions and other authorities. Since 2008 seminars on current AML/CFT issues and on the new amended AML/CFT Act have been provided to all supervised entities. Furthermore, training was provided on "Group level compliance on AML/CFT in cross-border financial groups in the EU", "Risk assessment and the risk-based approach to AML/CFT", "The New FATF Standards on AML/CFT". Other seminars are held at the request of other governmental institutions: a series of training programmes were provided to the Police Force, the Polish Internal Security Agency (on-going training programme), the Polish Border Guard, the Polish Anti-Corruption Office, the Polish Prosecutors' Office, and the notaries' public SRO.

815. Every year all the inspectors of the NBP who are responsible for the inspection of foreign exchange offices participate in internal seminars organised by the NBP in collaboration with the GIFI representatives.

Authorities' powers and sanctions

Recommendation 29 (rated LC in the 3rd round report)

Summary of 2007 factors underlying the rating

816. In the 3rd round evaluation the evaluators found that complex AML/CFT on-site inspections including review of policies, procedures and sample testing were not being carried out, particularly within the securities sector.

817. This issue has since been broadly addressed.

Power for Supervisors to Monitor AML/CFT Requirement (c. 29.1)

818. Pursuant Article 21 paragraph 1, the GIFI is responsible for monitoring financial institutions' compliance with the requirements under the AML/CFT Act. Paragraph 2 of the same article states that compliance monitoring shall be carried out by employees of the Department of Financial Information which assists the GIFI.

819. Furthermore, Article 21 paragraph 3 states that compliance monitoring of financial institutions may also be carried out by the PFSA, the NBP and the NSCCU within the legislative framework setting out the powers and functions of such supervisory authorities.

820. The supervisory powers, functions and responsibilities of the PFSA in relation to banks are set out under Chapter 11 of the Banking Act; in relation to insurance the relevant provisions are found under Chapter 12 of the Act on Insurance Activity; with respect to securities, the relevant provisions are set out under the Act on Capital Market Supervision; with respect to payment services, the relevant provisions are found under the Act on Payment Services.

821. Article 52 paragraph 2 states that the President of the NBP shall perform compliance monitoring tasks as determined by the provisions of Foreign Exchange Act. The Act contains the supervisory powers of the NBP with respect to foreign exchange offices.

822. The supervisory framework of the NSCCU with respect to savings and credit unions is contained in Articles 33 to 35 of the Credit Union Act of December 14, 1995.

Authority to Conduct AML/CFT Inspections by Supervisors (c. 29.2); Power for Supervisors to Compel Production of Records (c. 29.3 & 29.3.1)

GIFI

823. Pursuant to Article 21 paragraph 2 on-site inspections are carried out by the employees of the Department of Financial Information assisting the GIFI. This function is carried out by the Control Unit of the Department.

824. The procedure for an on-site inspection is covered by Article 22 of the AML/CFT Act. In the course of an on-site inspection, the inspectors may request financial institutions to disclose all documents and materials necessary for the proper monitoring of compliance. Financial institutions are required to immediately present documents and material for inspection when so requested and to provide timely explanations to inspectors. The inspectors are entitled to access the facilities and premises of the financial institution, to view documents which are necessary within the scope of the visit and to obtain certified copies of such documents and to demand verbal and written explanations from the employees of the financial institution being inspected. In the fulfilment of their functions the inspectors are entitled to the protection provided for under the Penal Code to public servants.

825. On-site inspections carried out by the Control Unit of the GIFI include the review of internal written procedures and documents collected and stored in compliance with the obligations set out under the AML/CFT Act. Inspectors also ensure that a record of transactions is properly maintained and that transaction reports are submitted to the GIFI in accordance with the applicable procedures by means of sample testing. As a general rule, all the obligations under the AML/CFT Act are reviewed during the on-site visit and the on-site team bases its conclusions and findings on sample testing and the review of documents. On average, an on-site inspection carried out by GIFI takes approximately one to three weeks depending on the ML/FT risks posed by the inspected entity and the complexity of the on-site inspection.

PFSA

826. According to Chapter 11 Article 133 paragraph 3 of the Banking Act, inspection activities shall be carried out by employees of the PFSA, who are required to produce the official identification card

and provide the authorisation granted by the Chairperson of the Polish Financial Supervision Authority.

827. On-site inspections of insurance undertakings are carried out by the PFSA in terms of Article 208 of the Act on Insurance Undertakings. Article 208 paragraph 4 states that inspectors shall have the right to:

1) admission to all premises of the inspected insurance undertaking;
2) free access to a separate office room and means of communication;
3) have access to all documents of the inspected insurance undertaking, and to request copies, duplicates and excerpts of these documents;
4) have access to the data included in the information system of the inspected insurance undertaking and to request copies or excerpts of those data, including in electronic form;
5) have access to all documents of the insurance intermediary of the inspected insurance undertaking and to request copies, duplicates and excerpts of those documents;
6) demand oral or written requests of explanations, including in electronic form, from the persons employed under an employment contract, commission contract or remaining in another legal relationship of a similar nature with the insurance undertaking, and from insurance agents of the inspected insurance undertaking;
7) request the preparation of the required data, including in electronic form;
8) secure documents and other evidence.

828. With respect to securities, inspections may be carried out pursuant to Articles 26 to 33 of the Act on Capital Market Supervision. These articles regulate the procedure that is to be followed in an on-site inspection, including the powers of inspectors within the context of an inspection.

829. Article 103 of the Act on Payment Services provides for the power of the PFSA to conduct on-site inspections of payment institutions. During an on-site inspection, the inspectors have the right to:

1) enter the premises of the entity being inspected;

2) free access to separate office accommodation and to communications facilities;

3) examine documents of the entity being inspected and to require the making of copies and extracts from those documents; and

4) examine data contained in the IT system of the entity being inspected and require the making of copies or extracts from those data, including in the form of electronic documents.

830. An AML/CFT on-site inspection by the PFSA is carried out in accordance with a written manual. The manual contains a detailed procedure to be followed by the inspectors which provides for the steps to be taken before the on-site inspection is carried out, the procedure to be followed during the on-site inspection and the post-inspection activities. In particular, during the on-site inspection, the inspector should at least establish whether the financial institution:

- Has appointed the person responsible for the compliance with the obligation set out in the Act;
- Drafted, enacted and is actually using the internal procedures establishing their AML/CFT regime, and are those procedures compliant with the provisions of the Act and the Regulation;
- Scrutinizes transactions using risk based approach;
- Includes the ultimate beneficial owner when scrutinizing transactions;
- Registers transactions and identifies customers according to the provisions of the Act and the Regulation;
- Keeps the transactions register and other documents related to the registered transactions, and the identification information for the period set out in the Act;

- Transfers correct information on the transactions, accounts and customers to the GIFI;
- Complies with GIFI's and prosecutors' orders to postpone a transaction or to block the account;
- Discloses gathered information according to the provisions of the Act and in the manner prescribed in it;
- Has taken all the necessary actions to verify should any of its customers or contractors, be a person mentioned in the provided by GIFI information on entities which might be suspected to be connected to acts of terrorism;
- Has provided the proper functioning of control mechanisms by separating the operational and control functions;
- Has engaged the OI's other operational units in the analysis of issues connected to AML/CFT;
- Has provided the participation of its employees in training programs on AML/CFT, according to article 10a paragraph 4 of the Act;
- Has engaged the internal audit in the analysis of issues connected to AML/CFT.

831. On average, an on-site inspection carried out by the PFSA takes approximately one to three weeks depending on the ML/FT risks posed by the inspected entity and the complexity of the on-site inspection.

NBP

832. The legal basis for on-site inspections carried out by the NBP on foreign exchange operators is set out under Article 2 paragraph 1 points 16-18 of the Foreign Exchange Act.

833. On-site inspections are carried out in accordance with a manual which provides for the procedure to be followed before, during and after an on-site inspection is carried out. During the on-site inspection, the inspectors are required to confirm, *inter alia,* whether the foreign exchange operator has an internal written AML/CFT procedure, whether training has been provided to employees, whether the register of transactions is properly maintained, whether CDD and record-keeping measures are carried out in accordance with the AML/CFT Act and whether a reporting procedure is in place.

834. According to the Polish authorities, the NBP checks whether the filing systems and programmes implemented by the obligated institutions satisfy the legal requirements. Additionally, the NBP checks the accuracy of the data sent to the GIFI. If the data is found to be incorrect the NBP makes a written recommendation to an exchange office, a copy of which is forwarded to GIFI. The NBP is not authorized to conduct sample purchases to monitor the registration of transactions.

835. On average, a visit by the NBP does not last longer than two hours. The evaluators are of the opinion that it is unlikely that an adequate review of the AML/CFT requirements implemented by a foreign exchange office is conducted within such a period of time.

836. Notwithstanding the fact that the on-site inspection procedure set out in the AML/CFT inspection manual of the NBP appears to be rather comprehensive, the evaluators noted that the level of appreciation of the ML/FT risks of the foreign exchange sector is rather low.

NSCCU

837. The NSCCU conducts on-site inspections in terms of Articles 33 to 35 of the Credit Union Act. No inspection manual has been prepared to assist inspectors during on-site inspections. The evaluators were informed that the average duration in the case of an inspection carried out by the NSCCU is 3 days. The evaluators noted with concern that the NSCCU does not appear to possess a satisfactory level of awareness of the AML/CFT risks associated with the savings and credit unions sector.

838. None of the supervisory authorities require a court order in order to compel production of or to obtain access for supervisory purposes.

Powers of Enforcement & Sanction (c. 29.4)

839. According to Article 21 (4) of the AML/CFT Act, upon the conclusion of an on-site inspection, a written report on the outcome of the inspection carried out by the PFSA, the NBP and the NSCCU is to be forwarded to the General Inspector within 14 days following its completion.

840. The on-site inspection report is forwarded by the Director of the Organisational Department of the GIFI to the director of the financial institution within thirty days from the completion of the on-site inspection (Article 24 paragraph 1). Before presenting the report to the financial institution, the Director of the Organisation Department may request the financial institution to submit additional clarifications in writing with respect to any shortcomings identified during the inspection. The inspection report contains findings of fact, an evaluation of the AML/CFT measures implemented by the financial institution and any shortcomings and conclusions identified by the inspectors (Article 24 paragraph 2). Additionally, the inspection report shall include recommendations to the financial institution to address any shortcomings identified and the period of time within which the financial institution is required to implement the recommendations made by the inspector. Pursuant to Article 25(4) financial institutions are obliged to submit to the GIFI within the term indicated in the post-inspection report information on the manner how recommendations were dealt with and the reasons for failure to address them.

841. Clause 10 paragraph 3 of the GIFI manual on on-site inspections states that the inspection report shall also require financial institutions to submit information on the manner in which the recommendations have been implemented within a specified deadline. Where those recommendations have not been implemented, the financial institution is required to provide the reasons and the estimated deadline within which such measures will be taken.

842. Once the inspection report is presented to the financial institution, the Director of the Organisational Department of the GIFI shall also submit the report to the supervisory authorities. In the event that a reasonable suspicion of a crime or offence is identified during an inspection, information is passed on to the Public Prosecutor's Office (Article 27 of the AML/CFT Act).

843. In terms of Article 21 paragraph 3a, the GIFI is the authority which is responsible for the imposition of sanctions for breaches of the AML/CFT Act. The sanctions are set out under Articles 34a to 34c. In addition, Chapter 8 provides for penalties with respect to breaches committed by a person who acts on behalf of or in the interest of the financial institution. The person who is responsible for the fulfilment of the financial institution's obligations under the AML/CFT Act is the person designated in accordance with Article 10b paragraph 1, who is a board member appointed by the management board (in the case commercial capital companies, cooperative or state banks) or the director (in the case of branches of foreign banks or credit institution). According to the Polish Authorities, when a notification is sent to the Public Prosecutor's Office in terms of Chapter 8, all persons involved in the breach (irrespective of whether they are directors or senior management) will be liable.

844. The GIFI, as the authority competent for the imposition of fines for AML/CFT violations, may initiate administrative proceedings *ex officio* for breaches of the AML/CFT Act (Article 34c paragraph 5) or send a notification to the Public Prosecutor's Office where a violation stipulated in Articles 35 or 36 is identified. In terms of Article 304 of the CPC, other supervisory authorities may also send a notification to the Public Prosecutor's Office where a violation stipulated in Articles 35 or 36 is identified.

845. Sanctions imposed by the GIFI are subject to the enforcement of payment under the provisions of the Polish administrative enforcement procedure.

Effectiveness and efficiency (R. 23 [c. 23.1, c. 23.2]; R. 29, and R. 30 (all supervisors))

846. The number of on-site visits conducted by the GIFI and financial supervisors is as follows:

Table 25: Number of conducted AML/CFT visits by entity and supervisor per year.

Type of supervisor	Type of financial institution	Number of visits conducted					
		2007	2008	2009	2010	2011	2012[37]
GIFI	Banks	9	3	10	2	3	3
	Credit institution branches	-	-	-	3	0	0
	Brokers	8	1	1	0	0	0
	Investment funds	6	4	1	0	0	1
	Insurance companies	2	2	2	0	0	4
	Cooperative banks	-	3	3	3	3	0
	Savings and credit unions	-	2	1	1	0	0
	Entities running factoring activities	-	-	-	-	2	3
	Leasing companies	-	-	-	-	-	3
	Payment institutions	-	-	-	-	-	1
PFSA	Banks	32	11	7	9	7	14
	Brokers	3	4	2	7	5	4
	Investment funds	-	-	1	2	7	5
	Cooperative banks	-	19	21	18	14	11
	Insurance companies	-	7	2	4	12	10
	Credit institution branches	-	-	7	8	3	0
NBP	Currency exchange offices	1,089	1,092	994	1,758	813	687
NSCCU	Savings and	25	15	22	22	13	19

[37] The figures represent the number of on-site visits conducted in the first half of 2012.

	credit unions						

Table 26: The total number of conducted AML/CFT visits by supervisor per year.

Type of supervisor	Year					
	2007	2008	2009	2010	2011	2012[38]
GIFI	25	15	18	9	8	15
PFSA	35	41	40	48	48	44
NBP	1,089	1,092	994	1,758	813	687
NSCCU	25	15	22	22	13	19

847. The figures indicate that the number of on-site inspections conducted on a yearly basis is more or less constant. The only exception is 2010, where the number of on-site inspections conducted by the NBP was significantly higher than other years. The NBP indicated that following the amendment of the AML/CFT Act on 22nd October 2009, a number of new obligations for financial institutions were introduced. Therefore, the NBP decided to increase the number of inspections to ensure that foreign exchange offices were adequately complying with these new obligations. In 2010 and 2011, the number of on-site inspections conducted by the GIFI decreased slightly when compared to other years. However, over the same period of time, there was a slight increase in the figures for the PFSA, possibly indicating that the PFSA took a more active role than the GIFI in those two years.

848. The evaluators noted that the inspections carried out by GIFI in 2011 and 2012 focussed on financial institutions which were included within the scope of the AML/CFT Law after 2010. The Polish authorities also indicated that in the future GIFI would focus more on the overall coordination of the supervision process and would delegate on-site inspection responsibilities to the supervisory authorities. Resources would be mainly allocated to the administrative sanctioning process and assistance to financial institutions on AML/CFT matters.

849. With respect to financial institutions, other than foreign exchange offices and savings and credit unions, the total number of on-site inspections carried out by the GIFI and the PFSA is on average 60 inspections per year. Compared to the number of financial institutions in Poland (which at the time of the on-site visit was 774), the number of inspections prior to implementation of the RBA appears to be on the low end of the scale. The evaluators are of the opinion that the number of on-site inspections is not sufficient to ensure that the entire financial sector is adequately complying with AML/CFT measures.

850. This is particularly the case with respect to certain financial institutions. For instance, with respect to cooperative banks the number of inspections carried out annually is on average 16 whereas the total number of cooperative banks at the time of the on-site inspection was 574. With respect to brokers, the average number of annual inspections is 5, whereas the total number of brokers is 52. As a result the gap between successive on-site inspections for certain financial institutions would be significantly long. The reason for the low number of inspections could possibly be attributed to the number of inspectors who conduct AML/CFT inspections. In particular, notwithstanding the fact that the PFSA is responsible for the entire financial sector, only six inspectors were allocated to the AML/CFT Unit (out of a total of one hundred and seventy four inspectors).

851. The number of on-site inspections conducted by the NBP and the NSCCU appears to be rather adequate. Nevertheless, the evaluators noted with concern that that the inspectors of the NSCUU do not appear to possess a satisfactory level of awareness of ML/FT risks.

[38] The figures represent the number of on-site visits conducted in the first half of 2012.

852. Monitoring of compliance within the Polish AML/CFT regime is mainly based on information gathered in the course of on-site inspections. Since financial institutions are not required to periodically submit information on their AML/CFT policies and procedures to the GIFI and other supervisory authorities, it is difficult for the authorities to conduct desk-reviews on the level of AML/CFT compliance by financial institutions. Therefore, for monitoring purposes, the GIFI and the other financial supervisors are obliged to rely entirely on the assessment carried out during on-site inspections and on the limited information submitted by other authorities in the form of complaints against obligated entities.

853. The GIFI and the supervisory authorities generally started carrying out their on-site inspection cycle on the basis of the level of risk to which the institution is exposed since 2013.[39]

Recommendation 17 (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

854. In the 3rd round evaluation, Recommendation 17 was rated 'Partially Compliant'. The sanctioning regime in the AML/CFT Act was not considered to be effective since it only consisted of criminal sanctions which were considered to be disproportionate to cater for minor cases.

855. The amended AML/CFT Act now imposes both administrative and criminal sanctions for breaches of the obligations set out in the law. The AML/CFT sanctioning regime is complemented by administrative and pecuniary sanctions set out in sectoral laws.

Availability of Effective, Proportionate & Dissuasive Sanctions (c. 17.1); Range of Sanctions—Scope and Proportionality (c. 17.4)

856. Chapter 7a of the AML/CFT Act contains the pecuniary (administrative) sanctions for breaches of the provisions of the AML/CFT Act. According to Article 34a, any obligated institution, with the exception of the NBP, which fails to:

> *1) register the transaction referred to in Article 8 paragraph 1, fails to provide the General Inspector with the documents related to this transactions or fails to store the transactions record or documents relating to the transaction for the required period of time;*
>
> *2) carry out the risk analysis in order to apply customer due diligence measures;*
>
> *3) apply customer due diligence measures;*
>
> *4) store documented results of the analysis for the required period of time;*
>
> *5) meet the obligation to provide the participation of employees in training programs;*
>
> *6) timely comply within the post inspection conclusions or recommendations; and*
>
> *7) establishes and maintains cooperation with a shell bank:*
>
> *shall be subject to a fine.*

857. Article 34b of the law stipulates the following:

[39] In 2013, the AML/CFT Unit of the Polish FSA starting using a risk-based mechanism (ORION) for the purpose of AML/CFT supervision. The mechanism allocates grades for each financial institution in relation to multiple underlying risk factors. Periodically, financial institutions are obliged to provide detailed information in response to a questionnaire which is then used to review the grades previously allocated. On the basis of this grading system, the PFSA determines the on-site supervisory cycle for every financial institution. The mechanism is dynamic and the frequency of on-site inspections is not fixed but is determined on the basis of the risk posed by the institution.

1. Any obligated institution which in breach of the following provisions of Regulation No 1781/2006:

1) Articles 5-7, does not ensure that the transfer of funds is accompanied by complete information on the payer;

2) Article 8, does not have effective procedures in place to detect the absence of information on the payer;

3) Article 9, does not inform the General Inspector about the payment service providers of the payer, which regularly fails to provide relevant information on the payer;

4) Article 12, when acting as an intermediary payment service provider, does not keep all the information on the payer accompanying transfers of funds;

5) Article 14, does provide a full response on the request of the General Inspector about the information on the payer accompanying transfers of funds, and does not provide the General Inspector with the requested relevant documents:

- shall be subject to financial sanctions.

2. Should the obligated institution fail to freeze funds of a person, group or entity, contrary to Article 20d paragraph 1, or fail to provide the General Inspector with all the available data to substantiate the freezing of funds, these institutions shall be subject to the same financial sanction.

858. The sanctions which are set out under Chapter 7a apply to both natural and legal persons, since the definition of an 'obligated institution' includes reporting entities which are legal entities, such as banks, and natural persons, such as lawyers, notaries and accountants.

859. As determined in Article 34c (1), pecuniary sanctions are imposed by a decision of the General Inspector. The AML/CFT Act establishes the maximum amount of the pecuniary penalty which may not be higher than PLN 750,000 (approximately €180,000). According to Article 34a (5), a penalty for failure to comply with the obligation to provide training to employees may not be higher than PLN 100,000 (approximately €24,000). Pursuant to Article 34a (9), whenever a pecuniary penalty is imposed on an obligated institution, GIFI is required to notify the supervisory authority which has oversight over that obligated institution.

860. According to Article 34c (2), in order to ensure that the pecuniary penalty is proportionate and dissuasive, the GIFI is to take into account the nature and the extent of the violations, the previous operations of the obligated institution and its financial capacity.

861. The procedure for the imposition of a pecuniary penalty shall be done in accordance with the provisions of the Code of Administrative procedure (Article 34c paragraph 5). An appeal against the decision of the GIFI may be instituted with the minister competent for financial institutions within 14 days from the receipt of the penalty.

862. Notwithstanding the fact that administrative penalties from breaches of the AML/CFT Act may only be imposed by the GIFI, this does not exclude the possibility of the PFSA from taking other measures under sectoral laws. The PFSA has a broad power to issue recommendations, warnings and orders. It may also impose fines, limit the scope of the activities of the institution and revoke a licence. For instance, under the Banking Act, the PFSA may revoke the licence of a bank when the bank's activities are found to be in contravention of the law (Article 138 paragraph 3 point 4 of the Banking Act). In such cases, the PFSA may also suspend from office the members of the management board of the bank. (Article 138 paragraph 3 point 2 of the Banking Act). Similar provisions are found under Article 167 of the Act in Trading in Financial Instruments, Article 228 of the Act on Investment Funds, Article 212 on the Act on Insurance Activities and Article 105 of the Act on Payment Services.

The sanctions imposed by the PFSA are published on its website by type and are listed in chronological order.

863. In addition to the administrative sanctions, Chapter 8 of the AML/CFT Act contains penal provisions for breaches of the provisions of the AML/CFT Act. According to Article 35 (1), any person acting in the name or in the interest of an obligated institution who, contrary to the provisions of the law, fails to:

- *register a transaction, to submit documentation relating to this transaction to the GIFI or to store the register of such transactions or documentation relating to this transaction for the required period of time,*
- *maintain financial security measures, in accordance with the procedure referred to in Article10a paragraph 1, or to store information obtained in connection with the implementation of financial security measures,*
- *notify the General Inspector about the transactions referred to in Article 16 paragraph 1,*
- *suspend a transaction or block an account,*
- *introduce the internal procedure referred to in Article 10a paragraph 1,*
- *designate a person responsible in accordance with Article 10b paragraph 1,*

shall be subject to the punishment of imprisonment of up to 3 years.

864. According to Article 35 (2), the same penalty shall be imposed on anyone who discloses the information collected in accordance with the authorisation of the law to any unauthorised persons, any account holder or any person to whom the transaction relates to or uses this information in any other manner inconsistent with the provisions of the Act.

865. Article 36 of the law stipulates that any person who, acting on behalf of or in the interest of the obligated institution, refuses to submit information or documents to the General Inspector, submits false data to the General Inspector or conceals data on transactions, accounts or persons, shall be liable to the punishment of imprisonment from 3 months to 5 years shall be.

866. Pursuant to Article 37 any person "w*ho commits an act described in Article 35 paragraphs 1 or 2, or in Article 36 causing substantial damage, shall be subject to the punishment of imprisonment from 6 months to 8 years."*

867. According to Article 37a (1), whoever hinders or obstructs an AML/CFT on-site inspection shall be subject to a fine.

Designation of Authority to Impose Sanctions (c. 17.2)

868. As already stated above, pecuniary sanctions are imposed by a decision of the General Inspector (Article 34c (1)). Pursuant to Article 34a (9), whenever a pecuniary penalty is imposed on an obligated institution, the GIFI is required to notify the supervisory authority which has oversight over that obligated institution.

869. The Polish authorities informed the evaluators that the supervisors are entitled to impose additional penalties in those cases where, following the imposition of a penalty by the GIFI, the financial institution still does not rectify the breaches identified or do not sufficient measures to address such deficiencies.

Ability to Sanction Directors and Senior Management of Financial Institutions (c. 17.3)

870. As stated above, the provisions set out in Chapter 8 of the AML/CFT Act provide for penal sanctions to natural persons acting on behalf of or in the interest of the obligated institution. The

person who is responsible for the fulfilment of the financial institution's obligations under the AML/CFT Act is the person designated in accordance with Article 10b paragraph 1, who is a board member appointed by the management board (in the case commercial capital companies, cooperative or state banks) or the director (in the case of branches of foreign banks or credit institution). According to the Polish Authorities, when a notification is sent to the Public Prosecutor's Office in terms of Chapter 8, all persons involved in the breach (irrespective of whether they are directors or senior management) will be liable. It is then within the discretion of the prosecutor to establish the persons who can be held criminally responsible for the breach.

871. According to Art 35 (3), these penal sanctions also apply when the perpetrator acts negligently.

872. There are also provisions in sectoral laws which enable the PFSA to impose sanctions on natural persons. For instance, as stated above, the PFSA may impose the following sanctions:

- the suspension from office or discharge the member of the management board in case of banks;
- in the case of insurance undertakings, the imposition of fines on the management board members up to an amount equivalent to the triple average monthly salary and the suspension or request to recall the management board members.

Effectiveness and efficiency - sanctions [c. 17.1-17.3]

873. The table below indicates the number of sanctions imposed by the GIFI provided by the Polish authorities for the 4th round evaluation.

Table 27: Total number of sanctions imposed by the GIFI

	2007	2008	2009	2010	2011	2012
Notifications submitted to the Public Prosecutor's Office	5	5	7	22	10	7
Proceedings carried out under the provisions of the Code of Administrative Procedure	-	-	-	51	65	76
Decisions	-	-	-	46	49	74
Total amount of fines (PLN)	-	-	-	136,455	636,250	2,063,500
Removal of manager/compliance officer	-	-	-	-	-	-
Withdrawal of license	-	-	-	-	-	-

874. The above table provides figures for the following measures taken by the GIFI:

- The number of notifications submitted to the Public Prosecutor's Office – this includes those breaches identified by the GIFI in terms of Chapter 8 of the AML/CFT Act, which deals with criminal sanctions.

- The proceedings carried out by the GIFI under the provisions of the Code of Administrative procedure – this refers to the number of initiated procedures and does not include the number of actual sanctions imposed.
- Decisions – this provides the total number of sanctions imposed by the GIFI following an administrative procedure.

875. An upward trend can be noted in the number of sanctions imposed by the GIFI. However, considering the number of financial institutions licensed in Poland (774 in total), the figures appear to be low. This could possibly be the result of the limited number of on-site inspections being carried out in view of the low number of staff responsible for AML/CFT inspections within the various supervisory authorities and the Control Unit of the GIFI.

876. For instance, as stated previously, with respect to cooperative banks the number of inspections carried out annually is on average 16 whereas the total number of cooperative banks at the time of the on-site inspection was 574. With respect to brokers, the average number of annual inspections is 5, whereas the total number of brokers is 52. In 2012 the number of sanctions imposed on cooperative banks and brokers was 1 and nil respectively. Therefore, there appears to be a direct link between the number of on-site visits carried out and the number of sanctions imposed.

877. Another factor of concern that demonstrates a lack of effective implementation of the sanctioning regime is the low volume of the total number of fines. For instance, in 2010 the total value was PLN 136,455 (approximately €33,000), PLN 636,250 (approximately €150,000) in 2011 and PLN 2,063,500 (approximately €500,000) in 2012. Although the volume has increased over the years, overall the evaluators believe that there is still room for improvement.

878. It is to be noted that the Polish authorities pointed out that although the number and volume of fines appears to be low, generally, in order to ensure that shortcomings are rectified by financial institutions, the PFSA issues compliance letters rather than imposing sanctions. In their opinion, in certain circumstances, a compliance letter is more effective than a pecuniary sanction, since it would contain a detailed recommendations on the manner in which a shortcoming is expected to be addressed (for instance, the setting up of an automated system of transaction monitoring within a bank). The PFSA issued 30 compliance letters with respect to the AML/CFT issues in 2008, 21 in 2009, 35 in 2010, 32 in 2011 and 46 in 2012.

879. As was mentioned in Table 27 the GIFI submitted 7 notifications to the to the Public Prosecutor's office on the basis of Chapter 8. 2 notifications led to the initiation of investigations, which are still in progress, 2 notifications led to refusal to initiate an investigation (in one case it was concluded that a violation occurred inadvertently, the second was appealed by the GIFI), with respect to 3 other cases, the GIFI received a decision on discontinuance of proceedings by the Public Prosecutor.

880. The figures also indicate that between 2007 and 2012 no financial institution licences were withdrawn by the supervisory authorities as a result of AML/CFT breaches.

881. The Polish authorities provided a breakdown of the list of sanctions by type of obligated institution for the year 2012.

Table 28: Breakdown of breaches and sanctions by type of obligated institution for the year 2012

Lp.	type of obligated institution	Number of breaches	Type of breaches	Sanctions (PLN)	Total amount of pecuniary penalty (PLN)
1.	Savings and credit unions	3	Article 34a point 2 & 3	2 discontinuation of proceeding 1 penalty imposed 92,000	92,000
		1	Article 34a point 4	1 discontinuation of proceeding	
		1	Article 34a point 4 & 5	proceeding in progress	
2	foreign exchange offices	4	Article 34a point 1	penalty imposed jointly 16,500	16,500
		15	Article 34a point 4	1 discontinuation of proceeding, 14 penalties imposed, jointly: 33,500	89,500
		9	Article 34a point 4 & 5	1 discontinuation of proceeding 8 penalties imposed, jointly: 31,500	
		5	Article 34a point 5	5 penalty imposed, jointly 6,500	
		1	Article 34a point 1 and 3	penalty imposed: 1,500	
3	entity engaged in games of chance and mutual betting	6	Article 34a point 1	penalties imposed, jointly 56,000	69,500
		7	Article 34a point 4	1 discontinuation of proceeding, 6 penalties imposed, jointly 13,000	
		1	Article 34a point 2 & 4	penalty imposed 500	
		2	Article 34a point 3	2 proceedings in progress	

4	Foundations	2	Article 34a point 2, 3, 4, 5	1 proceeding in progress, 1 penalty imposed 50,000	50,000
		1	Article 34a point 2, 3, 4	proceeding in progress	
5	Cooperative banks	1	Article 34a point 3, 4, 5,	penalty imposed 181,000	181,000
6	entrepreneurs	2	Article 34a point 4	penalty imposed, jointly: 3,500	16,000
		1	Article 34a point 2, 3, 4, 5	penalty imposed: 500	
		1	Article 34a point 3, 4, 5	penalty imposed: 12,000	
7	Insurance companies	1	Article 34a point 1	penalty imposed: 10,000	140,500
		2	Article 34a point 3	1 discontinuation of proceeding, 1 penalty imposed: 130,500	
8	Associations	1	Article 34a point 2, 3, 4, 5	penalty imposed: 500	500
9	notaries public	1	Article 34a point 5	penalty imposed: 2,000	7,000
		2	Article 34a point 1	1 proceeding in progress, 1 penalty imposed: 5,000	
10	entrepreneurs engaged in leasing activity	2	Article 34a point 3	proceeding in progress	proceeding in progress
11	entrepreneurs engaged in factoring activity	1	Article 34a point 2, 3, 5	proceeding in progress	proceeding in progress
12	entrepreneurs engaged in commission sale	1	Article 34a point 1	proceeding in progress	proceeding in progress
13	Banks	2	Article34a point 3	proceeding in progress	proceeding in progress

882. The most common breaches identified in 2012 (but also in the other years according to the Polish authorities) in the course of inspections conducted by the supervisory authorities are the following:

- Non-compliance with risk analysis and CDD requirements;
- incorrect completion of transaction register fields;
- not registering transactions which are equivalent to or do not exceed €15,000;
- untimely registration of transactions;
- transferring information to the General Inspector for Financial Information after the expiry of the deadlines set out in law.

883. With respect to sanctions for failure to identify a beneficial owner, the Polish authorities indicated that in the period between 2010-2012 only five sanctions were imposed as stated in the table below:

Table 29: administrative sanctions for failure to identify a beneficial owner (2010-2012)

Financial institution	No. of sanctions
Banks	2
Cooperative banks/credit unions	2
Brokerage house	1

884. The evaluators consider this a matter of concern since, as noted in relation to Recommendation 5, in those instances where a financial institution is not in a position to identify the beneficial owner, rather than refusing to enter into a business relationship or terminating a business relationship, the institution merely raises the risk profile of the customer.

885. Notwithstanding the fact that since the 3rd round evaluation, the Polish authorities have imposed a number of administrative sanctions for breaches of the AML/CFT Act, including a number of compliance letters sent to financial institutions by the PFSA and the GIFI, the evaluators consider the sanctioning regime to be effective and proportionate. As a result, the evaluators concluded that the sanctioning regime is sufficiently dissuasive.

Market entry

Recommendation 23 (rated PC in the 3rd round report)

Recommendation 23 (c. 23.3, c. 23.3.1, c. 23.5, c. 23.7, licensing/registration elements only)

Prevention of Criminals from Controlling Institutions, Fit and Proper Criteria (c. 23.3 & 23.3.1)

886. All financial institutions, except for foreign exchange offices and cooperative savings and credit unions, are required to obtain a licence from the PFSA. Foreign exchange offices and cooperative savings and credit unions are required to obtain a licence from the NBP and the NSCCU respectively. One of the elements of the licensing procedure is the requirement to set up internal procedures to cater for AML/CFT requirements and measures to ensure the fitness and propriety of the founders and the members of the board. The licensing requirements of each type of institution are set out in sectoral laws.

887. At the request of evaluators, the PFSA provided information on its cooperation with the Internal Security Agency (ISA) regarding licensing issues, in particular with respect to the fitness and propriety of applicants for a licence. During the licensing process the PFSA sends requests to the ISA

in order to verify the suitability of candidates for management boards, persons involved in the administration and shareholders of financial institutions. The goal of each request is to receive information within the scope of suitability laid down in the law. Information provided by the ISA includes a reference not only to whether the person has any criminal connections and whether the person is in the field of interest of the ISA. The ISA is required to provide a response within twenty one days (no response within the set out time frame is considered as *nihil obstat*). In the last two years the following number of request were sent: 92 for the licensing of brokerage services; 34 for the licensing of investment funds; 43 for the licensing of life insurance companies; and 132 for the licensing of banks. Each request usually contains a reference to more than one person. According to the data provided by the relevant Departments within the PFSA, none of the responses that were received from the ISA indicated that a person on whom a request was made was unfit to hold the position within the entity applying for the license.

Banks

888. The Banking Act provides for the licensing procedure to obtain an authorisation to provide banking activities.

889. One of the conditions of the licensing procedures is the requirement to submit an application to the PFSA which contains information on the founders and the persons proposed to be appointed as members of the management board (Article 31 of the Banking Act). This application is to include certain documents on the founders and their financial situation, as required by the PFSA.

890. In addition, Article 25 of the Banking Act, any partying intending to take up or acquire shares in a bank which would result in that party being entitled to 10%, 20%, one third or 50% or more of the total number of votes at a general meeting, shall be required to notify the PFSA. In terms of Article 25b such a notification shall include the identification of the notifying party, persons managing its activity and the persons proposed as members of the bank's management board, unless the notifying party intends to introduce changes in this regard. Furthermore, the notifying party is required to provide information on any criminal conviction, convictions relating to tax offences, on-going criminal proceedings and any other administrative and civil proceedings concerning the notifying party or persons and the persons proposed as members of the bank's management board.

891. Article 25b also requires the PFSA to ensure that any funds to be used in the taking up or acquisition of shares in a bank derive from a legitimate source.

892. According to Para 5 of Article 138 of the Banking Act, the PFSA shall dismiss a member of the management board in the event that that person is convicted of a wilful criminal offence or fiscal offence, excluding offences that are prosecuted upon a private complaint. According to Para 4 of Article 138, the PFSA may also suspend from office a member of the management board where that person has been charged with a criminal or fiscal offence.

893. Art. 30 of the Banking Act provides for the following:

> *"2) the founders and persons proposed for members of the bank's management board, including the president, give adequate guarantee of the sound and prudent management of the bank, and at least two of the persons proposed for members of the bank's management board are adequately educated and have professional experience necessary to manage a bank, as well as a proven knowledge of the Polish language,"*

894. It appears that the Banking Act does not explicitly cover the element of the directors' and senior management's integrity.

Securities firms and investment fund management companies

895. The Act on Trading in Financial Instruments provides for the licensing procedure to obtain an authorisation to provide investment activities.

896. Article 82 of the Act on Trading in Financial Instruments provides for a list of information to be included in an application to obtain a license. The application shall contain the personal details of the board, the supervisory board and audit committee members, or partners or general partners in a partnership, and other persons who are responsible for launching investment services, as well as information on their professional qualifications and employment history. Furthermore, the application shall contain the list of shareholders and the percentage of their total voting rights as well as the personal details of the shareholders who are natural persons and hold 10 or more percent of the total voting rights or 10 or more percent of the applicant's share-capital.

897. The applicant is required to declare that the board, the supervisory board and the audit committee members have not been found guilty of any offences set out in the Act. The application shall also indicate, subject to criminal liability, the natural persons who have a qualifying participation.

898. To prevent criminals from obtaining control of a securities company, Article 106b of the Act provides that the permission of the PFSA must be obtained before acquiring more than 10 %, 20 %, one third or 50 % of the total number of voting rights at a general meeting or to take or acquire shares in the authorised share-capital.

899. According to Article 22 of the Act on Trading in Financial Instruments, the personal details of the board members of the depositary, as well as the information from the National Criminal Register, shall be attached to the application for an authorisation to set up an investment fund. Article 58 sets out the requirement to obtain information from the National Criminal Register before granting a license of an investment fund management company.

900. The provisions determined in Article 54 of the Act ensure that the PFSA has control over any selling or buying of shares following the granting of a license.

Insurance sector

901. The Act on Insurance Activities provides for the licensing procedure to obtain an authorisation to provide insurance activities.

902. Article 92 of the Act on Insurance Activities provides for the general requirements for granting a licence. The application of insurance undertakings shall contain an indication of the founders and the names and surnames of the persons assigned as members of the management board and the supervisory board. The financial statement of the founders and a certificate indicating the absence of a criminal record or a declaration made by the persons proposed to be appointed as members of the management and supervisory board and the actuary shall be enclosed to the application.

903. The provisions set out in Article 35 of the Act ensure that the PFSA has complete oversight of the ownership structure of an insurance undertaking.

904. According to Article 98 of the Act, authorisation cannot be issued if :

- the membership of the management board or the supervisory board of the domestic insurance undertaking concerned includes persons who do not meet the requirements specified in the Act;
- the founders of the domestic insurance undertaking have been convicted for a wilful offence ascertained by a valid court sentence;
- the founders make use of material assets deriving from illegal or undisclosed sources.

Cooperative savings and credit unions[40]

905. The NSCCU supervises existing cooperative saving and credit unions, which are required to comply with prudential standards and other supervisory regulations established by the NSCCU.

906. The 3rd Round Report noted that, although cooperative savings and credit unions were registered by the National Court, there were no licensing procedures in line with the Basel Core Principles. The only existing licensing requirement for these entities was found under Para 1 of Article 10 of the Act on Cooperative Savings and Credit Unions, which stated that membership of supervisory and management boards may not include persons convicted for intentional offences against property or documents, or for fiscal offences. Since the 3rd round evaluation, a licensing system in line with the Basel Core Principles has still not been introduced.

Foreign Exchange Offices

907. According to Article 11 paragraph 1 of the Foreign Exchange Act, foreign exchange market providers are regulated by the Economic Activity Freedom Act of 2nd July 2004 and are required to be recorded to the register of foreign exchange market providers. Paragraph 2 of Article 11 states that the provisions related to foreign exchange market providers shall not apply to banks, branches of foreign banks, and to credit institutions and branches.

908. Pursuant to Article 12 foreign exchange market provider may be a natural persons, who has not been validly convicted for a fiscal offence or an offence committed for financial or personal gain, as well as legal entity and a partnership without legal personality, of which no members of the governing bodies or a partner, respectively, has been convicted for such offences.

909. In order to be recorded to the register a written request should be submitted to the NBP, which also includes the following information:

- business name, seat and address or the address of residence,
- number in the business register or business records,
- tax identification number (NIP), if the entrepreneur has one,
- seats and addresses of entities, in which foreign exchange market operations will be carried out,
- designation of the scope of foreign exchange market operations carried out by the entrepreneur in individual entities,
- signature of the entrepreneur and designation of the date and place of filling the request.

910. Additionally, the applicant shall accompany a written request by a declaration that he has no convictions and a document confirming his qualification.

Licensing or Registration of Value Transfer/Exchange Services (c. 23.5)

Money or value transfer service providers

911. In the 3rd round report it was noted that natural and legal persons providing a money or value transfer service were not licensed or registered. Apart from the banks and the Polish Post, these entities were not subject to an effective system for monitoring and ensuring compliance with the AML/CFT requirements. The issue has since been addressed through the enactment of the Act on Payment Services (22 August 2011).

912. In order to provide payment services in Poland, entities are required to obtain an authorisation from the PFSA in terms of Article 60 of the Act:

[40] Since 10 October 2012 a new Law entered into force containing the full BCBS core principles.

1. *The provision of payment services as a domestic payment institution requires the authorisation of the PFSA.*
2. *Authorisation may be granted to a legal person with its registered office on the territory of the Republic of Poland, upon its application.*

913. The provisions set out in Part IV of the Act on Payment Services provide that an applicant entity is required to submit various information and documentation to the PFSA, including:

(a) a description of the proposed policies and procedures for governance and internal control mechanisms concerning AML/CFT measures;

(b) the capital requirements of the entity;

(c) information that makes it possible to establish the identity of persons who directly or indirectly have a significant shareholding in the applicant entity, indicating the size of their holdings and documents that confirm that these persons ensure sound and prudent management of the payment institution.

914. Part IV also sets out the period of time within which an authorisation is to be granted and the cases where the PFSA may refuse to issue or withdraw an authorisation.

915. The PFSA is also responsible for the authorisation of branches and agents situated in Poland of payment institutions established in another member state of the EU. In terms of Article 97, an EU payment institution may commence providing payment services in Poland through a branch or agent after one month from the receipt of a notification by the PFSA from the supervisory authority of the home member state. This notification shall include information on, among other things, a description of the organisational structure of the branch and a description of internal control mechanisms concerning AML/CFT obligations of the branch or the agent.

Foreign exchange offices

916. Under the provisions of the AML/CFT Act, the activities related to currency exchange operations constitute regulated activity within the meaning of the Act of 2 July 2004 on Freedom of Economic Activity (Journal of Laws 2010, No. 220, item 1447, as amended), and have to be recorded in a register. The register shall be maintained by the President of the NBP.

917. The NBP has the competence to conduct on-site inspections to monitor compliance with the requirements laid down in the Foreign exchange Law and the AML/CFT Act. The NBP is also authorised to strike foreign exchange offices off the register in the event of a serious infringement of the law.

On-going supervision and monitoring

Recommendation 23 & 32 (c. 23.4, c. 23.6, c. 23.7, supervision/oversight elements only & c. 32.2d)

Application of Prudential Regulations to AML/CFT (c. 23.4)

918. All of the measures used by the PFSA in prudential supervision can also be utilised for AML/CFT purposes. As the PFSA is a single supervisory authority responsible for the majority of financial institutions, the AML/CFT Unit can have access to all data gathered and analysed for other supervisory purposes. The exchange of information goes both ways, as the AML/CFT Unit informs other Departments of the PFSA on their on-site visit plan, so to facilitate joint on-site visits in those cases were plans overlap. Furthermore all the recommendations made to financial institutions as a result of breaches identified during the on-site visits on AML/CFT are made available to those Departments in the PFSA which deal with prudential supervision.

Monitoring and Supervision of Value Transfer/Exchange Services (c. 23.6)

919. Following the implementation of the PSD, the PFSA acquired supervisory powers over MVT service providers.

920. According to point 1 letter u of Art. 2 of the AML/CFT Act, the MVT service providers are obligated institutions and are therefore subject to all AML/CFT requirements set out in the law. Pursuant to Para 3 of Art 21 of the AML/CFT Act, the PFSA has the power to conduct onsite visits of domestic MVT service providers in accordance with the rules and procedures laid down in Para 1 of Art. 103 of the Act on Payment Services.

921. According to Para 3 of Art. 104 the "*The regulations of Article 103 shall apply to branches of EU payment institutions and their agents operating within the territory of the Republic of Poland if it is agreed with the competent supervisory authorities of the home Member State that an inspection is to be carried out by the PFSA*."

922. With respect to foreign exchange services, on-site inspections are exercised by the NBP within the framework of the inspection of foreign exchange activities regulated by the Foreign Exchange Act of 27 July 2002 (Journal of Laws No. 141, item 1178, as amended). Inspections are carried out by 16 organisational units located throughout the country.

Supervision of other Financial Institutions (c. 23.7)

923. According to Polish authorities there are no other financial institutions which are not mentioned under criterion 23.4 operating in the territory of the Republic of Poland.

Statistics on On-Site Examinations (c. 32.2(d), all supervisors)

924. Statistics on the number of on-site visits performed by the GIFI, the PFSA, the NBP and the NSCCU were provided by the Polish authorities. A table containing data on on-site examinations is provided under the 'Effectiveness' of Recommendation 29.

3.10.2 Recommendations and comments

Recommendation 23

925. The criteria under Recommendation 23 appear to be adequately implemented. However, a licensing system as defined in the Basel Core Principles should be introduced for Cooperative Savings and Credit Unions.

Recommendation 17

926. Considering the number of financial institutions licensed in Poland (774 in total), the total number and volume of sanctions appears to be low. This could possibly be the result of the limited number of on-site inspections being carried out in view of the low number of staff responsible for AML/CFT inspections within the various supervisory authorities and the Control Unit of the GIFI. Nonetheless the evaluators believe that the compliance letters used by the PFSA could be considered as an immediate and effective sanction.

927. In particular, the evaluators noted that the sanctions imposed for failure to identify the beneficial owner of the customer is very low considering the fact that during the on-site visit it clearly emerged that where a financial institution is not in a position to identify the beneficial owner, rather than refusing to enter into a business relationship or terminating a business relationship, the institution merely raises the risk profile of the customer.

928. In addition, it was noted that no sanctions have ever been imposed on directors and senior management.

Recommendation 29

929. The evaluators noted that the number of on-site inspections is not sufficient to ensure that the entire financial sector is adequately complying with AML/CFT measures. The reason for this may possibly be attributed to the number of inspectors who conduct AML/CFT inspections. In particular, notwithstanding the fact that the PFSA is responsible for the entire financial sector, only six inspectors were allocated to the AML/CFT Unit (out of a total of one hundred and seventy four inspectors).

930. Since financial institutions are not required to periodically submit information on their AML/CFT policies and procedures to the GIFI and other supervisory authorities, it is difficult for the authorities to conduct desk-reviews on the level of AML/CFT compliance by financial institutions. Therefore, for monitoring purposes, the GIFI and the other financial supervisors are obliged to rely entirely on the assessment carried out during on-site inspections and on the limited information submitted by other authorities in the form of complaints against obligated entities. The authorities should ensure that an appropriate mechanism for periodic reporting by financial institutions for compliance purposes is set up.

931. Notwithstanding the fact that the on-site inspection procedure of the NBP appears to be rather comprehensive, the evaluators noted that the level of appreciation of the ML/FT risks of the foreign exchange sector is rather low.

932. The evaluators noted with concern that the NSCCU does not appear to possess a satisfactory level of awareness of the AML/CFT risks associated with the savings and credit unions sector. In addition, on-site inspections are not conducted in accordance with a manual.

933. The authorities should take measures to ensure that the NSCCU and NBP are properly apprised of the ML/FT risks within their sectors. An on-site inspection manual for the NSCCU should be drafted.

Recommendation 30 (all supervisory authorities)

934. The number of AML/CFT inspectors within the Control Unit of the GIFI and the PFSA appears to be insufficient. This has a negative bearing on the effectiveness of the on-site inspection mechanism and on the entire AML/CFT supervisory structure as a whole. The authorities should consider whether further human resources should be allocated for compliance monitoring purposes.

935. No information was provided by the NSCCU with respect to structure, staffing and funding of this entity. This was also the case with the NBP which only provided information on the number of on-site inspectors. In addition, neither authority provided information on the provisions ensuring professional standards and integrity of its officers.

Recommendation 32

936. The GIFI and supervisory authorities maintain accurate statistical information on the type and number of sanctions imposed on financial and other institutions.

3.10.3 Compliance with Recommendations 23, 29 and 17

	Rating	Summary of factors relevant to s.3.10. underlying overall rating
R.17	**LC**	**Effectiveness:** • No sanctions imposed on directors and senior management.
R.23	**LC**	• There is no registration or licensing system for Cooperative Savings and Credit Unions.

R.29	**LC**	**Effectiveness:** • Insufficient number of on-site inspections, prior to implementation of the RBA; • The level of appreciation of ML/FT risks by NSCCU appears to be low, thereby having an impact on the effectiveness of on-site inspections.

3.11 Money or value transfer services (SR. VI)

3.11.1 Description and analysis

Special Recommendation VI (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

937. In the 3rd Round evaluation, it was established that in Poland there was no system in place for the registration and/or licensing, direct monitoring and sanctioning of natural and legal persons that perform money or value transfer (MVT) services in Poland. Based on these factors Special Recommendation VI was rated 'Non-Compliant'.

938. The issue has since been addressed through the enactment of the Act on Payment Services (22 August 2011) and the amended AML/CFT Act.

939. The Act on Payment Services transposes Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services (PSD).

Designation of registration or licensing authority (c. VI.1), adequacy of resources – MVT registration, licensing and supervisory authority (R. 30)

940. MVT service providers are regulated under the provisions of the Act on Payment Services. According to Art. 4, only the following entities may provide payment services:

- a domestic bank;
- a branch of a foreign bank;
- a credit institution or a branch of a credit institution;
- an electronic money institution;
- a branch of an entity that provides postal payment services in a Member State other than the Republic of Poland, which is authorised in accordance with the law of that state to provide payment services;
- the Polish Post Office insofar as separate regulations authorise it to provide payment services;
- a payment institution;
- the European Central Bank, the NBP and the central bank of another member state if they are not acting in their capacity as a monetary authority or organ of public administration;
- an organ of public administration;
- a cooperative savings and credit union or the NSCCU;
- a payment service office.

941. In order to provide payment services in Poland, the above entities are required to obtain a an authorisation from the PFSA in terms of Article 60 of the Act:

> *1. The provision of payment services as a domestic payment institution requires the authorisation of the PFSA.*

2. Authorisation may be granted to a legal person with its registered office on the territory of the Republic of Poland, upon its application.

942. The provisions set out in Part IV of the Act on Payment Services provide that an applicant entity is required to submit various information and documentation to the PFSA, including:

(a) a description of the proposed policies and procedures for governance and internal control mechanisms concerning AML/CFT measures;

(b) the capital requirements of the entity;

(c) information that makes it possible to establish the identity of persons who directly or indirectly have a significant shareholding in the applicant entity, indicating the size of their holdings and documents that confirm that these persons ensure sound and prudent management of the payment institution;

(d) information that allows the identification of managers and documents that make it possible to assess whether these people ensure sound and prudent management of the payment institution, including whether they have the education and professional experience necessary for the management of operations in the area of the provision of payment services.

943. Part IV also sets out the period of time within which an authorisation is to be granted and the cases where the PFSA may refuse to issue or withdraw an authorisation.

944. The PFSA is also responsible for the authorisation of branches and agents situated in Poland of payment institutions established in another member state of the EU. In terms of Article 97, an EU payment institution may commence providing payment services in Poland through a branch or agent after one month from the receipt of a notification by the PFSA from the supervisory authority of the home member state. This notification shall include information on, among other things, a description of the organisational structure of the branch and a description of internal control mechanisms concerning AML/CFT obligations of the branch or the agent.

945. Article 4 paragraph 3 states that domestic payment institutions, payment service offices, agents and branches of such entities, as well as savings and credit unions, and their affiliates, are subject to registration in the registry of domestic payment institutions and other providers. According to Article 133, the PFSA shall keep and maintain the register. The register, which is public and accessible to third parties through the website of the PFSA, contains the data of these entities. Article 139 paragraph 2 obliges entities providing payment services to inform the PFSA of every change in the information contained in an entry in the register not later than fourteen days from the date of the change in the information. Failure to provide such information to the PFSA is subject to a fine.

946. The evaluators noted that there is no public register that contains a list of branches and agents of EU payment institutions.

947. In terms of Article 14 of the Act on Payment Services, the PFSA is responsible for ensuring compliance with the licensing requirements set out under the Act by all entities providing payment services. The PFSA is also responsible for the supervision of branches and agents of EU payment institutions in conjunction with the home supervisory authority.

948. At the time of the on-site visit there were 3 foreign exchange offices in Poland which applied for authorisation to provide MVT services under the PSD. Although foreign exchange offices are under the supervision of the NBP, insofar as MVT services are concerned supervision is conducted by the PFSA.

Application of the FATF 40+9 Recommendations (applying R. 4 – 11, 13 – 15 & 21 – 23 and SR IX (c. VI.2))

949. According to Article 2 paragraph 1 of the AML/CFT Act, all financial institutions providing MVT services, including payment institutions, branches of EU payment institutions, payment services offices and their agents (letter u of paragraph 1 of Art. 2) are subject to all AML/CFT requirements set out in the law.

950. Notwithstanding the fact that MVT service operators are subject to the AML/CFT Act, the various deficiencies identified with respect to Recommendations 4-11, 13, 21-23 may have an impact on the effective implementation of AML/CFT requirements by these entities.

Monitoring MVT services operators (c. VI.3)

951. Pursuant to Article 21 paragraph 1, MVT service operators are subject to the AML/CFT supervision and monitoring of the GIFI. In terms of Article 21 paragraph 3, such supervision and monitoring may also be performed by the PFSA and the NSCCU (with respect to savings and credit unions).

952. The Polish authorities informed the evaluators that no AML/CFT on-site inspections had been carried out with respect to MVT service operators. The reason for this was that, since the Act on Payment Services was enacted in August 2011, at the time of the on-site visit in May 2012 the licensing of MVT service operators was still underway.

953. Prior to the enactment of the Act on Payment Services, the Polish Post provided MVT services without being licensed or supervised. Nevertheless, it was subject to AML/CFT obligations and subject to the AML/CFT supervision of the GIFI. The last on-site AML/CFT on-site inspection of the Polish Post was conducted in 2005. The evaluators do not consider the level of monitoring of the Polish Post to be sufficient. However, the Polish authorities indicated that in the absence of on-site supervision (the last on-site inspection has been conducted in 2005), the GIFI conducts regular off-site reviews of the activities of the Polish Post.

Lists of agents (c. VI.4)

954. As mentioned above, according to Article 133 of the Act on Payment Services, the national register of MVT service providers is maintained and made public by the PFSA. It includes information on agents of payment institutions and payment service offices.

955. Art. 85 of the Act on Payment Services requires payment service providers to submit a written notification of their intention to provide payment services through the intermediation of an agent and shall submit a request for entry of the agent in the register.

Sanctions (applying c.17 – 1 – 17.4 & R. 17 (c. VI.5))

956. According to Article 2 of the AML/CFT Act, payment institutions, payment service offices and electronic money institutions are obligated institutions. They are therefore subject to the sanctioning regime applicable under the AML/CFT Act.

957. The range of supervisory measures and penalties at the disposal of the PFSA in relation to MVT service providers is listed in Part 4 of the Act on payment services.

958. According to Art. 105 of the Act on Payment Services, where a payment services provider fails to comply with a request of the PFSA or any provision of the Act, the PFSA may:

- request that the manager is dismissed or to suspend the person who is directly responsible for the breaches from the exercise of his functions;
- restrict the area of activities of the MVT service provider;

- impose a fine on the manager who is directly responsible for the identified breaches, which fine shall not exceed the gross monthly remuneration; or
- impose a fine on the MVT service provider, which fine shall not exceed PLN 1,000,000 (€240,000) or withdraw its license.

959. According to Para 7 of Art. 105, the PFSA shall immediately inform the competent supervisory authorities of a Member State in which the domestic payment institution conducts cross-border activities or operates through an agent or a branch, in those cases where an authorisation is withdrawn.

960. According to Para 1 of Art. 107, if an EU payment institution or its agent, conducting business in Poland, breaches the regulations of Polish law, the PFSA shall call on the institution in writing to comply with the regulations and set a timeframe within which the breaches are to be rectified. If the time limit expires without effect, the PFSA shall notify the competent supervisory authorities of the home Member State of the irregularities identified.

961. For a more detailed explanation on the sanctioning regime which is applicable in Poland reference should be made to Section 3.10 of this report.

Additional elements – applying Best Practices paper for SR. VI (c. VI.6)

962. Although certain aspect of the Best Practices paper for SR VI have been broadly implemented, in particular those issues relating to licensing, AML/CFT Regulation, compliance monitoring and sanctions, there appear to be limited efforts to detect unauthorised MVTS activity. Nevertheless, it should be noted that Article 150 of the Act states that a person who engages in activities in the area of provision of payment services without obtaining an authorisation shall be subject to a fine of up to PLN 5 million (approximately €1.2 million) or to imprisonment for up to two years or both such fine and imprisonment.

Effectiveness and efficiency

963. Since Poland implemented the Payment Services Directive in 2011, the licensing process was still underway at the time of the on-site visit. Therefore, the evaluators could not determine whether the system is effective.

3.11.2 Recommendations and comments

964. The Polish authorities should consider taking steps to ensure that a public list of branches and agents of EU payment institutions is included in the register.

3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors relevant
SR. VI	**LC**	• Deficiencies in the AML/CFT Law relating to preventive measures, particularly on CDD, apply to MVT operators; **Effectiveness:** • Effectiveness could not be demonstrated since the system for the licensing and supervision of MVT operators is still being set up.

4. PREVENTIVE MEASURES – DESIGNATED NON FINANCIAL BUSINESSES AND PROFESSIONS

Generally

965. According to Article 2 (1) of the AML/CFT Act, the obligated DNFBPs are the following:

- entities operating in the field of games of chance, mutual betting and automatic machine games and automatic machine games of low prizes,
- notaries in so far as notary's operations concerning trading in asset values, attorneys performing their profession, legal advisers practicing his profession outside their employment relationship with agencies providing services to the government authorities and local government units, foreign lawyers providing legal services apart from his employment, expert auditors, active tax advisers,
- entities operating in so far as accounts bookkeeping services,
- entities providing currency exchange operations,
- entrepreneurs engaged in: auction houses, antique shops, business factoring, trading in metals or precious/semi-precious stones, commission sale or real estate brokerage,
- foundations,
- associations with corporate personality established under the Act of 7 April 1989 - Law of Associations and receiving payments in cash of the total value equal to or exceeding the equivalent of €15,000, originating also from more than one operation,
- entrepreneurs within the meaning of the Act of 2 July 2004 on freedom of economic activity, receiving payment for commodities in cash of the value equal to or exceeding the equivalent of €15,000, also when the payment for a given product is made by more than one operation,

966. The 3rd Round Mutual Evaluation Report acknowledged the fact that domestic trusts cannot exist in Poland. Since the situation has not changed since the Third Evaluation, no assessment was made by the evaluators on the implementation of the Standards in relation to trusts.

967. Trusts and Companies Service Providers are not covered by the AML/CFT Act.

968. The AML/CFT Act provides a legal framework for the implementation of AML/CFT obligations by designated non-financial businesses and professions (DNFBPs). The requirements for DNFBPs are the same as those which are applicable to financial institutions with a few exceptions. Therefore, most of deficiencies and positive findings mentioned in this report with respect to financial institutions are also applicable to DNFBPs.

4.1 Customer due diligence and record-keeping (R.12)

(Applying R.5 to R.10)

4.1.1 Description and analysis

Recommendation 12 (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

969. At the time of the 3rd Round Evaluation the general CDD framework of the AML/CFT Act was applicable to the DNFBPs with all its deficiencies. Recommendation 12 was therefore rated 'Non-Compliant'.

970. Due to the general improvement of the situation with the enactment of the AML/CFT Act, the CDD and record keeping requirements for DNFBPs have also improved. Nevertheless certain deficiencies were identified.

Applying Recommendation 5 (c. 12.1)

971. According to the FATF Methodology, DNFBP should be required to comply with the requirements set out in Recommendation 5 (Criteria 5.1 – 5.18) for circumstances specific to casinos, real estate agents, dealers, lawyers, and trust and company service providers (TCSPs). DNFBP should especially comply with the CDD measures set out in Criteria 5.3 to 5.7 but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction.

972. Under Art. 2 paragraph 1 of the AML/CFT Act, all DNFBP listed under FATF Methodology are included as obliged entities.

Casinos (Internet casinos / Land based casinos)

973. The AML/CFT Act applies to entities operating in the field of games of chance, mutual betting and automatic machine games (Article 2 paragraph 1.i). The definition does not distinguish between land-based and internet gaming providers.

974. Article 9c of the AML/CFT Act requires casino operators and cash bingo rooms to identify all clients at the entrance regardless of the value of gambling chips or cards purchased for gaming purposes. The same identification obligations are imposed on casinos by the Gambling Law. Article 15b of the Gambling Law also requires casinos to install an audio-visual equipment to record the settlement of chips and cash at the cash desk, the issue of statements on winnings and the keeping of records of paid out (issued) winnings, as well as the possibility of controlling and verifying persons entering the casino.

975. All CDD requirements set out under the AML/CFT Act are applicable to casinos. The deficiencies identified under Recommendation 5 also apply to casinos, insofar as the standard applies to casinos.

Real estate agents

976. Real estate agents fall within the definition of an 'obligated institution' under Article 2 paragraph 1.q of the AML/CFT Act. All CDD requirements set out under the Act are applicable to real estate agents. The deficiencies identified under Recommendation 5 also apply, insofar as the standard applies to real-estate agents.

Dealers in precious metals and dealers in precious stones

977. Dealers in precious metals and stones fall within the definition of an 'obligated institution' under Article 2 paragraph 1.q. All CDD and record-keeping requirements set out under the AML/CFT Act are applicable to dealers in precious metals and precious stones. The deficiencies identified under

Recommendation 5 also apply, insofar as the standard applies to dealers in precious metals and precious stones.

Lawyers and other independent legal professionals

978. The AML/CFT Act applies to attorneys (in Poland this includes barristers who provide their services to natural persons and legal advisers who provide their services to legal persons), legal professionals who provide services to government authorities and local government units and foreign lawyers (Article 2 paragraph 1. n). The AML/CFT obligations apply to all activities of these legal professions and not only the activities referred to under Criterion 12.1(d).

979. Nevertheless, Article 10d of the AML/CFT Act exempts legal professionals from carrying out the following obligations:

- On-going analysis of transactions and on-going monitoring (Article 8a, 8b.3.4);
- Identification of the beneficial owner (Article 8b.3.2);
- Obtaining information for the purpose and nature of business relations (Article 8b.3.3);
- Applying enhanced CDD measures in case of a client who is not present for verification purposes (Article 9e.2);
- Applying measures to mitigate risks arising from products that allow anonymity (Article 9g);

980. Therefore, legal professionals are not required to carry out the measures prescribed by Criteria 5.5-5.7.

981. The other CDD requirements of the AML/CFT Act are applicable to legal professionals. The deficiencies identified under Recommendation 5 also apply, insofar as the standard applies to independent legal professionals.

Notaries

982. Article 2.1.n of the AML/CFT Act restricts the requirements of the Act to those activities of notaries which relate to trading in asset values, in particular buying or selling of real estate. This provision does not appear to cover the following activities set out under Criterion 12.1(d):

- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

983. The evaluators consider this to be a shortcoming.

984. In the interviews held during the onsite mission, the representatives of the National Council of Notaries acknowledged that the scope of application of the AML/CFT Act to notaries does not adequately reflect the functions carried out by the notaries in Poland and causes ambiguity in the practical implementation of the required measures.

985. Concerning notaries' activities which are covered by the AML/CFT Act all CDD requirements are applicable. The deficiencies identified under Recommendation 5 also apply, insofar as the standard applies to notaries.

Accountants

986. Accountants are subject to the AML/CFT Act in terms of Article 2 paragraph 1.o. All CDD set out under the AML/CFT Act are applicable to accountants. The deficiencies identified under Recommendation 5 also apply, insofar as the standard applies to accountants.

Trust and Company Service Providers

987. Trust and Company Service Providers are not included in the definition of obligated institutions under Article 2 paragraph 1 of the AML/CFT Act.

Recommendation 6, 8-11 (c.12.2)

988. Since all DNFBP (except for some legal professionals) are subject to the AML/CFT Act, all the obligations on PEPs, new and developing technologies, reliance on third parties (the only exception being in relation to legal professionals), record-keeping and complex, unusual large transactions contained within the Act apply to DNFBP. The deficiencies which were identified under R. 6, 8-11 apply to DNFBP.

Effectiveness and efficiency

989. Meetings with the DNFBPs during the on-site visit demonstrated the high level of awareness of the AML/CFT requirements. However, similarly to financial institutions, the understanding and awareness of the obligations dealing with the identification beneficial owners of DNFBP does not appear to be adequate.

990. During the on-site visit, notaries indicated discrepancies between the definition of notaries' activities in the AML/CFT Act and their functions conducted according to the Notary Law. This could have a negative impact on the effectiveness of the preventive regime implemented by notaries.

4.1.2 Recommendations and comments

991. Poland demonstrated a significant progress in the implementation of the AML/CFT requirements for DNFBPs since 3rd Round Evaluation. The Gambling Law in some case requires casinos to apply even stricter CDD measures than prescribed by the AML/CFT Act.

992. The deficiencies relating to R.5, 6, 8-11 are also applicable to DNFBPs insofar as these Standards apply to DNFBPs.

993. The exemption of legal professionals from the obligations prescribed by Criteria 5.5-5.7 and R.8 goes beyond what is permitted by R.12.

994. The Polish authorities should review the exemption applicable to legal professionals from certain CDD requirements set out in the AML/CFT Act Article 10d.

995. The Polish authorities should review the definition set out under Article 2.1.n of the AML/CFT Act to ensure that no ambiguities arise with respect to the scope of application of AML/CFT obligations to the activities of notaries. The Polish authorities should include company service providers within the scope of application of the AML/CFT Act.

Applying Recommendation 5

996. DNFBP should be required to verify customer identity on the basis of document, data or information obtained from a reliable and independent source.

997. DNFBP should be required to identify the beneficial owner, where applicable, and not simply attempt to identify the beneficial owner. Legal professionals should be not exempted from the requirement to identify the beneficiary owner. Additionally, there should be a clear provision to explicitly prohibit DNFBP from establishing (or continuing) a business relationship with a customer in those instances where the ultimate beneficiary owner cannot be determined.

998. DNFBP should be required to ensure that a person acting on behalf of a legal person is so authorised.

999. DNFBP should be required when conducting on-going due diligence on the business relationship to establish, where necessary, the source of funds.

1000. DNFBP should not be permitted to waive the application of CDD measures entirely when dealing with low risk customers and products.

1001. DNFBP should be required to complete the verification of identity as soon as reasonably practicable in those cases where verification is not carried out before the establishment of a business relationship.

Applying Recommendation 6

1002. The PEP definition should be extended to cover persons entrusted with prominent public functions in a foreign country irrespective of their residence.

1003. DNFBP should be required to apply enhanced CDD measures when the beneficial owner is a PEP.

1004. DNFBP should be required to conduct enhanced on-going monitoring on the entire business relationship and not just transactions.

Applying Recommendation 8

1005. A requirement to have policies and measures to prevent the misuse of technological developments in ML/FT schemes should be introduced.

1006. DNFBP should be required to have policies and procedures to address the specific risks associated with non face-to-face business relationships when conducting on-going due diligence.

Applying Recommendation 9

1007. The provisions on reliance should be entirely amended to be brought in line with the different criteria set out under Recommendation 9.

Applying Recommendation 10

1008. The Polish legislation should explicitly empower competent authorities to request DNFBP to extend the record-keeping period beyond five years.

1009. The record-keeping period for identification data under the AML/CFT Act should commence on the date of the termination of a business relationship. Additionally, DNFBP should be required to maintain records of business correspondence.

Applying Recommendation 11

1010. The Polish authorities should consider introducing a specific requirement to pay special attention to all complex or unusual transactions and unusual patterns of transactions.

1011. Moreover, a requirement to make transaction records available to competent authorities and auditors should also be included in the law.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	PC	• Company Service Providers are not covered by the AML/CFT Act;

		• Legal professionals are exempted from the obligation to identify the beneficial owner of the client and certain other CDD requirements; • Not all the activities of notaries fall within the scope of the AML/CFT Act; ***Applying Recommendation 5*** • DNFBP are required to verify the customer identity on the basis of documents and information from a public source, but not specifically from reliable and independent sources; • There is no requirement to verify whether any person purporting to act on behalf of a legal person is so authorised; • When conducting on-going due diligence on the business relationship there is no requirement to establish, where necessary, the source of funds; • The provisions dealing with simplified CDD permit DNFBP to waive all CDD measures, except for on-going monitoring; • There is no prohibition to apply simplified CDD when there is a suspicion of ML/FT; • There is no requirement to complete verification of identity as soon as reasonably practicable in those cases where verification is not carried out before the establishment of a business relationship; **Effectiveness:** • The understanding and awareness of the obligations dealing with the identification beneficial owners of DNFBP does not appear to be adequate; ***Applying Recommendation 6*** • The PEP definition does not cover persons entrusted with a prominent public function by a foreign jurisdiction who are resident in Poland; • No requirement to apply enhanced CDD if the beneficial owner is a PEP; • There is no requirement to conduct enhanced on-going monitoring on the entire business relationship with a PEP; ***Applying Recommendation 8*** • No requirement to have policies and procedures in place to prevent the misuse of technological developments in ML/FT schemes; • No requirement to have policies and procedures to address the specific risks associated with non face-to-face business relationships when conducting on-going due diligence; ***Applying Recommendation 9*** • No requirement to immediately obtain from the third party the necessary information concerning certain elements of the CDD process; • Partial requirement to take adequate steps to ensure that that

		copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay; • No requirement to ensure that the third party is regulated and supervised and has measures in place to comply with the CDD requirements; • No measures to determine whether the country in which the third party is based adequately applies the FATF Recommendations; ***Applying Recommendation 10*** • There is no requirement empowering competent authorities to request DNFBP to extend the record-keeping period beyond 5 years; • The commencement of the record-keeping period under the AML/CFT Act in relation to customer data is not linked to the date of the termination of a business relationship; • No requirement to keep the business correspondence; ***Applying Recommendation 11*** • There is no specific requirement to make transaction records available to competent authorities and auditors; **Effectiveness:** • The manner in which Article 8a paragraph 1 is drafted could potentially detract the focus from complex, unusual large transactions or unusual patterns of transactions.

4.2 Suspicious transaction reporting (R. 16)

(Applying R.13, 15 and 21)

4.2.1 Description and analysis

Summary of 2007 factors underlying the rating

1012. In the 3rd evaluation round, Recommendation 16 was rated 'Non-compliant' based on the general deficiencies identified with respect to the reporting system and the low level of awareness of DNFPs of their reporting obligations.

1013. Since the 3rd evaluation round the level of awareness has increased significantly due to the efforts of the GIFI. During October 2009 – March 2012 additional training was provided through the E-learning platform and 19,853 DNFBPs have received a certificate for completion of a training programme.

1014. The general regime of suspicion reporting is applicable to DNFBPs in its entirety. Additionally, casinos, notaries, accountants and dealers in precious metals/stones are subject to the threshold reporting requirement.

1015. The reporting regime has also improved, however, some deficiencies still remain.

Recommendation 16 (rated NC in the 3rd round report)

Applying Recommendations 13 and 15

Requirement to Make STRs on ML/FT to FIU (c. 16.1; applying c. 13.1 & c.13.2 and SR. IV to DNFBPs)

1016. According to Article 2 paragraph 1 of the AML/CFT Act the following DNFBPs fall under the scope of application of this Act:

- entity operating in the field of games of chance, mutual betting and automatic machine games and automatic machines games of low prizes;
- notaries in so far as notary's operations concerning trading in asset values, attorneys performing their profession, legal advisers practicing his profession outside their employment relationship with agencies providing services to the government authorities and local government units, foreign lawyers providing legal services apart from his employment, expert auditors, active tax advisers;
- entities operating in so far as accounts bookkeeping services;
- entrepreneurs engaged in: auction houses, antique shops, business factoring, trading in metals or precious/semi-precious stones, commission sale or real estate brokerage;
- entrepreneurs within the meaning of the Act of 2 July 2004 on freedom of economic activity (Journal of Laws of 2007 No. 155 item 1095, as amended), receiving payment for commodities in cash of the value equal to or exceeding the equivalent of €15,000, also when the payment for a given product is made by more than one operation.

1017. As was noted under Section 3.7 of all obligated institutions including DNFBPs have a duty to report suspicious transactions to the GIFI in terms of Article 11 paragraph 1 and Article 16 paragraph 1.

1018. In addition, according to Article 11 paragraph 4 lawyers, notaries, legal advisers and foreign lawyers can report via a SRO. Nonetheless it should be noted that when lawyers, notaries, legal advisers and foreign lawyers report under Article 16 paragraph 1 Article 11 paragraph 4 does not apply.

Table 30: STRs (ML) submitted by DNFBPs

Reporting Entities	2007	2008	2009	2010	2011	01.01.2012-31.01.2012	Total
Notaries	82	41	19	122	42	11	**317**
Entrepreneurs conducting activity in the scope of commission sale	0	0	0	0	1	2	**3**
casinos, including games of chance	0	0	0	1	6	1	**8**

Entrepreneurs conducting activity in the scope precious and semi-precious metals and stones trade	0	0	0	0	1	0	**1**
real estate agents	0	0	0	0	0	0	**0**
legal advisers	0	2	3	9	5	0	**19**
tax advisers	0	0	0	4	2	0	**6**
accountants/auditors	0	0	0	5	16	1	**22**
other entrepreneurs receiving payments in cash	0	0	0	1	13	2	**16**
Total	**82**	**57**	**24**	**145**	**90**	**17**	**415**

1019. As evident from Table 30 notwithstanding the fact that all DNFBP are subject to the reporting requirements the level of reporting is low. Real estate agents have never submitted any STRs. The Polish authorities informed the evaluation team that since notaries are involved in selling and buying real estate it is their duty to report to the GIFI but not the responsibility of real estate agents.

1020. The only DNFBP that summited STRs on TF were notaries and accountants/auditors. Notaries submitted 4 STRs on TF in 2007, 2 in 2008, 1 in 2010 and 2 in 2011. Accountants/auditors submitted 2 STRs on TF in 2011.

1021. The deficiencies identified under Section 3.7 with respect to financial institutions also apply to DNFBPs.

Legal Privilege

1022. According to Article 18.4 of the Notary Law professional secrecy restrictions do not apply to the provision of information in cases prescribed by the AML/CFT Act. With respect to barristers and legal advisers according to Article 6.4 of the Law on Barristers and Article 3.6 of the Law on Legal Advisors professional secrecy restrictions do not apply in the situations prescribed by the AML/CFT Act.

1023. Although pursuant to Article 11 paragraph 5 of the AML/CFT Act legal professionals are exempted from a reporting obligation if lawyers, legal advisers and foreign lawyers, auditors and tax advisers represent their client on the basis of a power of attorney related to proceedings pending or provide advice for the purpose of such proceeding.

No Reporting Threshold for STRs (c. 16.1; applying c. 13.3 to DNFBPs)

1024. The reporting requirements under Articles 11 and 16 are not subject to any threshold limitations.

1025. Article 16 paragraph 1 covers attempted transactions, since it requires DNFBP to report when they are in possession of information indicating that a customer intends to carry out a suspicious transaction. However, no similar requirement is found under Article 11 paragraph 1.

Making of ML/FT STRs Regardless of Possible Involvement of Tax Matters (c. 16.1; applying c. 13.4 to DNFBPs)

1026. All DNFBPs are required to report suspicions of ML/FT irrespective of the nature of the underlying activity.

Reporting through Self-Regulatory Organisations (c.16.2)

1027. According to Article 11 paragraph 4 of the AML/CFT Act notaries, attorneys, legal advisers and foreign lawyers can submit information on transactions to the GIFI via a SRO, if a SRO adopts a resolution that determines detailed rules and a course how the information should be submitted to the GIFI. In addition, the SRO submits a list of persons responsible for providing such information to the GIFI.

1028. At the time of the on-site visit, none of the SROs had established such reporting regime and all DNFBPs send reports directly to the GIFI.

Legal Protection and No Tipping-Off (c. 16.3; applying c. 14.1 to DNFBPs) Prohibition against Tipping-Off (c. 16.3; applying c. 14.2 to DNFBPs)

1029. Considering that Recommendation 14 was rated 'Largely Compliant' and according to the Rules of Procedure this Recommendation is not reassessed in the 4th round, in this respect the reader should refer to the analysis of Recommendation 14 (paragraph 538) under Section 4 of the 3rd round mutual evaluation report of Poland.

Establish and Maintain Internal Controls to Prevent ML/FT (c. 16.3; applying c. 15.1, 15.1.1 & 15.1.2 to DNFBPS), independent Audit of Internal Controls to Prevent ML/FT (c. 16.3; applying c. 15.2 to DNFBPs), on-going Employee Training on AML/CFT Matters (c. 16.3; applying c. 15.3 to DNFBPs), Employee Screening Procedures (c. 16.3; applying c. 15.4 to DNFBPs), Additional Element—Independence of Compliance Officer (c. 16.3; applying c. 15.5 to DNFBPs)

1030. Considering that Recommendation 15 was rated 'Largely Compliant' and according to the Rules of Procedure this Recommendation is not reassessed in the 4th round, in this respect the reader should refer to the analysis of Recommendation 15 (paragraphs 539-540) under Section 4 of the 3rd round mutual evaluation report of Poland.

Applying Recommendation 21

Special Attention to Persons from Countries Not Sufficiently Applying FATF Recommendations (c. 16.3; applying c. 21.1 & 21.1.1 to DNFBPS), Examinations of Transactions with no Apparent Economic or Visible Lawful Purpose from Countries Not Sufficiently Applying FATF Recommendations (c. 16.3; applying c. 21.2 to DNFBPS), Ability to Apply Counter Measures with Regard to Countries Not Sufficiently Applying FATF Recommendations (c. 16.3; applying c. 21.3 to DNFBPs)

1031. The analysis of Recommendation 21 under Section 3.6 of this report in respect of financial institutions also applies to DNFBPs, as well as deficiencies noted under this section.

Additional Elements – Reporting Requirement Extended to Auditors (c. 16.5)

1032. 'Expert auditors, tax advisors' are subject to the AML/CFT Act. All the operations carried out by accountants/auditors and tax advisors are subject to AML/CFT obligations.

Additional Elements – Reporting of All Criminal Acts (c. 16.6)

1033. According to Article 111 paragraph 1 of the Criminal Code of Poland the liability for an act committed abroad is subject to the condition that liability for such an act is likewise recognised as an offence, by a law in force in the place of its commission. In view of this requirement this additional element is not covered.

Effectiveness and efficiency

1034. Since the 3rd round MER, the number of STRs from DNFBPs has increased. Nevertheless, the reporting level of certain DNFBPs is still inadequate. The FIU performed outreach activities to DNFBPs, however, no sector specific guidelines have been issued to assist these sectors.

1035. During the interviews, the representatives of the DNFBPs demonstrated a high level of awareness of their reporting obligations. The notaries queried the effectiveness of the analytical process of threshold reports, especially in view of the significant amount of reports that are submitted.

1036. During the on-site visit, the representatives of the real estate sector explained that real estate agents are not involved in the transfer of money. They were of the opinion that since the real estate agent's role in a real estate transaction is merely to facilitate a deal, the need to report STRs does not arise in practice. It was also stated that the large majority of real estate purchases are done subject to a loan and mortgage contract and activity within the real estate market is declining as a result of the recent financial crisis. Although the evaluators believe that such conditions could have an impact on the level of reporting by real estate agents, the National Program for Prevention and Combating the Organised Crime in 2012-2016, developed by the Ministry of Interior in item 3.1.5 identified "the use of real estate transactions to co-mingle income from legal and illegal sources and to carry out fictitious transactions for services and materials" among the business areas particularly vulnerable to money laundering in Poland.

4.2.2 Recommendations and comments

1037. The reporting regime for DNFBPs inherits all the positive elements and deficiencies of the reporting regime applicable to financial institutions.

1038. The Polish authorities should identify reasons for the complete absence of reporting by the real estate sector and implement measures to rectify the situation.

Applying Recommendation 13

1039. The scope of the ML reporting requirement should be extended to the reporting of "funds" suspected to be the proceeds of a criminal activity.

1040. The FT reporting obligation should be extended to "funds" as required under Criterion 13.2.

1041. The reporting requirement under Article 11 paragraph 1 should expressly provide for attempted transactions.

1042. The Polish authorities should revise the legal text of the entire reporting regime to remove any overlaps between the requirements under Article 11 and 16, to provide for a clear legal basis for the reporting of suspicious activity reports and to include an obligation to refrain from conducting a suspicious transaction before reporting it to the GIFI.

Applying Recommendation 21

1043. The Polish authorities should revise the entire provisions dealing with Recommendation 21. In particular, a specific requirement to give special attention to business relationships with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be introduced.

1044. The written findings in relation to the analysis of transactions that have no apparent economic or visible lawful purpose should be available to assist competent authorities and auditors.

1045. Competent authorities should be empowered to apply appropriate counter-measures.

1046. The PFSA and the GIFI should provide further assistance to DNFBPs regarding the practical implementation of the requirements under Recommendation 21.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	**PC**[41]	• Not all the activities of notaries fall within the scope of the AML/CFT Act; • Company Service Providers are not covered by the AML/CFT Act; ***Applying Recommendation 13*** • The scope of the reporting requirement is only linked to transactions related to ML/TF and does not extend to the reporting of "*funds"* suspected to be the proceeds of a criminal activity; • The FT reporting obligation is limited to *"transactions"* related to FT and does not extend to *"funds"*; • The deficiencies identified with respect to Recommendation 1 and Special Recommendation II restrict the scope of the reporting requirement; • Possible confusion between reporting obligations under Articles 8.3, 11.1 and 16 (e.g. attempted transactions are not covered under Article 11.1); ***Applying Recommendation 21*** • There is no requirement to give special attention to business relationships with persons from or in countries which do not or insufficiently apply the FATF Recommendations; • There is no requirement to make written findings available to assist to competent authorities and auditors; • There is no requirement to apply appropriate counter-measures; **Effectiveness:** • Low level of STRs submitted DNFBPs; • No reporting from the real estate sector despite the fact that the real estate market is considered to be particularly vulnerable to money laundering in Poland.

[41] The review of Recommendation 16 has taken into account the findings from the 3rd round report on Recommendations 14 and 15.

4.3 Regulation, supervision and monitoring (R. 24)

4.3.1 Description and analysis

Recommendation 24 (rated PC in the 3rd round report)

Summary of 2007 factors underlying

1047. In the 3rd round evaluation, Recommendation 24 was rated 'Partially Compliant' as a result of the low number of AML/CFT inspections and the lack of resources made available to supervisors.

1048. The Polish authorities have since addressed these deficiencies. The supervisory framework is similar to the framework for the supervision of financial institutions – the GIFI is the authority responsible for the AML/CFT supervision of all reporting entities and has the power to apply sanctions. Sectoral supervisors can also exercise AML/CFT supervision over respective DNFBPs.

Regulation and Supervision of Casinos (c. 24.1, c.24.1.1, 24.1.2 & 24.1.3)

1049. AML/CFT supervision over casinos (land-based and internet) is exercised by the GIFI pursuant to Article 21(1) of the AML/CFT Act and by the Ministry of Finance, namely by the Customs Service in terms of Article 21(3).

1050. All the supervisory powers that fall within the competence of the GIFI with respect to financial institutions also apply to casinos. This includes the power to conduct AML/CFT on-site inspections of casinos and to impose sanctions with respect to any identified breaches. For a more detailed explanation of the compliance-monitoring powers and functions of the GIFI reference may be made to 3.10 on R. 23 and 29.

1051. The pecuniary and penal sanctions set out under Chapter 7a and 8 also apply to casinos (see section 3.10 on R. 17). In addition, Article 59 of the Gambling Act empowers the Customs Service to withdraw a casino license in case of serious violations of regulations or where non-compliance has been not rectified within the stipulated time.

1052. In terms of Article 30 paragraph 2 of the Gambling Act (19 November 2009), the Customs Service is also empowered to carry out on-site inspections of casinos. Pursuant to Article 33 of the Gambling Act, casinos are required to:

- facilitate access to documents and records covered by the on-site inspection;
- provide copies of documentation;
- make available sketches, filming, photo- and sound-recording;
- disclose the means of communication to the extent necessary to carry out auditing procedures.

1053. Casinos are required to obtain a licence under the Gambling Act before commencing their operations. Licences are granted by the Customs Service in terms of Article 32 paragraph 1 of the Gambling Act.

1054. The conditions to obtain a licence are set out under Article 34 which states that an entity may only obtain a licence if it declares that:

- the capital originates from legal sources;
- it does not have arrears in the payment of taxes being the income of the state budget or customs duties;
- it does not have arrears in the payment of social security contributions or health insurance contributions.

1055. The application for a casino operating licence shall include, among other things:

- personal data (names, surnames, nationality, place of residence, series and number of identity document and information about education and professional experience) of the shareholders being natural persons and representing at least one-hundredth of the share capital of the company, members of the management board, supervisory board and audit committee as well as persons to become casino managers; for commercial companies being shareholders – additionally, the information about their current and past legal status and the financial standing;
- documents confirming that the capital originates from legal sources, and in particular:
    a) for a shareholder being a natural person and representing at least one-hundredth of the share capital of the company – a certificate issued by a competent head of a tax office stating the shares are covered by disclosed income sources,
    b) for shareholders being legal persons – a financial report made under separate regulations;
- valid certificates of clearance of taxes being the income of the state budget and of clearance of social security contributions and health insurance contributions;
- statements of shareholders representing shares in the value exceeding one-hundredth of the share capital of the company or members of the management board, supervisory board and audit committee stating that there are no proceedings against them underway before the justice authorities concerning the offences set forth in Article 299 of the Penal Code;
- valid certificates stating that the shareholders representing shares in the value exceeding one-hundredth of the share capital of the company as well as members of the management board, supervisory board and audit committee have not been convicted of an intentional offence or an intentional fiscal offence.

1056. Article 11 of the Gambling Act states that in respect of any person or company that owns more than 1% of the share capital in a casino, as well as any member of the management board, supervisory board or audit committee, there should be '*no justified reservations present relating to the security of the state, public order or safety of economic interests of the state*'. Additionally, these persons should not be subject to judicial proceedings relating to a money laundering offence.

Monitoring and Enforcement Systems for Other DNFBP (c. 24.2 & 24.2.1)

1057. The GIFI is the authority responsible for monitoring and ensuring compliance with the AML/CFT Act of all DNFBP (except for certain activities of notaries and TCSPs which are not subject to AML/CFT obligations). All the supervisory powers that fall within the competence of the GIFI with respect to financial institutions also apply to DNFBP. This includes the power to conduct AML/CFT on-site inspections of DNFBP and to impose sanctions with respect to any identified breaches. For a more detailed explanation of the compliance-monitoring powers and functions of the GIFI reference may be made to 3.10 on R. 23 and 29.

1058. The pecuniary and penal sanctions set out under Chapter 7a and 8 also apply to DNFBP (see section 3.10 on R. 17).

1059. Pursuant to Article 21 paragraph 3 of the AML/CFT Act, the presidents of appeal courts and tax audit authorities are empowered to monitor notaries and tax advisors, respectively, for AML/CFT compliance purposes.

1060. Various professional SROs also monitor and supervise compliance of certain categories of DNFBPs.

1061. Article 5 of the Act on Legal Advisers, establishes the National Council of Legal Advisers and District Councils, which acts as a SRO for legal advisers. The corporation is supervised by the Ministry of Justice. The corporation monitors the compliance of its members. According to the Act on Legal Advisers, the decision of the disciplinary commission of the SRO may result in the suspension of activities of a legal advisor or removal from the list of legal advisors.

1062. Article 3 of the Act on Barristers, establishes a SRO for barristers. The corporation is also supervised by the Ministry of Justice. The corporation monitors the compliance of its members. According to Article 81 of the Act on Barristers where a barrister is found to be in breach of his obligations he may be fined, his activities may be suspended or he may be expelled from the organisation.

Adequacy of resources supervisory authorities for DNFBPs (R. 30)

1063. According to an organisational chart of the GIFI, the compliance monitoring function of the GIFI is carried out by the Control Unit of the Department of Financial Information which consists of eight officers. The Control Unit is responsible for the AML/CFT supervision of the financial and DNFBP sector.

Effectiveness and efficiency (R. 24)

1064. Casinos are subject to comprehensive supervision. During the interviews, the casino representatives indicated that the Customs Service inspects casinos more than once annually (mainly for fiscal reasons). The FIU conducts a one-week inspection of every casino approximately every 2 to 3 years. Additionally, the National Bank conducts annual inspections (for casinos that operate exchange offices).

1065. The GIFI is not sufficiently equipped with human resources in order to conduct an adequate level of on-site inspections of all DNFBPs. E.g. according to the GIFI's annual report of 2010, the FIU conducted a total number of 21 on-site inspections of DNFBPs (8 notaries, 2 legal advisers, 2 casinos, and an accountant). In the same period the notarial supervisor conducted on-site inspections of 151 notaries and the Customs Service conducted 176 inspections of casinos.

1066. The SROs can provide an adequate level of AML/CFT monitoring of notaries and legal professional. At the same time, the level of supervision over the real estate agents cannot be considered as sufficient, especially taking into account the high vulnerability of real estate to money laundering.

1067. TCSPs are not subject to the AML/CFT Act and there is therefore no AML/CFT supervision over them.

1068. The Polish authorities provided statistics on the number of sanctions imposed on DNFBPs in the period 2010-2012. These sanctions were imposed for failure to identify the beneficial owner:

Table 31: Number of sanctions imposed on DNFBP

DNFBPs	No. of sanctions
Casinos	5
Public notaries	7
Foundations	2

1069. As evident from the figures presented in the table, the number of sanctions imposed for breaches of the AML/CFT Act by DNFBPs is very low.

4.3.2 Recommendations and comments

1070. Casinos, notaries and legal professionals receive sufficient attention from supervisory bodies. This is due to the involvement of Customs Service in the casinos supervision and SROs for the legal professionals. For the real estate agents, the FIU resources are not adequate, especially taking into account the complete absence of reporting and the high ML vulnerability of the real estate sector.

1071. The Polish authorities should take measures to ensure that all DNFBP, especially real estate agents, are subject to effective supervision.

1072. Additionally, the sanctioning regime for DNFBP should be reviewed to determine whether it is being effectively applied.

4.3.3 Compliance with Recommendation 24

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	**LC**	• No supervision over TCSPs; • Certain activities of notaries are not subject to AML/CFT obligations; **Effectiveness:** • Insufficient focus on the supervision of the real estate agents; • The number of sanctions imposed for breaches of the AML/CFT Act by DNFBPs is very low.

5. LEGAL PERSONS AND ARRANGEMENTS AND NON-PROFIT ORGANISATIONS

5.1 Legal persons – Access to beneficial ownership and control information (R.33)

Recommendation 33 (rated PC in the 3rd round report)

5.1.1 Description and analysis

Summary of 2007 factors underlying the rating

1073. Recommendation 33 was rated Partially Compliant in the 3rd round MER of Poland. The rating was based on the following deficiencies:

- Polish Law, although requiring some transparency with respect to immediate ownership, does not require adequate transparency concerning beneficial ownership and control of legal persons. Access to information on beneficial ownership and control of legal persons, when there is such access, is not always timely.
- No real measures in place to guard against abuse in the context of R. 33 of bearer shares.

Legal framework

1074. The Act of 15 September 2000, Code of Commercial Partnerships and Companies is a comprehensive source of commercial law and regulates the formation, structure, operation, dissolution, merging, division and transformation of commercial partnerships and companies.

1075. The Act on the National Court Register(1997) regulates the following:

- issues connected with the registration of the entities carrying on business activity,
- organisation and operation of the National Court Register.

1076. The Act on Freedom of Economic Activity (2004) as amended, regulates the following issues:

- commencement, conduct and termination of economic activity within the territory of Republic of Poland
- entering of the entrepreneur to the Central Records and Information on Economic Activity (further referred to as: CEIDG) (Chapter 3); data revealed in CEIDG is publicly available and is presumed to be true pursuant to Article 33 .
- inspection of entrepreneurs' economic activity (Chapter 5), except for inspection of banks and other institutions operating in financial market (in this respect the provisions of the Act of 21 July 2006 on Financial Market Supervision apply),
- creation in the territory of Poland of branches and agencies of foreign entrepreneurs (Chapter 6).

1077. Civil Code (Act of 23 April 1964, as amended) regulates civil law relationships among natural persons and legal persons

1078. The Act of 29 January 2004 on Public Procurement Law, as amended, regulates purchasing by public sector bodies and certain utility sector bodies of contracts for goods, works or services, tasks of public administration authorities in this respect.

1079. General issues connected with activities of the companies operating in the financial market, are regulated by the following acts:

- Act of 29 July 2005 on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies (Consolidated text: Journal of Laws of 2009, No. 185, item 1439).
- The Banking Act of 29 August 1997 .
- The Act of 29 July of 2005, on Trading in Financial Instruments
- the Payment Service Act of 19 August 2011, which entered into force on the 24th of October 2011.

1080. Rules for maintaining and keeping accountancy records are established in the Accounting Act of 29 September 1994.

1081. Pursuant to the Act on Freedom of Economic Activity an "entrepreneur" is any person, organization or non-corporate organizational unit with legal capacity conducting economic activity on its own, while 'economic activity' is defined as professional (permanent and professional activity, as opposed to occasional and amateur), subordinated to the rules of profitability and profit, repeatable and resulting in economic turnover. The term "entrepreneur" applies to natural persons, legal persons and organisational entities which are not legal persons and are endowed with legal capacity by force of a separate Act – carrying on economic activity in their own name. Partners in a civil partnership are considered to be entrepreneurs to the extent of an economic activity conducted by them. This Act is horizontal in terms of establishing rules for inspection of the economic activity of the entrepreneurs being natural persons (including partners to civil partnerships).

1082. Each entrepreneur registered in the Central Records and Information on Economic Activity (CEIDG) or in National Court Register (Register of Entrepreneurs) must place Tax Identification Number (TIN) on each written statements or declarations as well as use this number in legal and business transactions. For the purposes of the registries, the entrepreneur is identified by TIN. This is a significant change in the entrepreneurs' identification system which has been in force since the 1st of January 2007. TIN is a single identification number (basic number). All remaining numbers presently functioning, such as REGON (statistical number), KRS (NCR) number etc., will retain their significance only within a given registry.

1083. Carrying on economic activity requires prior registration in the Register of Entrepreneurs of the National Court Register or in the Economic Activity Registry.

1084. In order to perform economic activity in Poland, an entrepreneur is obligated to:

- obtain a tax identification number (TIN) at the appropriate tax office and for use in official business (official correspondence, company seals etc.),
- register in the Register of Entrepreneurs of the National Court Register (KRS), where they obtain a KRS number
- obtain an identity number based on the type of activity (REGON) at the Statistical Office,
- register the business with and pay contributions to the Social Security Office (ZUS) when employing staff,
- open a bank account and use it for all business related transactions,
- file monthly returns and pay taxes (i.e. VAT, income tax, advances on payroll tax etc.) to the local tax office,
- file financial statements and statistical reports as required by appropriate regulations.

1085. The Economic Activity in Poland may be conducted in following main forms:

- Sole Trader

-Civil Partnership

- Registered Partnership
- Professional Partnership
- Limited Partnership
- Limited Joint-Stock Partnership
- Limited Liability Company
- Joint-Stock Company

1086. -**Branch Office** - Foreign entrepreneurs may, for purposes of conducting economic activity within the territory of the Republic of Poland, create branches with a seat within the territory of the Republic of Poland. A foreign entrepreneur who creates a branch may carry on economic activity solely to the extent of the object of the foreign entrepreneur's activity. The scope of the object of economic activity of a branch office might constitute only a part of the entire business conducted by the foreign entrepreneur. Branch Office does not possess a legal personality.

1087. Obligations of a foreign entrepreneur related to the functioning of a Branch Office:

-appointment of a person who shall represent a foreign entrepreneur in the branch office

-use of the original name of the foreign entrepreneur, together with a Polish translation of the entrepreneur's legal form of operating and with words "*oddział w Polsce*" added;

-keeping of accounting records in accordance with provisions of Polish accountancy law notification of the Minister of the Economy of any factual and legal changes (the commencement and termination of any proceedings to wind-up the business of the foreign entrepreneur and of the loss of their right to conduct business activity or possess property, within 14 days following the occurrence of an event.) A **Branch Office** has to be registered in the Register of Entrepreneurs of the National Court Register

1088. **Representative Office -** Foreign entrepreneurs may create representative offices with the seat within the territory of the Republic of Poland. Object of an activity of a Representative Office is, exclusively, promotion and advertisement of a foreign entrepreneur. Representative offices may also be created by foreign persons established for purposes of promoting the economy of the country in which they have their seat, provided that the scope of activity of such an agency shall cover no other pursuits than promoting and advertising the economy of its country. Obligations of a foreign entrepreneur related to the functioning of a Representative Office are as follows : use original name of the foreign entrepreneur, together with the Polish translation of the entrepreneur's legal form of operating and with words '*przedstawicielstwo w Polsce';* added keeping of accountant records in accordance with provisions of Polish accountancy laws applicable; notification of the Minister of the Economy of: any factual and legal changes concerning data included in the application for registration of a representative office in the Register of Representative Offices (the commencement and termination of any proceedings to wind-up the business of a foreign entrepreneur and of the loss of their right to conduct business activity or possess property, within 14 days following the occurrence of an event.)

1089. A Representative Office has to be registered in the Register of the Representative Offices of Foreign Entrepreneurs kept by the Minister of Economy.

1090. The Economic Activity in Poland may be performed by Polish and EU citizens according to the same rules. Foreigners who are not citizens of any EU country may perform Economic Activity in Poland on the basis of the same rules applicable to the Polish citizens if such a foreigner possesses:

- a permit to settle, a long term residents' EC residence permit, a residence permit for e fixed period granted,(for the purpose of bringing family together or to a foreigner

who was granted a long-term residents' EC residence permit in another EU country and his/her spouse), a permit for tolerated stay,

- a refugee status, a supplementary protection, a valid card of the Pole

1091. Foreigners who do not possess any of the above indicated permits have a right to initiate and perform economic activity in a form of: limited partnership, limited joint-stock partnership, limited liability company, joint-stock company. The obligation of registration of economic activity in a competent commune binds as well foreigners who have the right to perform economic activity within the territory of Republic of Poland.

Measures to prevent unlawful use of legal persons (c. 33.1)

1092. Recommendation 33 requires countries to take legal measures to prevent the unlawful use of legal persons in relation to money laundering and terrorist financing by ensuring that their commercial, corporate and other laws require adequate transparency concerning the beneficial ownership and control of legal persons. Competent authorities must be able to have access in a timely fashion to beneficial ownership and control information, which is adequate, accurate and timely. Competent authorities must be able to share such information with other competent authorities domestically or internationally. Bearer shares issued by legal persons must be controlled.

1093. As previously described obligated institutions must, in accordance with Article 8b of the AML/CFT Act, attempt, with due diligence, to identify a beneficial owner as defined in Article 2 paragraph 1a of the same law. To enable these several publicly available tools presume to provide the necessary transparency which may prevent unlawful use of legal persons, maintaining and gathering information on business conduct. Some of them are publicly available, some of them have restricted access. More and more databases are becoming accessible on-line to dedicate authorised users. However, the most commonly used tool providing transparency, as far as it regards possible use of legal persons to unlawful activity connected with money laundering and financing of terrorism, is National Court Register (NCR).

1094. The National Court Register (NCR) is a centralised, electronic database introduced in 2001. The NCR is operated by selected district courts situated in major Polish cities and consists of three separate registers: register of entrepreneurs, register of associations, other social and professional organisations and public health service establishments and register of insolvent debtors.

1095. There are several forms of enterprises established in Poland for the purpose of undertaking business and which have to be registered in the NCR. The Register is kept in electronic form by district courts (Commercial Courts of Law; hereinafter "the registry court") with the jurisdiction which covers the area of each voivodship or a part there of (Art 2 § 1 of the Act of 20 August 1997 on the National Court Register). The Minister of Justice has established a Central Information of the National Court Register with branch offices in the registry courts and its tasks include the creation and operation of register links in the IT system, the collection of register data and providing information contained in the register. Furthermore, the Central Information shall *ex officio* provide local government bodies, which are competent for the domicile (seat) of an entrepreneur, with the Register data on entering and cancelling of an entrepreneur along with the address and scope of its activity within 7 days following the date of registration. The Central Information of the NCR shall also issue copies, excerpts and certificates from the Register; these documents have the validity of documents issued by a court. The Central Information of the NCR collects fees for these documents (the fees are income of the state budget).

1096. Access to the data of the NCR is open to the public which may also receive certified copies, excerpts and certificates on data included in the Register (Art 8 of the Act of 20 August 1997 on the National Court Register). The NCR is available on-line with a search engine that provides for the possibility to find all forms of legal persons. One may search by NCR number, by company name or legal form.

1097. Registration in the NCR shall be made upon an application, unless a specific regulation stipulates registration *ex officio* (Article 19 § 1); examples for *ex officio* registration can be found in Articles 74 § 3, 277 § 3, 464 § 3, 510 § 1. 545 § 1 and 552 of the Commercial Companies Code and Article 8.(2) of the Research Units Act (e.g. a court may obtain some information during jurisdiction; under certain circumstances such information may be registered without application). For registration an official form has to be filled in. Prior to the registration, the applicants have to pay a court fee; if the registration has to be announced in the Court and Economic Monitor, an additional fee has to be paid. The Court and Economic Monitor is the court official journal being issued by the Ministry of Justice, in which the announcements required by Polish legal acts are published.

1098. Specimens of signatures of persons authorized to represent an entity or proxy, certified by a notary or made in presence of a judge or an authorized court employee, have to be enclosed with an application for registration of the entity which has to be entered into the Register.

1099. The Application for registration shall be examined no later than within 14 days from the filing date. If the examination of application requires call for the elimination of an obstacle for registration, the application shall be examined within seven days from the date on which the obstacle was eliminated by the applicant (this does not infringe time limits stipulated in special regulations).

1100. The central and local government bodies, courts, banks, court executive officers and notaries are to immediately advise the registry court of the events which have to be entered in the Register *ex officio*. The registry court cooperates with the Head of the National Centre of Criminal Information within the scope necessary to execute its statutory tasks.

1101. The registry court examines whether the documents enclosed with the application comply with the regulations in terms of form and content. Furthermore it examines whether the data as defined by Article 35 of the Act on the National Court Register (*inter alia* for natural persons: IDs; for companies: the identification number provided by the Statistical Office) completed on the application are true. Within the remaining scope the registry court examines whether the submitted data comply with the state of affairs, if justified doubts arise in this respect (Article 23 § 2).

1102. Article 36 of the Act on the National Court Register deals with the types of entrepreneurs which have to be registered. NCR provides access to almost entire spectrum of business activity conducted in Poland (the only exception is the legal form of company - "entrepreneur running business activity"). There are 16 types of entities enumerated (e.g.; limited liability companies, joint stock companies, European companies cooperatives, state enterprises, branches of foreign enterprises etc.).

1103. Section 1 of the Register of Entrepreneurs contains the following data for each entity:

- name or company name, under which it operates,
- legal form of identification,
- head office and address,
- its previous court register number or its number in the records of economic activity,
- in the case of a legal person – information about the statutes or agreement, period for which the entity has been established and its national business registry number (REGON)

1104. Regarding a limited liability company the following data are kept:

- the amount of share capital,
- information on whether a partner can have one or more shares,
- identification of the partners who individually or jointly have at least 10 % of the share capital, and the number and total value of shares owned by these partners,

- in the case of a one-partner company – a mention that she/he is the only partner of the company

1105. Regarding a joint – stock company, the National Court Register keeps the following data:

- the amount of share capital, the number and face value of shares,
- the amount of target capital if the status prescribes it, and a mention of whether the board is licensed to issue subscription warrants or not,
- the number of preferential shares and the type of preference,
- a mention of the proportion of the share capital that has been paid,
- the face value of conditional increase in the share capital,
- if the statute prescribes the granting of a personal licence to specific shareholders or titles of participation in the company income or assets not resulting from shares – an indication of these circumstances,
- in the case of a one-shareholder company – identification of the shareholder and mention that she/he is the only shareholder of the company,
- a mention of the resolution on the issue of convertible bonds and shares given in exchange for these bonds, a mention about the bondholders` right to participation in profits

1106. In accordance with Article 40 of the Act on the National Court Register, Section 3 of the register of entrepreneurs includes *inter alia* the following data:

- a mention that an annual financial statement was filed and mention of the filing date,
- in the case of limited liability companies, insurance undertakings, joint stock companies and cooperatives – a mention that the statement on their activity was filed, if the regulations concerning accountancy require it to be filed with the registry court.

1107. Sections 2, 4, 5 and 6 of the register on entrepreneurs include data on representative bodies, supervisory bodies, tax and customs in arrears under enforcement, mention of appointing and dismissing a trustee, information on initiation and termination of liquidation etc.

1108. The Polish authorities indicated that documents supporting application to be entered on the register are also available to the public on request (e.g. financial statements, deeds of partnership etc.).

1109. During the onsite visit the evaluators where advised that as of this year registration in the NCR can now be done online remotely even from abroad. Such registration is performed apparently with no additional checks or due diligence which raises some concern as to the accuracy of such registration.

1110. Another new relevant registry is with the Ministry of Economic Affairs which runs the Central Registry and Information on Economic Activity (CEIDG) which was created in 2011 in accordance with the amendments to The Act on Freedom of Economic Activity. The register includes anybody who wishes to conduct business in Poland and as confirmed in a recent court case this includes E-Business as well. The Registry includes all the necessary identification data on entrepreneurs (i.e. individual person who run own business) and partners working individually civil partnerships. The access to the register is possible by the Internet.

1111. The Act on Freedom of Economic Activity (2004) regulates the following issues:

- entering of the entrepreneur to the Central Records and Information on Economic Activity (CEIDG, Chapter 3); data revealed in CEIDG is publicly available and is presumed to be true pursuant to Article 33 of the Act on Freedom of Economic Activity;

- inspection of entrepreneurs' economic activity (Chapter 5), except for inspection of banks and other institutions operating in financial market (in this respect the provisions of the Act of 21 July 2006 on Financial Market Supervision apply),
- creation in the territory of Poland of branches and agencies of foreign entrepreneurs (Chapter 6).

1112. To be able to commence activity, a natural person should complete and submit the application for entry into the CEIDG. The application for entry into CEIDG must be accompanied by the statement on the lack of prohibitions pronounced with regard the applicant, made under pain of criminal liability for making a false statement. The entrepreneur has the right to indicate in the application for entry into CEIDG a later day of commencement of economic activity than the day of the application submission. The entrepreneur has the right to start economic activity on the day on which the application for entry in CEIDG is submitted.

1113. The application for entry in CEIDG may be field:

- **on line** – using electronic signature, verified on the basis of qualified certificate, signature confirmed by means of entrusted profile at ePUAP, or personal signature referred to in legal provisions on personal identity cards, or using any other manner accepted by CEIDG that allows for definite identification of the person submitting the application and the time of submitting it;
- **in gmina office** – (the **gmina** is the principal unit of administrative division of Poland at its lowest uniform level) in person or by registered mail (an application sent by registered mail should bear the handwritten signature of the applicant certified by a notary public). If the application for entry into CEIDG is submitted in person, the gmina office verifies the identity of the entrepreneur and confirms the acceptance of the application by means of a confirmation of receipt. An applicant needs to present his/her personal identity card or other identity document.

1114. Should the application for entry into CEIDG be incorrect: 1. if the application was submitted on line – CEIDG will immediately notify of the incorrect data in the application; 2. if the application was submitted in the gmina office – the body will immediately call for amending or supplementing the application within 7 working days.

1115. Upon registration identification is verified with other national databases, though the evaluators were surprised to learn that no such verification is conducted with regard to foreign passports and other identity documents.

1116. Additional databases are maintained by the competent authorities (the access to the particular ones is dependent on the powers of the particular authorities, the access may be direct or indirect, some of them are accessible on-line). Databases available are as follows:

- **SIGIIF** – the internal database kept by the GIFI and accessible exclusively by the GIFI. It contains threshold transactions, STRs, data concerning analytical issues, as well as information on cash declarations over €10,000 (the latter one – until 2008 was kept in RWPG database. Since 2011 – customs authorities input data on border cash declarations electronically, directly into SIGIIF).
- **KCIK** (National Centre of Criminal Information) - administered by the Police
- **KEP** (National Tax-payers Register) – gathers data of natural and legal persons; provides possibility to verify some information by searching the usage of NIP number in business conduct. It has applications, e.g. to search links between entities, contacts to the persons analysed, identity documents, bank accounts, nationality, etc.

- **KRS** (National Court Register) - publicly available database, administered by the Ministry of Justice. (For details – see above).
- **PESELnet** (access to the database gathering information on personal identification number assigned to Polish citizens)
- **CELINA** (system of analysis of customs declarations) – one may search by: name, REGON (number assigned by National Register of Business Activity that is maintained by the Central Statistical Office), PESEL (personal identification number), NIP (tax identification number). The effects of searches are SAD documents, which define country of destination, date, entity name (importer/exporter), identification data, description of goods, as well as the value.
- **VIES** - database which gathers data on turnover of goods within the EU, such as quotas from customs declarations, dates and country of destination, data that may identify the ordered/foreign beneficiary (e.g. VAT-EU number, name, address)
- **REMdat** (tax declarations register)
- **CERBER** (bank accounts and accounts held by cooperative savings and credit unions, including deposits register) - one may use applications enabling him to search by accounts owned by particular owner.

Timely access to adequate, accurate and current information on beneficial owners of legal persons (c. 33.2)

1117. Essential criterion 33.2 requires that competent authorities be able to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons and this information is not required in the company register. There have not been any improvements since the 3rd MER as to the access to information on the ownership of companies (and particularly joint stock companies) in particular on the ultimate beneficial owners. The prosecutors met onsite informed the evaluators that the limited access to information on the beneficial ownership was an obstacle in cases where the company was represented by a straw man in transactions claiming that he/she was the fully responsible owner of the company.

1118. The AML/CFT Act gives power to the GIFI to compel production of information that may refer to the beneficial ownership or any financial information for the purposes of conducted analysis. In line with Article 13a:

> *"1. At the written request of the General Inspector, any obligated institution shall immediately disclose any information about the transactions covered by the provisions of the Act. Such a disclosure consists in particular the provision of information about the parties of transaction, the content of documents, including the balances and turnovers on the account, provision of certified copies of theirs, or a disclosure of relevant documents for insight of the authorized employees of the unit referred to in Article 3 paragraph 4 in order to produce notes or copies.*
>
> *2. The information referred to in paragraph 1, shall be forwarded to the General Inspector free of charge.*
>
> *3. The General Inspector may request to be provided with the information referred to in paragraph 1 in an electronic manner."*

1119. Moreover, there is good practice worked out that in correspondence with the obligated institutions the GIFI requests information to be delivered within fortnight. In urgent cases – there is request to forward information to the GIFI immediately.

1120. Similarly to the above mentioned powers of the GIFI towards obligated institutions, the Article 15 of the AML/CFT Act provides for the obligations imposed on cooperating units in this regard:

> "*At the request of the General Inspector, all the cooperating units are obligated to provide, within their statutory authority, any information necessary to carry out his tasks in the field of prevention as referred to in Article 165a* [i.e. financing of terrorism offence] *and Article 299 of the Penal Code* [i.e. money laundering offence]."

1121. Article 14 of the AML/CFT Act set out the obligation to inform the GIFI on the ML/FT suspicious cases that were analysed by the Prosecutor's Office, the Internal Security Agency, the Central Anticorruption Bureau and the units subordinated to the minister competent for internal affairs and supervised by him.

1122. According to the Customs Service Act (2009) in the course of the proceedings conducted in cases of fiscal crimes and offences the units subordinated to the Minister competent for Financial Institutions (Fiscal Control, Customs Service, Tax Administration) can request the bank to provide the following information concerning the suspected person:

- their bank accounts or savings accounts, its number, turnover and balance;
- their cash accounts or securities accounts, its number, turnover and balance;
- concluded credit or loan agreements as well as deposit agreements;
- Treasury Shares or Treasury Bonds purchased via banks as well as trading in these securities;
- turnover of deposit certificates issued by banks or other securities.

1123. This also applies to non-bank operators leading brokerage companies and cooperative savings and credit. Also, fund managers, upon written request of a competent authority, are required to prepare and submit, at its own cost, information about the discontinued units of participation.

1124. Please be advised that any responsibilities PFSA may have not to allow criminals to hold interest in legal persons fall under the requirements set out under criterion 23.3.

1125. The powers of the PFSA to request information and data are described mostly under Recommendation 4.

1126. Polish FSA has access to all information which are in the possession of financial institutions operating under its supervision in the territory of the Republic of Poland. The disclosure requirements are set out in laws regulating respective financial sectors,(banking secrecy - Article 105 paragraph 1 point 2 of the Banking Act , Capital market secrecy - Article 88 of the Act on trading in financial instruments, Article 225 paragraph 2 of the Act on investment funds, Insurance secrecy - Article 19 of the Act on insurance activities)

1127. The mentioned provisions also allow the exchange of information between proper authorities, however it is important to mention that in AML/CFT respect the PFSA uses the provision of Article 15a of the AML/CFT Act which states:

> *"1. Within their statutory authority, the cooperating units, with the exception of the bodies referred to in Article 14 paragraph 2, are obligated to cooperate with the General Inspector on the prevention of the criminal offences referred to in Article 165a and Article 299 of the Penal Code, by:*
>
> *1) immediately notifying the General Inspector on any suspicion of money laundering and terrorist financing;*
>
> *2) submitting certified copies of documents relating to the transactions for which there is a suspicion that they are connected to criminal offences referred to in Article 165a and Article 299 of the Penal Code, along with the information on the parties of such transactions.*

2. Cooperating units are required to have an instruction for the cases referred to in paragraph 1."

1128. PFSA as a cooperating unit in the sense of this article has a procedure referred to in paragraph 2 of this article.

1129. The Customs have powers to execute number of responsibilities of entities being under control. According to statutory rules prescribed in the Customs Service Act those entities are generally obligated to provide conditions and means for carrying out a control (The Customs Service Act, Article 33) including:

- facilitating insight to documents and records covered by the control,

- facilitating preparation of copies of the documentation

- facilitating preparation of sketches, filming photo- and sound recording

- disclosure of means of communication to the extent necessary to carry out auditing procedures

- delivering of any explanation in matters of the control.

Prevention of misuse of bearer shares (c. 33.3)

1130. In Poland legal persons are able to issue bearer shares both in private as in publicly traded companies. Trades in public companies are registered in the National Depository for Securities. However they have no information on the volume of such shares existing on the Polish market. The Polish authorities indicated that the holder of a bearer share would be identified if he or she seeks to vote in an annual shareholder meeting. The Polish authorities understood that this does not prevent the holder of a bearer share handing it to a third party for the exercise of his voting rights in an annual meeting on behalf of an (unidentified) shareholder. During the onsite visit the Polish authorities were unable to provide any statistics as to how wide spread bearer shares were in use in practice.

1131. In line with Article 5 of the Act on Trading in Financial Instruments of 29 July 2005, securities which are offered in a public offering or admitted to trading on a regulated market, or introduced to an multilateral trading facility, or issued by the State Treasury or the National Bank of Poland – shall exist in uncertificated form as of the date of their registration under the agreement on the registration of the securities in the securities depository (dematerialisation). The Polish authorities consider this to suffice against the risk of misuse of bearer shares of public companies, as in these cases it is always possible to point the owner of shares.

1132. Securities may also exist in uncertificated form if permitted under separate regulations concerning the issue of such securities.

1133. An issuer of securities, which are mentioned in Art 5.1, shall conclude with the National Depository for Securities an agreement on the registration of the securities in the depository for securities.

1134. Securities which are offered in a public offering but are not to be admitted to trading on a regulated market, or introduced only to an multilateral trading facility, do not have to undergo dematerialisation, mentioned in Art 5.1 of the Act on Trading in Financial Instruments , if so determined by the issuer.

1135. In the case of securities issued outside the Republic of Poland, only the portion of such securities which is to be offered in a public offering, or securities which are to be traded on a regulated market or introduced to a multilateral trading facility in the Republic of Poland, shall be subject to registration.

1136. The conclusion of the agreement on the registration of rights to shares and on the registration of shares in a depository for securities with a company other than a public company shall

require an authorisation in the form of a resolution of the general shareholders meeting of the company, and if the issuer has its registered office outside the territory of the Republic of Poland - in the form of a resolution adopted by the appropriate decision-making body of the issuer. An authorisation to conclude the agreement on the registration of shares in a depository for securities is synonymous with an authorisation to conclude an agreement on registering, in a depository for securities, rights to shares, which confer the right to receive those shares.

1137. Moreover Article 7 paragraph 1 of the Act on Trading in Financial Instruments defines the moment of registering dematerialized securities as the moment when the rights thereof start to exist:

"1. The rights attached to dematerialised securities shall accrue as of the moment such securities are first registered in a securities account and shall inure to the benefit of the account holder."

1138. Nonetheless, the Polish authorities consider that several measures were taken, in their view, to mitigate the risk of abuse of bearer shares. Broker dealers can provide safekeeping of shares issued by companies, which is done usually under a written agreement with the company itself and which allows to keep track of owner changes. The PFSA supervises only the way in which this activity is being conducted, and transaction conducted in this way are expected to be registered under the provisions of article 8 section 1 of the AML/CFT Act. Similarly, these services would be registered, if performed, by a notary. Nevertheless, as the Polish authorities themselves point out, safekeeping of shares is not mandatory, in this respect the risk of abuse of bearer shares in private companies remains.

1139. When private companies with bearer shares want to go public, a person presenting the shares to dematerialisation (as they should be always) must prove the full chain of ownership. This of course is important but does not allow real time supervision of ownership change, which may be misrepresented ex post factum.

1140. According to Article 921^{12} of the Polish Civil Code - the transfer of rights from a bearer instrument require the hand-over of the instrument. The legal act of share transfer creates a new 2% tax obligation based on a self-declaratory system 14 days after the transaction. Nevertheless the evaluators consider the impact of such a self-declaratory system, when no other regulatory measures exist, to be limited.

1141. To conclude this point legal persons are able to issue bearer shares. Nevertheless Poland has not taken the appropriate measures to ensure that bearer shares of private companies are not misused for money laundering, and that the principles set out in criteria 33.1 and 33.2 apply equally to legal persons that use bearer shares.

Additional element - Access to information on beneficial owners of legal persons by financial institutions (c. 33.4)

5.1.2 Recommendations and comments

1142. Polish Law does not clearly provide information about the beneficial ownership of companies as it is defined in the Glossary to the FATF Recommendations (i.e. who ultimately owns or has effective control). This is particularly the case where one company buys shares of another company and so on. There is no requirement to identify for the Register the beneficial owners of a company which holds shares of another registered company. Similarly foreign companies are registered in Poland. Also, in relation to such foreign companies, beneficial ownership information is not available. In some cases, information on beneficial ownership may be available in the company's books at the registered office.

1143. During the onsite visit several representatives from different law enforcement agencies all conveyed to the evaluators their frustration due to insufficient available information as to beneficial ownership both with regard to domestic and foreign legal entities.

1144. It thus appears to the examiners that Polish law does not require adequate transparency concerning beneficial ownership and control of legal persons and it is bound to be difficult and lengthy for competent authorities to obtain the necessary information. Polish authorities can in practice rely on investigative and other powers of law enforcement to produce from company records the immediate owners of companies. However if these in turn are also legal persons, the competent authorities have to investigate further up the chain.

1145. It was already recommended in the 3rd round evaluation that Poland reviews its commercial, corporate and other laws with a view to taking measures to provide adequate transparency with respect to beneficial ownership.

1146. This recommendation is hereby reiterated and reinforced due both to technological advancement of the NCR which poses new challenges as to the authenticity of the information provided by the NCR, and considering the comments from law enforcement agencies.

1147. Moreover there are no real measures in place to guard against abuse in the context of R. 33 of bearer shares. Measures should be put in place to address this issue.

5.1.3 Compliance with Recommendation 33

	Rating	Summary of factors underlying rating
R.33	**PC**	• Polish Law, although providing some transparency with respect to immediate ownership, does not require adequate transparency concerning beneficial ownership and control of legal persons; • Access to information on beneficial ownership and control of legal persons, when there is such access, is not always timely; • No real measures in place to guard against abuse in the context of R. 33 of bearer shares of private companies.

5.2 Legal arrangements – Access to beneficial ownership and control information (R.34)

Recommendation 34 (rated N/A in the 3rd round report)

5.2.1 Description and analysis

Summary of 2007 factors underlying the rating

1148. In the third round mutual evaluation report Recommendation 34 was rated as non-applicable.

1149. The evaluation team of the previous round rated R.34 as "not applicable" and found out that domestic trusts cannot be established in Poland. The evaluators were advised that the reason for that was that the different types of enterprises are provided by the Polish law and that there was no such type foreseen in Polish law and could not be registered in the National Court Register.

1150. The evaluators of the present round are not aware of any different information in this respect. There is no provision in domestic law which allows for the formation of trusts in Poland and they cannot be registered as such according to the legislation in force and therefore cannot be recognised in law. In this respect the Recommendation stands.

5.2.2 Recommendations and comments

1151. Recommendation 34 is not applicable.

5.2.3 Compliance with Recommendation 34

	Rating	Summary of factors underlying rating
R.34	**N/A**	

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and analysis

Special Recommendation VIII (rated NC in the 3rd round report)

Summary of 2007 factors underlying the rating

1152. Special Recommendation VIII was rated based on the following conclusion:

- no special review of the risks in the NPO sector has been undertaken. Though there is some financial transparency and reporting structures; these measures do not amount to effective implementation of the essential criteria VIII.2 and VIII.3. Consideration needs to be given to ways in which effective and proportionate oversight of this sector can be achieved in the context of SR VIII.

Legal framework

1153. In Poland the NPO sector comprises various NGOs: corporate and non-corporate entities not forming part of the public finance sector, not operating for profit, and formed against relevant legislative provisions, including foundations and associations, religious organisations and unions and also local authority unions.

1154. In the Polish legal system NPOs are foundations, associations and other entities. There are also associations and other subjects referred to in art 3 paragraph 2 of the Act on public Benefit and Volunteer Work of 24 April 2003:

> *Non-governmental organisations are:*
>
> *1) entities which do not form part of the public finance sector as defined in the Act on Public Finance;*
>
> *2) which do not operate for profit – corporate and non-corporate entities, which according to separate legal provisions have capacity to perform acts in law, such as foundations and associations, subject to § 4.*

1155. The basic acts regulating the functioning of foundations in Poland are:

- Constitution of the Republic of Poland of April 2, 1997
- Act on Foundations of 6 April 1991
- Decree of the Minster of Justice of 8 May 2001 regarding the scope of activities of foundations
- Act on law on associations of 7 April 1989
- Act on public Benefit and Volunteer Work of 24 April 2003

- Other acts (e.g. the Accounting Act of 29 September 1994; the Act of 15 February 1992 dealing with income taxation of legal entities; the Act of 26 November 1998 dealing with public finances).

1156. The Act on Foundations does not provide a definition of foundations and leaves that to jurisprudence. The only requirement for a foundation is that its aims must be based on public benefit. Foundations with personal goals (so-called private foundations which operate for the benefit of a private person or his family) are prohibited. The rules do not regulate any other aspects of a foundation other than those described above.

1157. A foundation can be established by private individuals, regardless of their citizenship or residence, or by legal entities. The headquarters of a foundation must be located in Poland. Foreign foundations may establish a branch in Poland, which can begin its activities after receiving permission from the appropriate ministry.

1158. The founder of a foundation must draw up a charter for it and indicate the property which will be used to accomplish the goals listed in the charter. There are no maximum or minimum limits by law on the amount of property a foundation must have or may acquire. Property may be in the form of money, shares, liquid assets or real estate. A foundation must be established with a notarised act. Before starting its activities, a foundation must be entered in the appropriate register (i.e. for associations, social organisations, etc. at the National Court Registry). Founders must provide evidence of a location for their foundation. They also have to show the property and funds which will be used to obtain their goals, although they do not have to specify exactly how much they own. Each foundation is required to submit an annual report on its activities to the appropriate ministry. This report should also be made public. The Ministry of Justice dictates the range of information which must be included.

1159. If a foundation seriously breaks the law then the appropriate ministry may obtain a court order to suspend the foundation's board and appoint in its place administrators from outside the foundation.

1160. The Act of 24 April 2003 on Public Benefit and Volunteer Work (Annex 24) sets rules for:

- engaging in public benefit work by non-governmental organisations, and the use of such work by public administration authorities when performing public benefit tasks;
- securing public benefit organisation status by non-governmental organisations, and operating public benefit organisations (PBO) and
- supervision to be exercised over public benefit work.

1161. PBOs have to fulfil all the requirements listed in Article 20 and 21 of this Act, i.e.:

- their statutory activities include work to the benefit of the entire society;
- they do not engage in for-profit business operations or engage only in operations to an extent sufficient to cover the due performance of statutory tasks;
- their entire income is allocated to activities as defined by Paragraphs 1 and 2 of Article 20;
- they have a statutory collegiate audit or supervision body, separate from the management body and not reporting thereto within the scope of internal audit or supervision (members of such audit and supervision body shall *inter alia* not be members of the management body, shall not have been convicted by virtue of a final court judgment for any crime involving intentional fault).

1162. The statutes, articles of association, or other internal documents of non-governmental organisations or entities specified in Article 3 § 3 of this law (i.e. local authority organisation unions and entities with a religious purpose), have to prohibit the following:

a) issuing loans or pledging the organisation's property to cover any financial liabilities of such organisation's members, authority members, employees, or the spouses, relations, or relations in lineal or collateral affinity thereto, or of individuals remaining in adoption, guardianship, or *ad hoc* guardianship therewith, all of whom jointly referred to as "next of kin",

b) the transfer of their property to such organisation's members, authority members, employees, or their next of kin under terms and conditions other than those applying to unrelated third parties, in particular should such transfer be free of charge or under preferential terms,

c) the use of the organisation's property to aid such organisation's members, authority members, employees, or their next of kin under terms and conditions other than those applying to unrelated third parties, unless such use stems directly from the statutory objectives of such organisation or entity defined in Article 3 clause 3,

d) the purchase under special terms of commodities or services from entities whose operations are engaged in by such organisation's members, authority members, employees, or their next of kin.

1163. Non-governmental organisations and local authority organisation unions which have been registered in the National Court Register gain public benefit organisation status from the time of the entry of data proving conformity with the requirements as described above. NGOs shall lose - *ex officio* or upon application - their public benefit organisation status as of the date of removal of data proving conformity to requirements under Article 20 from National Court Register.

1164. A public benefit organisation has to draft and submit annual performance reports describing its activities; these reports have to be made public by the organisations. Furthermore PBOs have to draft and publish annual financial statements. Regardless of any obligation arising from separate legal provisions, a PBO has to submit the report and statement to the minister responsible for social security issues.

1165. According to Article 29 § 1 in conjunction with Article 28 § 1, the operation of PBOs is supervised by the minister responsible for social security issues (at the time of the on-site visit the Ministry of Labour and Social Policy). The ministry has to supervise that the benefits of the organisations are duly and properly used. For public benefit organisations which are active in rescue services and civil defence, the Minister for Home Affairs shall supervise their operations in terms of their performance of public tasks commissioned, and the due and proper form of their use of benefits described herein (Article 28 § 2).

1166. An audit procedure is announced *ex officio* by the minister or upon application by a public administration authority and is performed by individuals duly authorised in writing by the minister. The final audit results contain a description of the *status quo* found in the course of the audit, including any disclosed misdemeanours (reasons for their arising, the scope and results of such misdemeanours) and the deadline for their removal which should be no shorter than 30 days.

1167. The endorsement in the register "public benefit organisation status" has constitutional effect [meaning that only the entry in the Register provides this status]. Should a public benefit organisation fail to remove the detected misdemeanours, the minister has the right to apply to the court of registration to remove the information concerning the public benefit organisation status, or to delete such an organisation from National Court Register.

1168. According to Article 2 of AML/CFT Act foundations as well as associations with corporate personality established under the Act of 7 April 1989 - Law of Associations are the obligated institutions that fall within the scope of obligations imposed by the Act. They are subject to reporting obligations in line with AML/CFT regime, and they apply CDD measures.

1169. The above mentioned Institutions from NPO sector are obligated to apply CDD measures, in line with Article 8 b of the AML/CFT Act:

> *"1. Any obligated institution shall apply financial security measures for its clients. Their scope is determined on the basis of risk assessment as for money laundering and terrorist financing, hereinafter referred to as "risk assessment", resulting from the analysis, taking into account in particular type of a client, economic relationships, products or transactions."*

1170. NPOs in Poland must comply with the reporting obligations imposes by the AML/CFT Act in Article 8 paragraph 3 [i.e. registering suspicious transactions] and Article 11 [i.e. forwarding registered transactions to the GIFI]

1171. (For more detailed information on CDD measures applied by the above mentioned obligated institutions – please see section on Recommendation 12; for more detailed information on reporting regime – see section on Recommendation 16, as they both refer to the relevant sector of obligated institutions.)

1172. The Interpretation of the provisions of the Act of 24 April 2003 On Public Benefit and Volunteer Work is within Ministry of Labour and Social Policy competence. The above mentioned act regulates the rules for performance by non-governmental organizations of public benefit activities, cooperation of public administration authorities with NPOs what includes entrusting NPOs with the performance of public tasks and awarding a grants. The act regulates also the procedure of granting, loosing the NPO's status and executing the supervision of the NPOs' activity.

1173. Preparation of the executive acts is also within Ministry of Labour and Social Policy competence.

1174. According to the above mentioned act every organization granted NPO status is obligated to draft annual performance report and financial statement describing its activity, which shall be both submitted to Ministry of Labour and Social Polic, in line with Article 23 of the Act of 24 April 2003 On Public Benefit and Volunteer Work. Since 1.01.2012 the submission is exercised in electronic form on Ministry of Labour and Social Policy website. This gives the opportunity to obtain all the statistic information about subjects and data from National Court Register and increases the transparency of the sector.

Review of adequacy of laws and regulations (c.VIII.1)

1175. The Polish authorities have not indicated whether a formal Review of adequacy of laws and regulations has been conducted. During the on-site visit the evaluators were told that such an interagency meeting took place 2 years ago followed by a series of steps addressing the risk of terrorist financing within the NPO sector.

1176. Following this meeting steps were taken as to enhancing transparency (e.g. with regard to NPOs participating in government tenders) and establishing an IT system with information regarding NPOs.

1177. Since May 2012 there is electronic database available gathering statements of public benefit organisations. There are financial statements involved, as well as those on the activity of PBOs. The database is publicly available at the website of the ministry of Labour and Social Policy **(**http://www.sprawozdaniaopp.mpips.gov.pl/**).**

1178. Mentioned to the evaluators was the Ministry of Digitization which registers on a voluntary basis the different practicing denominations in Poland (173 different ones) seeking tax relief offered to religious NPOs. No information is gathered by the ministry with regard to the persons behind these NPOs (directors, trustees etc.)

Outreach to the NPO Sector to protect it from Terrorist Financing Abuse (c.VIII.2)

1179. The provisions of the Section III of the Act of 24 April 2003 On Public Benefit and Volunteer Work regulate the requirements and obligations of the NPO. Publication of submitted performance reports and financial statements is part of the transparency policy that may result in diminishing the potential risk of using the sector for financing terrorism purposes.

1180. Moreover the GIFI provides e-learning platform that is efficient tool to raise awareness of obligated institutions in the scope of preventive measures concerning AML/CFT area.

1181. As far as it regards e-learning statistics in the sector: the GIFI has trained via e-learning facility 327 persons from foundations, and 121 persons from associations in the years 2009-2012, which totally makes the number of 448 employees trained in the AML/CFT area as follows:

2009 – 7 from foundations; 1 from associations

2010 – 125 from foundations; 62 from associations

2011 – 168 from foundations; 49 from associations

2012 – 27 from foundations; 9 from associations.

Supervision or monitoring of NPO-s that account for significant share of the sector's resources or international activities (c.VIII.3)

1182. In the case of foundations (Article 12 of the Law on Foundations) the court decides about the compliance of foundation's actions with the law, statute and the purpose for which the foundation was set up in non-litigious proceedings at the request of the competent minister or the mayor. The foundation annually submits a report of its activities to the competent minister which is also made accessible to the public.

1183. In accordance with Article. 8 paragraph 5 of the Act of 7 April 1989 Law on Associations:

"Supervision of the activities of the associations adheres to:

1)voivod competent with respect to the seat of the association - the supervision of activities of the associations of local governments,

2)proper governor for the seat of the association - the supervision of other than associations mentioned in point 1

- Hereinafter referred to as "regulatory bodies".

1184. Pursuant to Article 25 of the above Act supervisory authority is entitled to require the provision by the Board of the Association, within the prescribed period, copies of resolutions of the General Assembly (meeting of delegates) require of the Association authorities necessary explanations:

"*The supervising agency has the right:*

1) to demand that the board of an association supply copies of acts passed by general assembly (assembly of delegates) within a specified period of time;

2) to review documents concerning activities of the association and to make notes, excerpts and copies of them at the seat of an association and in the presence of association authorities' representative;

3) to demand appropriate explanations from the authorities of an association."

1185. The entitled PBOs may receive a personal taxpayer donation in amount of 1 % of personal income tax. Those PBOs are under the Ministry of Labour and Social Policy constant supervision. When informed that the funds received are not used appropriately or when cast doubts as to the data incorporated into reports – the Ministry of Labour and Social Policy is entitled to demand the NPO to

provide necessary clarifications and to exercise control procedure due to the provisions of the Section IV of the Act of 24 April 2003 On Public Benefit and Volunteer Work.

Information maintained by NPO-s and availability to the public thereof (c.VIII.3.1)

1186. Data on performed activity and aim of PBOs, members of the management and controlling bodies are publicly available on Ministry of Labour and Social Policy website. Moreover that information shall be published on the NPO's website. National Court Register also has the data registered and publicly available. Due to the Act of 24 April 2003 On Public Benefit and Volunteer Work, Foundation and Association Law, PBOs shall have statute as an internal document which regulates the functioning procedures and the statutory objectives of its target.

Measures in place to sanction violations of oversight rules by NPO-s (c.VIII.3.2)

1187. Due to the Act of 24 April 2003 On Public Benefit and Volunteer Work PBOs are under the Ministry of Labour and Social Policy supervision. When revealed during the control proceed or other supervising activity undertaken that the NPO is not appropriately managed – the Ministry of Labour and Social Policy is entitled to put forward the motion to remove the NPO form the National Court Register.

Licensing or Registration of NPO-s and availability of this information (c.VIII.3.3)

1188. Due to the Act of 24 April 2003 On Public Benefit and Volunteer Work NPOs, when legally obligated, acquire the status of a public benefit organization at the moment they are included in the National Court Register. Data on legal obligation fulfilment is publicly available on Ministry of Labour and Social Policy and Ministry of Justice websites.

1189. In accordance with Article 7 of the Act of 6 April 1991 on Foundations:

> *"1 The Foundation is subject to enter into the National Court Register."*
>
> *2. The Foundation acquires legal personality upon entering the National Court Register"*

1190. In accordance with Article 8, par. 1 of the Act of 7 April 1989 Law on Associations:

> *"Association has to enter the National Court Register, unless the provision of the Act provides otherwise."*

Maintenance of records by NPO-s, and availability to appropriate authorities (c.VIII.3.4)

1191. The legal duty of data on accepted annual reports collecting is subject to accounting regulation Article 74.1 and 74.2 of the Accounting Act.

Measures to ensure effective investigation and gathering of information (c.VIII.4)

1192. Due to the Act of 24 April 2003 On Public Benefit and Volunteer Work every organization granted PBO status shall draft annual performance report and financial statement describing its activity, which shall be both submitted and published on Ministry of Labour and Social Policy website. Moreover that information shall be published on the NPO's website. Publication of submitted performance reports and financial statements is part of the legal requirement for the transparency policy.

Domestic co-operation, coordination and information sharing on NPO-s (c.VIII.4.1); Access to information on administration and management of NPO-s during investigations (c.VIII.4.2); Sharing of information, preventative actions and investigative expertise and capability, with respect to NPO-s suspected of being exploited for terrorist financing purposes (c.VIII.4.3)

1193. Basic data concerning the NPOs is collected by Ministry of Labour and Social Policy, Ministry of Justice and Ministry of Finance. In individual cases all above mentioned organs cooperation guarantee successful supervision on the NPO.

1194. According to the Act of 24 April 2003 On Public Benefit and Volunteer Work, during the control proceed, the Minister of Labour and Social Policy is entitled to access all the data and documents of NPOs.

1195. There are special provisions under the AML/CFT Act which regulate the information sharing on AML/CFT issues among all relevant competent authorities, (which is not regulated by the Act of 24 April 2003 on Public Benefit and Volunteer Work). The provisions of the Articles 15, 15a, 15b of the AML/CFT Act are relevant in this respect, as long as the subject matters of the cooperation and sharing of information among the cooperating units are the information about the NPOs. Under the meaning of Article 2 point 8 cooperating units are any government and local government authorities and other public organizational units, as well as the National Bank of Poland, the Polish Financial Supervision Authority and the Supreme Chamber of Control.

1196. At the request of the General Inspector, all the cooperating units are obligated to provide, within their statutory authority, any information necessary to carry out his tasks in the field of prevention as referred to in Article 165a and Article 299 of the Penal Code. The cooperating units (excepted the Prosecution Office, the Internal Security Agency, the Central Anticorruption Bureau and the units subordinated to the minister competent for internal affairs and supervised by him) are obligated , according to the Article 15a to immediately notify the General Inspector on any suspicion involving committing money laundering and terrorist financing and to submit certified copies of documents relating to the transactions for which there is a suspicion that they are related to the commitment of crimes referred to in Article 165a and Article 299 of the Penal Code, along with the information on the parties of such transactions.

1197. Article 14 of the AML/CFT Act provides for the cooperation and the sharing of information among the Prosecution Office, the Internal Security Agency, the Central Anticorruption Bureau and the units subordinated to the minister competent for internal affairs and supervised by him and the GIFI on all the cases involving receipt of information indicating suspicion of crimes having been committed as referred to in Article 165a and Article 299 of the Penal Code. The GIFI shall immediately notify these authorities of the circumstances indicating the connection between the information obtained in the manner specified in this provision, and information on the transactions referred to in Article 8 paragraph 3, Article 16 paragraphs 1 and 1a, and Article 17 of the AML/CFT Act. This mechanism is also available in respect of NPOs related information.

1198. The Border Guard and the Customs authorities shall provide the General Inspector with the information referred to in Article 5 of 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, and with the information contained in the declaration referred to in the regulations issued under Article 21 of the Act of 27 July 2002 - Foreign Exchange Law. This mechanism is also available in respect of NPOs related information.

1199. According to the Article 15b of the AML/CFT Act in reasoned cases, the General Inspector may request the tax authorities or the fiscal control authorities to investigate the legality of origin of certain asset values. The information on the results of the activities conducted shall be submitted to the General Inspector without delay.

Responding to international requests regarding NPO-s – points of contacts and procedures (c.VIII.5)

1200. According to the AML/CFT law (the Article of 14, 15 and 15a) each cooperating units (i.e. public authority) is obligated to inform the GIFI on immediately notify the GIFI on any suspicion involving committing money laundering and/or terrorist financing. In turn, the GIFI can – on the grounds of the bilateral agreements on cooperation (memoranda of understanding) as well as the Council Decision no. 200/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information - exchange information with the foreign FIUs

1201. Moreover, the Internal Security Agency (ISA) and especially the Counter-Terrorist Centre located in the ISA are first of all responsible in Poland to recognize and combat the terrorism crimes. According to the Article 5 section 3 of the Act on the Internal Security Agency and the Intelligence Agency, the Head of the ISA is doing the tasks of the national contact point in the field of the information exchange mentioned in the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. Relevant in this regard is particularly the Article 16 of the Council Decision.

Effectiveness and efficiency

1202. Regarding the supervision provisions it is unclear whether the above mentioned control/supervisory bodies are sensitised with regard to the issues as set out in SR VIII and whether they take them into account in their controls/ audits.

1203. Noteworthy are the outreach attempts by GIFI to the NPO sector.

1204. It appears that - since Special Recommendation VIII was introduced - there has been no formal review of the adequacy of laws and regulations which relate to non-profit organisations that can be abused for the financing of terrorism as required by Criterion VIII.1. There are very limited measures in place to ensure that terrorist organisations cannot pose as legitimate non-profit organisations or those funds or the assets collected by or transferred through non-profit sector are not diverted to support the activities of terrorists or terrorist organisations, as required by Criteria VIII.2 and VIII.3. What there is in place does not appear to amount to effective implementation of Special Recommendation VIII.

5.3.2 Recommendations and comments

1205. It appears that no formal review of the adequacy of laws and regulations relating to entities which can be abused for the financing of terrorism has taken place, though the examiners noted that some steps have been taken, and as a result there are reporting structures and also steps to ensure enhanced financial transparency.

1206. The Polish authorities are first advised to undertake a formal analysis of threats posed by this sector as a whole and to identify its risks. Then they should review the existing system of relevant laws and regulations in order to assess the adequacy of the current legal framework with respect to criterion VIII.1.

1207. Consideration should also be given in such a review to the effective and proportional oversight of the NPO sector, the issuing of guidance to financial institutions on the specific risks of this sector and consideration of whether and how further measures need to be taken in the light of the Best Practices Paper for SR.VIII. In particular, programme verification and direct field audits should be considered in identified vulnerable parts of the NPO sector. Consideration might usefully be given as to whether and how any relevant private sector watchdogs could be utilised.

1208. It would be helpful also to raise awareness for SR.VIII among existing control bodies engaged with the NPO sector so that they also could fully take account of SR VIII issues in their oversight.

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	**PC**	• Limited review of the risks in the NPO sector has been undertaken; • 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 this sector.

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and co-ordination (R. 31 and R. 32)

6.1.1 Description and analysis

Recommendation 31 (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

1209. Poland was rated "Partially Compliant" in respect of Recommendation 31 based on the following deficiency – existing coordination measures are not completely effective.

Effective mechanisms in place for domestic cooperation and coordination in AML/CFT (c.31.1)

1210. In the view of the evaluation team, since the 3rd round evaluation, the Polish authorities continued to improve and strengthen cooperation between the main stakeholders as important part of the AML/CFT system.

1211. The legal basis for national cooperation in the area of AML/FT between relevant competent authorities is set out in the AML/CFT Act.

Policy mechanisms

1212. At the time of the 3rd round evaluation an intergovernmental Working Group was created to review gaps in the AML/CFT regime for the purpose of making changes to the AML/CFT legislation. The evaluators recommended that the Group should continue its work as intergovernmental coordinating body of the main players (the policy makers, the FIU, law enforcement, prosecutors and supervision) in the area of AML/CFT for the purpose of reviewing systematically and collectively ML and TF vulnerabilities, resolving interdisciplinary issues, periodically reviewing the performance of the system as a whole against some key strategic performance indicators and reviewing collectively, where appropriate, the available statistical information to better carry our each agency's task. During the 4th round on-site visit the evaluators were informed that after the new AML/CFT Act was finished the intergovernmental body ended its work. There is no legal basis for formal mechanism in place for domestic coordination in AML/CFT area and there is no such body that would coordinate activities in the area of AML/CFT. Nevertheless, the GIFI appears to be main stakeholder in the polish AML/CFT system.

1213. The fight against money laundering and terrorist financing is one of the Polish strategic priorities. It was reflected by the National Security Strategy of the Republic of Poland adopted in 2007.

> *"The state will oversee the stability and security of the domestic money market and the proper functioning of the banking system. Efforts will be made to enhance the monitoring of financial transactions and operational and investigative cooperation with Internal Security Agency, the Central Anti-Corruption Bureau, the Police, State Border, as well as – in the international dimension – with financial intelligence units of other countries, aimed primarily at preventing introduction into financial turnover of pecuniary values originating from illegal or undisclosed sources and counteracting financing terrorism. It is very important that we cooperate with those organisations which have as their goal counteracting money laundering*."

1214. The strategy of combating money laundering and terrorism financing adopted after the third round of the mutual evaluation by the Polish authorities involved actions in numerous key areas.

1215. In particular, the Polish authorities:

f. adopted measures to create and implement legal provisions in area of combating money laundering and terrorism financing,
g. facilitated the implementation of international AML/CFT standards,
h. created an effective inter-institutional cooperation,
i. participated in national, regional and international AML/CFT initiatives,
j. provided assistance to other countries in the area of AML/CFT.

1216. The specific crimes of money laundering and terrorism financing are among the priority areas identified by the National Program for Counteracting and Combating Organised Crime for the years 2012 – 2016 and National Program for Combating Terrorism for the years 2012 -2016. The Ministry of Internal Affairs, in cooperation with other relevant governmental institutions, among others the GIFI, has prepared two draft strategic documents. The main goal of the first one is to streamline the Polish system for counteracting and combating organised crime. The document also refers to the crime of money laundering as one of main symptoms of the activity of organised crime groups. The document was prepared with significant participation of the Ministry of Finance (especially the GIFI). It has been designed on the basis of "Diagnosis of organised crime in Poland" (document prepared last year by the Ministry of Interior with broad cooperation of other governmental bodies (including active participation of the GIFI). The second strategy – National Program for Combating Terrorism for the years 2012 -2016 – is dedicated to all issues connected with terrorism and its determinants.

1217. In addition to the abovementioned strategies, the Polish authorities prepare annually a report on Security Level in Poland on the basis of information from numerous law enforcement agencies supervised by the Ministry of Interior, as well as data from other sources (incl. the GIFI and the Customs). The report describes areas of risk, among others – money laundering. It is published on the Ministry of Interior website, in Polish.

1218. Cooperation is also an essential component of the Polish AML/CFT strategy. As a result of conducted analyses, the GIFI sends to the public prosecutor reports on justified suspicions of money laundering along with all financial information gathered in the course of analyses (including information protected by bank secrecy).

1219. Apart from reports on money laundering offences submitted to the Public Prosecutor's Office, the GIFI provides information on suspicious transactions to: fiscal control offices, the police, the Internal Security Agency (including the Counter -Terrorist Centre), Border Guards, the Central Anticorruption Bureau, tax authorities.

1220. It appears that there is some policy co-operation in Poland, as was mentioned above, the main stakeholders are involved in drafting strategies, sharing and providing necessary information, including statistics, discussing issues related to ML/FT. However it is not clear whether they have to meet on regular basis, also the evaluators came to the conclusion that there is no centralised coordinating body at a policy level in the area of AML/CFT.

Operational co-operation

1221. Cooperation between the FIU and cooperating units is set out, as described above, in Articles 14, 15, 32 and 33 of the AMLFT Act. Cooperating units are government and local government authorities and other public organizational units, as well as the National bank of Poland, the Polish Financial Supervision Authority and the Supreme Chamber of Control.

1222. On a practical level, the GIFI cooperates with law enforcement authorities, especially with the Public Prosecutors' Office and the Police. In the course of an ML/FT investigation the Police and the Public Prosecutors' Office co-operate closely with the GIFI. In fact, the GIFI is commonly relied upon by the Police to obtain additional information, whether such information is to be obtained from a reporting entity or from a foreign authority.

1223. The GIFI has managed to build the necessary trust with the law enforcement agencies and prosecutors. The law enforcement agencies refer to the GIFI as an effective channel for obtaining banking information of persons suspected of committing predicate offences and for freezing their accounts. Nevertheless, the GIFI is not approached systematically to detect suspicion of money laundering by entities unknown to law enforcement. The law enforcement agencies make little use of reports sent to them by the FIU regarding such suspicions.

Law enforcement authorities

1224. Co-operation and coordination between law enforcement authorities involved in the investigation of ML/FT are formalised in different agreements signed by various law enforcement authorities (see Annex 7).

1225. In order to facilitate cooperation in tracing and identifying crime-related assets, the Minister of Interior, the Minister of Finance and the General Prosecutor signed the Declaration of Cooperation of 18th December 2008. The parties undertook, within their powers, to work together in order to effectively carry out tasks of detection and identifying illegally obtained proceeds and other property derived from criminal activity. The parties have established authorised proxies for the implementation of the Declaration of Cooperation. Additionally, on 15 September 2009 an Agreement between the Minister of Interior, the Minister of Finance and the General Prosecutor has been signed. The Parties agreed to cooperate within the detection and identification of the proceeds of crime or other crime-related assets within the scope of tasks of the National Asset Recovery Office.

1226. Cooperation between of the GIFI and the National Asset Recovery Office is based on the following two pillars: information exchange concerning suspicious persons and other entities, as well as their assets, and working meetings between representatives of the ARO and the Polish FIU concerning important issues related to information exchange (e.g. ways, types and scopes of exchanged information); frequency of meetings depends on the appearance of issues which should be discussed – the last meeting was in November 2012.

1227. There are no separate statistics concerning exchange of information with domestic institutions. In 2012 ARO sent and received the total number of 1739 pieces of correspondence. We can estimate that 90% of them concerned exchange of information on crime related assets with both domestic and foreign institutions. The rest made a correspondence concerning administrative matters.

1228. For the purpose of combating terrorism 2 inter-ministerial bodies were created. Inter-Ministerial Committee of Financial Security which is a consultative and advisory board and performs tasks in relation to application of specific restrictive measures against persons, groups and entities acting under auspices of the General Inspector. Inter-ministerial Team for Terrorist Threats (hereinafter – Team) subsidiary body of the Cabinet was established on the basis of the Order no. 162 of the Prime Minister of 25 October 2006 and ensures cooperation of the governmental administration in the field of identifying, preventing and combating terrorism.

1229. The basic tasks of the Team include e.g.: monitoring of terrorist threats, presenting opinions and conclusions for the Cabinet, elaborating projects of standards and procedures in the field of combating terrorism, initiating and coordinating actions taken by competent authorities of the governmental administration, organising cooperation with other countries in the area of combating terrorism. During the on-site visit the evaluators were advised that a specific subcommittee for financing of terrorism will set up.

1230. The Inter-ministerial Team for Terrorist Threats meets at least once a month (usually with the Permanent Group of Experts) and the Permanent Group of Experts – at least three times a month (including once usually with the Team).

1231. In addition, the GIFI cooperates with the Counter-Terrorist Centre of Internal Security Agency. This co-operation in mainly focused on exchange of information in the scope of conducted FT cases and the general cooperation within the frame of the Inter-ministerial Team for Terrorist Threats and

the Permanent Group of Experts as for monitoring, analysis and assessment of terrorist threats and activities conducted by the governmental bodies in this field.

1232. Working meetings between representatives of the CTC and the Polish FIU are focused on important issues related to information exchange (e.g. channels of information exchange, types and scopes of information exchange); frequency of meetings depends on the appearance of issues which should be discussed – the last meeting was in November 2012.

Supervisory authorities

1233. As to co-operation between the GIFI and supervisory authorities pursuant Article 21 paragraph 1, the GIFI is responsible for monitoring financial institutions' compliance with the requirements under the AML/CFT Act. Paragraph 3 states that compliance monitoring of financial institutions may also be carried out by the PFSA, the NBP and the NSCCU within the legislative framework setting out the powers and functions of such supervisory authorities. Following such inspections the supervisory authorities submit information to the GIFI on the results of these inspections. In addition, a reference should be made to Section 3.10, which in detail describes the co-operation between the GIFI and the supervisory authorities.

1234. Cooperation between DNFBP supervisory authorities and the GIFI is impeded by the shortcomings identified in the regulation of supervisory bodies as described under Recommendation 24.

Additional element – Mechanisms for consultation between competent authorities and the financial sector and other sectors (including DNFBPS) (c. 31.2)

1235. Although there is no formal mechanism for consultation, regulation or other enforceable means for consultation between competent authorities and the financial sector and other sectors (including DNFBP) in place, the Polish authorities have confirmed that consultations between the competent authorities, the financial sector and other sectors (including DNFBP) has occurred whenever the need arises to exchange views and experiences or to solve any kind of problems with regard to the AML/CFT issues. So far the Polish authorities have held consultative meetings with the following representatives of obliged institution: notaries, foundations, Western Union, leasing, investment fund societies, banks, Polish Post. Those meetings concentrated on providing the FIU guidance which aimed at elimination of typical errors made by obliged institutions while providing information on transactions to the GIFI that are typical for the particular categories of obliged institutions.

1236. Moreover, the GIFI consults (via phone and e-mail) on daily basis all sectors of obliged institutions on on-going problems connected with the reporting obligation. No statistics are held, it is not clear which designated post/department deals with this kind of communication

Review of the effectiveness of the AML/CFT system on a regular basis (Recommendation 32.1)

1237. According to the Polish authorities, report covering 3 year period was drafted by the Department for Organised Crime and Corruption of the Office of the Prosecutor General. Such report describe effectiveness of ML investigations conducted in every Appellate Prosecution Office, review common problems identified and proposed some solutions. Reports were disseminated among all prosecution offices in Poland and also discussed during conferences.

1238. There is insufficient review of the effectiveness of the system for combating money laundering and terrorist financing on a regular basis. Some bodies carry out activities for the purpose of analysing their activities in the context of combating ML/FT. However, in order to identify problems of the system and to propose adequate solutions it is necessary to review system as a whole. This function could be established within a coordinating body in the area of AML/CFT so all main stakeholders could partake and contribute with their specific insight of the system.

Recommendation 30 (Policy makers – Resources, professional standards and training)

1239. All Polish policy makers: the FIU, law enforcement bodies, and supervisors appear to have adequate human and technical resources.

1240. The Staff of competent authorities appear to maintain high professional standards, including standards concerning confidentiality, are of high integrity and are formally skilled which is guaranteed by provisions of the sectoral laws prescribing legal conditions for employment.

1241. According to the Polish authorities, trainings are conducted on regular basis for all policy makers. Overall, it appears that statistics management on trainings lacks systematic approach.

Effectiveness and efficiency

1242. Further efforts should be pursued to ensure regular coordinated actions with regard to analysis of current trends for the purpose of reviewing systematically and collectively ML and TF vulnerabilities, resolving interdisciplinary issues, reviewing periodically the performance of the system as a whole against some key strategic performance indicators and reviewing collectively, where appropriate, the available statistical information to better carry out each agency's task.

6.1.2 Recommendations and Comments

Recommendation 31

1243. Central coordinating body in the area of combating ML/FT should be established in order to coordinate AML/CFT at policy level.

1244. More efficient mechanism for domestic cooperation and coordination should be established in order to enhance the effective utilisation of the GIFI information.

Review of the effectiveness of the AML/CFT systems on a regular basis (Recommendation 32.1)

1245. A mechanism for reviewing effectiveness of the AML/CFT systems on a regular basis should be established.

Recommendation 30 (Policy makers – Resources, professional standards and training)

1246. Further trainings should be organized that emphasise ML/FT issues.

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	**LC**	• There is no mechanism for facilitating a regular and joint review of the AML/CFT system and its effectiveness by competent authorities; • No central coordinating body at policy level in the area of AML/CFT.

6.2 The Conventions and United Nations Special Resolutions (R. 35 and SR.I)

6.2.1 Description and analysis

Recommendation 35 (rated PC in the 3rd round report) & Special Recommendation I (rated PC in the 3rd round report)

Summary of 2007 factors underlying the rating

1247. Poland was rated 'PC' for Recommendation 35 in the 3rd round mutual evaluation report based on the following deficiency:

- While Poland has ratified the relevant conventions, it has failed to effectively implement two of them or to make their non-self-executing provisions part of domestic law.

Ratification of AML Related UN Conventions (c. R.35.1 and of CFT Related UN Conventions (c. SR I.1)

1248. Poland has ratified the Vienna Convention, the Palermo Convention and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention). It has now, and since the 3rd evaluation, progressed towards fully implementing all three after the enactment of the TF offence. Article 87 of the Polish Constitution provides that ratified agreements are a source of binding law, unless the relevant provisions are not self-executing. Poland needs to incorporate the non-self-executing provisions of those conventions in its domestic law. Reservations have been expressed earlier also in respect of the coverage in domestic law of all the physical aspects of the money laundering offence.

Implementation of Vienna Convention (Articles 3-11, 15, 17 & 19, c. 35.1)

1249. Poland law complies with many provisions of the Vienna Convention (See Annex 4 for further information).

1250. The language in Article 299 of the Penal Code to date does not clearly replicate the language of the Convention and does not cover conversion or transfer for the purposes of concealing/disguising the proceeds' illicit origin. Also not covered is conversion or transfer of such property for the purpose of assisting any person who is involved in the commission of the offences established in accordance with Article 3 subparagraph a of the Convention. It is less clear whether concealment or disguise of the true nature, source, location disposition, etc. would be covered. Acquisition, possession or uses, which the 2006 evaluators found were missing elements, are still uncovered.

1251. Confiscation and seizing measures are available for all offenses under the Convention and the power of law enforcement agencies to identity and trace property that is or may become subject to confiscation is generally not hindered by financial secrecy.

1252. Poland may provide a number of different types of mutual legal assistance with respect to drug-related ML offenses.

Implementation of Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31 & 34, c.35.1)

1253. Poland law complies with many provisions of the Palermo Convention (See Annex 4 for further information).

1254. ML offence is not fully in line with the Article 6 of the Palermo Convention (subject to the shortcomings described under Section 2.1). Confiscation and seizing measures in relation to proceeds obtained through the offenses described by the Convention or property the value of which corresponds to that of such proceeds are available.

1255. The Poland may also provide a wide range of different types of mutual legal assistance with respect to ML offenses involving transnational organized crime. Assistance in searching or seizing for property or evidence in relation to such offenses may be granted.

1256. Preventive measures and supervisory regime are in place for banks and non-bank financial institutions. However, the legal framework setting out the various obligations is still subject to a number of shortcomings as discussed under section 3 of this report.

1257. Poland has established the GIFI and applied the EU's cross border declaration system.

Implementation of the Terrorist Financing Convention (Articles 2-18, c.35.1 & c. SR. I.1)

1258. Concerning the Terrorist Financing Convention, after enacting the TF offence in accordance with section 2.2 of the Convention it remains to examine if the preventive measures in Article 18 of the Convention, including full identification of beneficial owners and consideration of licensing of money or value transfer services (MVT) have been met.

1259. Poland law complies with many provisions of the TF Convention (See Annex 4 for further information).

Implementation of UNSCRs relating to Prevention and Suppression (c. SR.I.2)

1260. Poland has implemented UNSCR 1267 and UNSCR 1373 under European Union legislation (subject to the shortcomings described under Section 2.4) (See Annex 5). With respect to UNSCR 1373, Poland has provided the United Nations' Counter-Terrorism Executive Directorate (CTED) with five periodical reports describing its implementation efforts. United Nations' Resolutions 1267 and 1373 (in respect of Non-European Union citizens) are legally implemented through European Union mechanisms. These lists are circulated to the obligated entities. With the enactment of section 5a of the AML/CFT Act a clear legal mechanism, which would cover designations in Poland in respect of European Union citizens or named persons not covered by the European Union clearing house list proposed by other countries, now exits but still needs to be implemented. The US lists were automatically circulated. It appeared the obligated institutions sporadically check against the lists, but no terrorist accounts had been identified. Supervisors should check compliance with this obligation.

Additional element – Ratification or Implementation of other relevant international conventions

1261. The 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS 141) was signed by Poland in November 1998, ratified on 20 December 2000, and came into force on 1 April 2001. Poland has signed in May 2005 and ratified in 2007 (entered into force in 1st of May 2008) the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the financing of Terrorism (CETS No 198).

6.2.2 Recommendations and comments

1262. Poland has ratified the Vienna and Palermo Conventions and the Terrorist Financing Convention. Since the last round of MONEYVAL evaluations, the domestic legislation has been amended, however, the existing legislation does not fully cover requirements under Recommendations 1 and 3 and Special Recommendation II. Therefore, it is recommended that Poland should take necessary measures to remedy identified deficiencies under Recommendations 1 and 3 and Special Recommendation II to fully implement the Vienna, Palermo and TF Conventions.

1263. In addition, the Polish authorities should also take steps to address the deficiencies identified under SR.III to fully implement the requirements of the UNSCRs, in particular implement the mechanism set out in Chapter 5a of the AML/CFT Act.

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	**PC**	*Vienna and Palermo Conventions* • The physical elements of money laundering offence do not fully correspond to the Vienna and Palermo Conventions, in particular conversion, concealment, disguise, acquisition, possession or use are not covered in all circumstances (R.1); • Not all essential criteria are provided for in the Polish legislation, e.g. association with or conspiracy as an ancillary offence (R.1); • The confiscation of instrumentalities is discretionary (R.3); • Confiscation regime does not cover instrumentalities transferred to third parties (R.3); *Convention for the Suppression of the Financing of Terrorism* • Funding terrorist organisation for "any purpose" not fully criminalised (SR.II); • The funding of an individual terrorist is not criminalised in all circumstances (SR.II); • Terrorist Financing abroad is not fully covered (SR.II); • There are purposive supplementary elements for some of the acts constituting offences in the treaties annexed of the Convention (SR.II); • Limited scope of terrorist financing offence potentially affects the scope of confiscation and provisional measures especially with regard to "legal" activities of terrorist organisations and individual terrorists (R.3).
SR.I	**PC**	*Convention for the Suppression of the Financing of Terrorism* • Funding terrorist organisation for "any purpose" not fully criminalised (SR.II); • The funding of an individual terrorist is not criminalised in all circumstances (SR.II); • Terrorist Financing abroad is not fully covered (SR.II); • There are purposive supplementary elements for some of the acts constituting offences in the treaties annexed of the Convention (SR.II); • Deficiencies under SR.III.

6.3 Mutual legal assistance (R. 36, SR. V)

6.3.1 Description and analysis

Recommendation 36 (rated LC in the 3rd round report)

Summary of 2007 factors underlying the rating

1264. Recommendation 36 in the 3rd round MER of Poland was rated LC based on the following factor:

- Though Poland can provide a wide range of mutual legal assistance the lack of statistics means there is a reserve on effectiveness.

Legal framework

1265. The legal framework for international judicial co-operation in criminal matters is addressed in the Criminal Procedure Code, Part XII "*Procedure in criminal cases in international relations*".

1266. Mutual legal assistance in criminal cases is addressed in the provisions of Chapter 62 of this part of the Code of Criminal Procedure "*Judicial assistance and service of documents in criminal cases"*, which provides for the activities of criminal proceedings amenable to be taken in the course of legal assistance, the conditions and modalities of their execution.

1267. The execution of the orders on retention of evidence and to secure the property which imply the cooperation with an EU Member State is regulated by the Chapters 62a and 62b of the Code of Criminal Procedure.

1268. In addition, mutual legal assistance may also be afforded under the self-executing provisions of certain conventions and treaties:

- European Convention on mutual assistance in criminal matters of 20 April 1959 (CETS 30),
- Additional Protocol to the European Convention on mutual assistance in criminal matters of 17 March 1978 (CETS 099),
- Second Additional Protocol to the European Convention on mutual assistance in criminal matters of 8 November 2001 (CETS 182),
- The Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000,
- Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 16 October 2001,
- the Convention implementing the Schengen Agreement 1990.

Widest possible range of mutual assistance (c.36.1)

1269. Poland is able to provide a wide range of mutual legal assistance in AML/CFT investigations, prosecutions and related proceedings, including assistance in the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons; the taking of evidence or statements from persons; providing originals or copies of relevant documents and records as well as any other information and evidentiary items, effecting service of judicial documents; facilitating the voluntary appearance of persons for the purpose of providing information or testimony to the requesting country and identification, freezing, seizure, or confiscation of assets laundered or intended to be laundered, the proceeds of ML and assets

used for or intended to be used for FT, as well as the instrumentalities of such offences, and assets of corresponding value.

1270. Almost every type of action permissible under international and domestic law can be sought, apart from cross-border observations, videoconferencing the suspect or the accused and temporary transfer of a detained person without consent (information provided through official site of the European Judicial Network). But these actions are not listed in Essential criteria 36.1.

1271. The provisions on mutual legal assistance are addressed in Article 588 of the Criminal Procedure Code which established that courts and public prosecutors shall provide legal assistance upon a request of courts and public prosecutors of foreign countries. Section Two directs that courts and prosecutors shall refuse assistance if the requested action conflicts with "the legal order" of Poland or constitutes "an infringement of its sovereignty." Section Three provides three circumstances under which assistance may be denied, including the lack of reciprocity or dual criminality. However, the evaluators were assured that this discretionary provision was rarely applied in practice.

1272. Where a Mutual Legal Assistance Treaty (MLAT) or other information-sharing agreement exists, mutual legal assistance can be rendered directly by the relevant agency. With respect to EU partners, there is typically direct contact between judicial authorities. In the absence of such an agreement, the request is received by the Ministry of Foreign Affairs and is directed to the appropriate ministry. The powers of competent authorities required under Recommendation 28 are generally available for use in response to requests for mutual legal assistance.

Provision of assistance in timely, constructive and effective manner (c. 36.1.1)

1273. With respect to the issue of timely execution, there are no provisions authorising prosecutors to give such requests priority over domestic cases. Nevertheless, requests for mutual legal assistance are given the same priority as domestic cases. An Ordinance of Minister of Justice of 24 March 2010 is in force, which sets forth rules of internal office activities of the entities of public prosecutor's office including affording MLA. Pursuant to § 284 of the Ordinance of 24.03.2010, incoming MLA requests are dealt with by the Appellate Prosecution Offices, Regional Prosecution Offices and District Prosecution Offices acting under supervision of Regional Prosecution Offices.

1274. A special unit in the Prosecutor General's Office, the Department of International Co-operation, is primarily responsible for timely and constructive assistance, along with the Ministry of Foreign Affairs and the Ministry of Justice.

1275. The Polish authorities insist that the requests for mutual legal assistance are given the same priority as domestic cases. Moreover, under Paragraph 4 (1) of the "Regulation of the Ministry of Justice of 28 January 2002 concerning the detailed courts activities in cases of international civil and criminal proceedings in international relations" the courts are obligated to give priority in the area of international legal cooperation.

Provision of assistance not prohibited or made subject to unreasonable conditions (c.36.2)

1276. Article 588 of the Criminal Procedure Code, as mentioned above, sets out the grounds for refusal of a legal assistance request which could not be deemed as unreasonable conditions.

Clear and efficient processes (c. 36.3)

1277. Overall, the existence of the Department of International Co-operation within the Prosecutor General's Office seems to warrant an efficient process for dealing with and executing MLA requests in a timely way and without undue delays.

Provision of assistance regardless of possible involvement of fiscal matters (c. 36.4)

1278. A request for assistance is not refused on the sole ground that the offence is also considered to involve fiscal matters.

Provision of assistance regardless of existence of secrecy and confidentiality laws (c. 36.5)

1279. In the course of execution of foreign requests issues of secrecy or confidentiality do not present obstacles. Pursuant to Article 105 § 1 subsection 2) let. c) of the Banking Law, banking secrecy can be lifted on a motion filed by prosecution authorities or courts executing foreign requests for legal assistance, provided that a ratified international agreement binding on the Republic of Poland concerning legal assistance is in place.

1280. According to article 588 § 4 of the Code of Criminal Procedure (CPC), Polish law shall be applied to the procedural actions performed pursuant to a request from a foreign court or state prosecutor. If a MLA request contains demands as to obtain evidence covered with secrecy or confidentiality requirements, a prosecutor in charge will apply provisions on lifting secrecy foreseen in article 105 § 1 item 2b) and 2c) of the Banking Act or in article 149 item 2) of the Act of 29 July 2005 on trading in financial instruments.

Availability of powers of competent authorities (applying R.28, c. 36.6)

1281. All the powers linked with criminal investigation, required under R.28 are available for use in response to requests for mutual legal assistance. As stated above according to article 588 § 4 of the CPC, Polish law shall be applied to the procedural actions performed pursuant to a request from a foreign court or state prosecutor.

Avoiding conflicts of jurisdiction (c. 36.7)

1282. In order to avoid conflicts of jurisdiction, in selected cases, Poland has reportedly considered devising and applying mechanisms for determining the best venue for prosecutions in cases that are subject to prosecution in more than one country. Though they are not party to the European Convention on the Transfer of Proceedings in Criminal Matters (ETS 73), the Polish authorities indicated that they had bilateral agreements with several countries regarding the transfer of proceedings on the basis of best venue (e.g. Russian Federation and Latvia). By virtue of Council Decision of 28 February 2002 establishing EUROJUST, Poland can request EUROJUST to arbitrate on issues of best venue between European Union states.

Additional element – Availability of powers of competent authorities required under R. 28 (c. 36.8)

1283. The powers required under R.28 are also available in case of direct communication between foreign and domestic judicial authorities. Pursuant to Article 588. § 1of the CPC, courts and state prosecutors offices shall give judicial assistance when requested by letters rogatory, issued by the courts and the state prosecutors' offices of foreign states. If there should be exercised powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence, than articles 217-220 of the CPC are applied..

Special Recommendation V (rated PC in the 3rd round report, applying 36.1 – 36.6 in R.36, c.V.1)

1284. The analysis under Recommendation 36 applies equally to ML and TF conduct.

Additional element under SR V (applying c. 36.7 & 36.8 in R. 36, c.V.6)

1285. The analysis under Recommendation 36 applies equally to ML and TF conduct.

Recommendation 32 (Statistics – c. 32.2)

1286. The Prosecutors' General Office maintains statistics concerning the number of requests for legal assistance sent from Poland and received by Poland. On the basis of an order issued by The Deputy Prosecutor General on 10 July 2010, Appellate Prosecutors are obligated to submit precise and complex information on money laundering investigations conducted by the subordinated prosecutors.

1287. From 2009 to 2011 only requests for MLA were submitted by foreign prosecutors. In the same period of time all the request (incoming and outgoing) were granted by Polish/foreign law enforcement authorities in ML cases.

Table 32: Number of MLA requests

	2009	2010	2011
MLA requests made in ML cases	130	104	115
MLA requests received ML cases	1	1	7

1288. Out of all outgoing MLA requests only one (filed to Switzerland in 2009) referred to seizure of property. Also only one incoming MLA request (submitted by Dutch authorities in 2010) concerned seizure of property on the territory of Poland.

1289. The underlying predicate offences related to requests for MLA filed by the Polish prosecution service in 2009-2011 were as follows:

Art. 231 § 1 PC (abuse of power by a public official)

Art. 258 § 1 and 3 PC (participation in or leading a criminal group)

Art.271 § 1 and 3 PC - (intellectual forgery)

Art.278 § 1 PC (theft)

Art.284 § 1 and 2 PC (appropriation of goods)

Art. 286 § 1 PC (fraud)

Art.287 § 1 PC (phishing attack)

Art. 296 § 1 PC (causing damages in business transactions)

Art 54 § 1 of the Fiscal Penal Code (tax evasion)

Art. 56 § 1 of the Fiscal Penal Code (tax fraud)

Art.63 § 1 of the Fiscal Criminal Code (illegal import of goods subject to excise)

Art. 305 § 1 of the Law on Industrial Property (labeling goods with counterfeited trade marks)

1290. Average time of execution of the MLA request by the Polish authorities was between 30 days and 3 months. Average time of execution of the Polish MLA request by foreign authorities was between 1,5 and 6 months.

1291. Turning to criteria V.6, to the extent such records are kept, there is no reason to believe that mutual legal requests would be treated or applied differently under the obligations of SR. V, now that terrorist financing is an autonomous offence in Poland. Nevertheless the shortcomings in the TF offence definition may lead to the lack of dual criminality which is one of the discretionary bases for denying mutual legal assistance. The evaluators were assured that denial of assistance for such reasons occurs rarely, if ever.

Effectiveness and efficiency

1292. During the onsite visit the evaluators were informed by the Polish authorities that the average time to execute a MLA request is 30 days but there were not provided relevant statistics.

1293. The Polish authorities have confirmed during the onsite meetings that, as a consequence of deficiencies related to Recommendation 3, the instrumentalities cannot be seized and confiscated on the basis of MLA requests.

1294. The lack of the specific statistics makes impossible to assess the effectiveness and efficiency of the competent authorities related to MLA in ML and TF cases.

6.3.2 Recommendations and comments

Recommendation 36

1295. Poland can provide a wide range of mutual legal assistance and co-operation. Statistics provided in respect of mutual legal assistance relating to money laundering and terrorist financing offences show an extremely low number of incoming requests which may be indicative as to a systemic problem though the evaluators cannot comment on either the effectiveness of current provisions or the timeliness of the provision of mutual legal assistance in such a small number of cases.

1296. In addition, no statistics were provided regarding MLA regarding offences other than ML or TF leaving the evaluators unable to comment on either the effectiveness of current provisions or the timeliness of the provision of mutual legal assistance in such cases.

1297. The fact that terrorist financing is not fully covered in Polish legislation may potentially be problematic to the provision of mutual legal assistance, although the Polish authorities assured the evaluators that dual criminality would be very widely interpreted in these cases. The fact remains that this has not been tested.

1298. Additional concern with regard to effectiveness is the fact that there has been no practice with MLA with regard to foreign confiscation requests.

6.3.3 Compliance with Recommendation 36 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3. underlying overall rating
R.36	**C**	
SR.V	**LC**	• 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.

6.4 Other Forms of International Co-operation (R. 40 and SR.V)

6.4.1 Description and analysis

Recommendation 40 (rated LC in the 3rd round report)

Summary of 2007 factors underlying the rating

1299. In the third round MER Poland was rated 'Largely Compliant' based on the following factor:

- Broad capacity for exchange by the FIU and supervisory bodies but no data on information exchange between supervisory bodies.

Legal framework

1300. The legal basis for co-operation between GIFI and foreign authorities is set out in Article 33 § 5 of the AML/CFT Act.

Wide range of international co-operation (c.40.1); Provision of assistance in timely, constructive and effective manner (c.40.1.1); Clear and effective gateways for exchange of information (c.40.2), Spontaneous exchange of information (c. 40.3)

FIU

1301. Pursuant to Article 33 paragraph 5 of the Act the GIFI empowered to disclose information related to asset values originated from ML and FT to its foreign counterparts on a reciprocal basis, in the manner specified in bilateral agreements concluded by the General Inspector and also by computerised data storage carriers.

1302. As could be seen from Article 33 paragraph 5, the GIFI has legal provision to respond to foreign FIUs. Article 33 paragraph 3 specifically allows the GIFI to disseminate information to domestic authorities on its own initiative, however, the AML/CFT Act is silent whether the GIFI can send spontaneous requests to foreign FIUs. According to the GIFI annual report of 2011, 171 requests were sent to foreign FIUs, the statistics clearly show that in practice the GIFI sends requests to foreign FIUs.

1303. In terms of Article 33 paragraph 3, it should be noted that the GIFI can only exchange information related ML and FT and not the information in relation to underlying predicate offences.

1304. According to Article 33 paragraph 3 the General Inspector can conclude bilateral agreements. As a result of this power the General Inspector signed 63 MoUs (See Annex 8) and is negotiating an additional twenty.

1305. In addition to provisions of the AML/CFT Act, the EU Council Decision 2000/642/JHA concerning arrangements for co-operation between financial intelligence units of the Member States in respect of exchanging information could also be used as a way of international co-operation and information exchange.

1306. As was mentioned under Recommendation 26, the GIFI became a member of the Egmont Group in June 2002. The evaluators were informed that the GIFI exchanges information mainly via Egmont Secure Web and FIU.NET.

1307. The average response time for requests of information made by foreign counterparts since 2007 is 3 weeks and in urgent cases (especially those related to reports on suspicious transactions sent under Article 16 (1) of the Act [*i.e. ex-ante reporting*] the response does not usually exceed 2-3 days.

1308. As noted under the analysis of Recommendation 26, AML/CFT Act grants a wide-ranging power to the GIFI to request and receive information necessary for the proper exercise of its powers from public authorities, enterprises, institutions, organisations and reporting entities, including for the

purpose of exchanging information with foreign FIUs. It was also noted that the GIFI has direct access to various databases which facilitates the timely, constructive and effective collection of information to be exchanged with other FIUs.

Supervisory authorities

1309. The Polish supervisory authorities can cooperate and exchange information with foreign financial supervisors according to the provisions set out in sectoral laws. In particular, the PFSA can exchange information with foreign regulatory authorities according to Article 78 of the Act on Financial Market Supervision, Articles 141e and 141f of the Banking Act. It should be noted that the NBP only supervises foreign exchange offices.

1310. Currently the PFSA has signed 49 MoUs with other jurisdictions to facilitate exchange of information. Furthermore the PFSA is a party to 2 MoUs (the IOSCO MoU and CESR MoU) and 15 collegial agreements which were concluded to facilitate supervision over some of the financial groups operating in the territory of Poland. The agreements provide for spontaneous exchange of information and also exchange of information upon request, including the information concerning banking secrecy.

Law enforcement authorities

1311. The Act on exchange of information with law enforcement authorities of the Member States of the European Union defines the terms and conditions for the exchange of information with law enforcement authorities of the Member States of the European Union in order to detect and prosecute perpetrators of criminal offences or fiscal offences, to prevent and combat crime, to process information, as well as entities authorised in these matters.

1312. The following entities are authorised to exchange information with law enforcement authorities of the Member States of the European Union in order to detect and prosecute perpetrators of criminal offences or fiscal offences, to prevent and combat crime, as well as to process information: Internal Security Agency, Central Anti-Corruption Bureau, Police, Customs Service, Board Guard, tax inspection authorities and Military Police.

1313. Furthermore, the provisions of the mentioned Act apply to the exchange of information by the national Asset Recovery Office referred to in Article 1 Paragraph 1 of the Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime (OJ L 332, 18.12.2007, p. 103). The entities authorised to exchange information through the national Asset Recovery Office are entities mentioned above, as well as: the minister competent for public finances, General Inspector of Financial Information, tax chambers and offices and prosecutors.

1314. The Head of the Internal Security Agency performs as a contact point for the exchange of information, which is referred to in article 16. paragraph 3 of the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up cross-border cooperation, particularly in combating terrorism and cross-border crime (EU Journal of Laws No. L 210 of 6 August 2008).

1315. The cooperation with CARIN and other international networks of experts is on the basis and within the framework of existing legislation and international agreements. The Act of the 16th of September 2011 on the information exchange with law enforcement authorities came into force on the 1st of January 2012. It implements i.a. the *Council* Framework *Decision 2006/960*/JHA of 18 December 2006 and the *Council Decision 2007/845*/JHA of 6 December 2007 and the basis for information exchange, including that on the profits from crime and criminal assets, quickly and efficiently. It indicates contact points responsible for international information exchange as well as entities/subjects/institution authorized to exchange information and at the same time obliged to cooperate in implementation of foreign requests.

1316. The Polish ARO is in a position to provide a reply for urgent requests within the 8 hour period of time provided for by Framework Decision 2006/960/JHA. Such replies are prepared on the basis of information obtained from directly-accessible databases.

1317. According to the Polish authorities, the Police cooperate with its foreign counterpart through liaison officers, Europol and Interpol and are able to provide rapid assistance, if necessary.

1318. The Central Anti-Corruption Bureau (CBA) deals with the implementation of international commitments, according to the UN Convention against corruption, the UN Convention against transnational organised crime and others. The CBA exchanges information using bilateral agreement with State-Parties, multilateral agreements and the liaison officers' information exchange channel. It provides assistance without undue delay. The above-mentioned channels of international cooperation allow the CBA to request information on its own initiative (spontaneously), as well as upon the request of a requesting State-Party, in the field of ML and predicate offences.

1319. The Internal Security Agency is authorised to prepare and conduct negotiations on bilateral agreements on mutual protection of classified information, which regulate principles of handling classified information in Poland's relationship with other countries. The Internal Security Agency cooperates with intelligence and security services from other countries. The cooperation takes the form of information exchange, joint expert meetings, conferences as well as consultations and specialised training

Making inquiries on behalf of foreign counterparts (c.40.4), FIU authorised to make inquiries on behalf of foreign counterparts (c. 40.4.1), Conducting of investigation on behalf of foreign counterparts (c. 40.5)

FIU

1320. Upon the request of foreign FIUs, the GIFI is able to search its internal database as well as accessible external databases. In line with the AML/CFT Act it may also request information from obligated entities and cooperating units about the transactions covered by the AML/CFT Art.

Supervisory authorities

1321. There is no restriction in Polish legal framework which prohibits any search of information by the PFSA on the request of a foreign counterpart, and no limitation in the powers of PFSA in this scope in any other way.

Law enforcement authorities

1322. The Polish law enforcement authorities are entitled to co-operate with their foreign counterparts and, if necessary, they can conduct investigation on behalf of them.

1323. The CBA has not conducted any investigations on behalf of a foreign counterpart. However, it can provide MLA related to various international conventions and agreements.

1324. The Head of the CBA, on the basis of Article 2.2 of the Law on the CBA, can cooperate with relevant bodies and services of other countries and with international organisations, after obtaining approval from the Prime Minister.

No unreasonable or unduly restrictive conditions on exchange of information (c.40.6)

FIU

1325. As supported by the positive feedback received by the evaluators from MONEYVAL members, it appears that the exchange of information is not subject to any unreasonable or unduly restrictive conditions for the FIU.

Law enforcement authorities

1326. According to the representatives of the Police, exchange of information is conducted in the most rapid and efficient way possible.

1327. The Central Anti-corruption Bureau (CBA) provides for international cooperation in accordance with international rules on cooperation and on the basis of reciprocity referred to a number of conventions and international agreements.

Supervisory authorities

1328. The Polish authorities informed the evaluation team that there were no requests sent to or received from foreign supervisory authorities in this respect the cannot assess whether the exchange of information is subject to any unreasonable or unduly restrictive conditions for the supervisory authorities.

Provision of assistance regardless of possible involvement of fiscal matters (c.40.7)

FIU and law enforcement authorities

1329. According to the Polish authorities, both the CAB and the GIFI have not refused assistance on the grounds of possible involvement of fiscal matters.

Provision of assistance regardless of existence of secrecy and confidentiality laws (c.40.8)

1330. The AML/CFT Act contains specific provision that deals with secrecy and confidentiality issues. Pursuant to Article 21 in order to disclose any information in the manner and extent provided by the Act to the General Inspector, the regulations restricting the disclosure of confidential information shall not apply.

Safeguards in use of exchanged information (c.40.9)

FIU

1331. Article 30a of the AML/CFT requires the General Inspector and the staff of the Department of Financial Information to maintain confidential any information which came in their possession pursuant to the performance of their duties, in accordance with the principles and procedures specified in separate regulations.

Law enforcement authorities

1332. Law enforcement authorities provide protection of classified and non-classified information on the basis of sectoral specific laws, in particular the Law on Police, the Law on protection of classified information (Dz.U.2010.182.1228), and the Law on personal data protection (Dz.U.2002.101.926).

Additional elements – Exchange of information with non-counterparts (c.40.10 and c.40.40.1); Exchange of information to FIU by other competent authorities pursuant to request from foreign FIU (c.40.11)

FIU and law enforcement authorities

1333. It is not clear whether the GIFI can exchange information with non-counterparts since the AML/CFT Act refers to foreign institutions and international organisations involved in AML/CFT.

1334. However, as was noted above the Polish authorities are obligated to exchange of information with foreign counterparts on the basis of international law, national financial authorities. Therefore, it appears that there are no legal obstacles to obtaining the necessary financial information from other competent authorities on behalf of foreign counterpart authorities.

International co-operation under SR.V (applying 40.1-40.9 in R.40, c.V.5) (rated PC in the 3rd round report)

1335. The provisions prescribed under R.40 apply equally to the fight against financing of terrorism. It should be noted, however, that the deficiencies described under SR.II and R.40 may have an impact on Poland's ability to provide other forms of international co-operation.

Additional element under SR.V – (applying 40.10-40.11 in R.40, c.V.9)

1336. The analysis for Recommendation 40 also applies to cooperation in relation to the financing of terrorism.

Recommendation 32 (Statistics – other requests made or received by the FIU, spontaneous referrals, requests made or received by supervisors)

Table 33: Table on information which GIFI has exchanged with its foreign counterparts:

	No. of received requests	Entities referred	Countries[42]	No. of sent requests	Entities referred	Countries[43]
2007	111	460	GB, Ukraine, Belgium	175	308	USA, Germany, GB
2008	95	282	Ukraine, Luxemburg, Belgium	143	255	Germany, USA, Ukraine
2009	96	507	GB, Ukraine, Belgium	175	308	USA, Germany, GB
2010	102	411	Belgium, Luxemburg, Latvia	118	244	Germany, GB, Cyprus
2011	191	820	Luxemburg, Belgium, Slovakia	171	529	GB, Cyprus, Latvia

1337. Table 33 clearly shows that the GIFI co-operates quite actively with its foreign counterparts, which is very welcome. The main counterparts are Germany, the US, Cyprus, Luxemburg.

1338. With respect to statistics on information exchange with foreign counterparts by law enforcement authorities, the Polish authorities provided some statistics to the evaluation team, in particular, the statistical data on international information exchange is run by the International Police Cooperation Bureau (BMWP), which uses the electronic system of correspondence named STBS.

1339. The amount of correspondence received by BMWP (information exchange + international search) is the following:

2009 – 291.294 (Interpol-24%, Europol-1,3%, SIRENE-23%),
2010 – 264.514 (Interpol-23%, Europol-1,2%, SIRENE-20%),
2011 – 302.868 (Interpol-22%, Europol-1,8%, SIRENE-25%),
2012 – 271.632 (Interpol-22%, Europol-2%, SIRENE-27%).

1340. The evaluators, however noted that the provided statistics is too general and does not describe the whole picture of international cooperation carried out by law enforcement, particularly it does show how many requests were sent and received, how many responses were received and sent.

[42]Countries from which most request for the GIFI come from
[43] Countries to which the GIFI sent most of its requests

1341. Pursuant to information provided by Polish financial supervisors did not send or receive any formal request for assistance relating to or including AML/CFT in the period of 2007-2012.

Table 34: Number of international requests by the ARO

Polish ARO	2009	2010	2011	2012
incoming requests	21	20	25	64
outcoming requests	10*	26*	46*	61*
number of people in request	157	87	269	663
number of companies in request	61	43	119	252

**some of the requests were addressed to several countries at the same time, but are counted as one request for statistical purposes.*

Effectiveness and efficiency

FIU and law enforcement authorities

1342. In the 3rd Round MER confirmed non-existence of statistics on information exchanged with foreign counterparts. During the 4th Round on-site visit, apart from the GIFI, other law enforcement bodies did not present detailed statistics on the information exchanged with foreign counterparts.

6.4.2 Recommendation and comments

Law enforcement authorities

1343. Law enforcement authorities should keep detailed statistics on the exchange of information with foreign counterparts. It is recommended that procedures are set out in place to centrally record and monitor all international cooperation requests on matters related to ML and TF.

6.4.3 Compliance with Recommendation 40 and SR.V

	Rating	Summary of factors relevant to s.6.5 underlying overall rating
R.40	**LC**	**Effectiveness:** • Effectiveness issues regarding law enforcement authorities.
SR.V	**LC**	• Deficiencies under SR.II have a negative impact; **Effectiveness:** • Effectiveness issues regarding law enforcement authorities.

7. OTHER ISSUES

7.1 Resources and Statistics (R.30 and R.32)

1344. The text of the description, analysis and recommendations for improvement that relate to Recommendations 30 and 32 is contained in all the relevant sections of the report i.e. all of section 2, parts of sections 3 and 4, and in section 6. There is a single rating for each of these Recommendations, even though the Recommendations are addressed in several sections. Section 7.1 of the report contains only the box showing the ratings and the factors underlying the rating.

	Rating	Summary of factors underlying rating
R.30	**PC**	• The Analytical Units of the Department of Financial Information appear to be understaffed; • High fluctuation of experienced and specially skilled Police staff; • Concern over training in relation to conducting modern financial investigations by all LEAs involved in combating ML/TF, not only Police; • Insufficient number of AML/CFT inspectors within the Control Unit of the GIFI and the PFSA.
R.32	**LC**	• Lack of detailed statistics kept by LEAs; • No statistics on confiscation of proceeds of crime which are not ML or TF related; • Insufficient review of effectiveness of the AML/CFT systems on regular basis; • Lack of detailed statistics on information exchanged between domestic law enforcement bodies and their foreign counterparts.

7.2 Other Relevant AML/CFT Measures or Issues

1345. N/A

7.3 General Framework for AML/CFT System (see also section 1.1)

1346. N/A

IV. TABLES

8. TABLE 1. RATINGS OF COMPLIANCE WITH FATF RECOMMENDATIONS

The rating of compliance vis-à-vis the FATF 40+ 9 Recommendations is made according to the four levels of compliance mentioned in the AML/CFT assessment Methodology 2004 (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC)), or could, in exceptional cases, be marked as not applicable (N/A).

The following table sets out the ratings of Compliance with FATF Recommendations which apply to Poland. *It includes ratings for FATF Recommendations from the 3rd round evaluation report that were not considered during the 4th assessment visit. These ratings are set out in italics and shaded.*

Forty Recommendations	Rating	Summary of factors underlying rating[44]
Legal systems		
1. Money laundering offence	**PC**	• The physical elements of money laundering offence do not fully correspond to the Vienna and Palermo Conventions; in particular conversion, concealment, disguise, acquisition, possession or use are not covered in all circumstances; • Not all essential criteria are provided for in the Polish legislation, e.g. association with or conspiracy as an ancillary offence; • Shortcomings in the definition of TF as a predicate offence; **Effectiveness** • The overall effectiveness of ML criminalisation raises concerns considering a low number of convictions for ML, given a high level of proceeds generating offences in Poland; • The perception among practitioners with regard to high evidentiary standards for some of elements of the ML offence, e.g. mental element, has a negative impact on effectiveness.
2. Money laundering offence Mental element and corporate liability	*Largely Compliant*	• *It is unclear whether the intentional element can be inferred from objective facts and circumstances;* • *The provision on criminal liability of legal persons has not been applied yet.*
3. Confiscation and provisional measures	**PC**	• The confiscation of instrumentalities is discretionary; • Confiscation regime does not cover

[44] These factors are only required to be set out when the rating is less than Compliant.

		instrumentalities transferred to third parties; • Limited scope of terrorist financing offence potentially affects the scope of confiscation and provisional measures especially with regard to "legal" activities of terrorist organisations and individual terrorists; **Effectiveness:** • Low effectiveness - relatively small amounts confiscated especially when compared with amounts provisionally held, and with the size of the economy and estimated crime; • Law enforcement experience difficulty in detecting criminal property and determining beneficial ownership in legal persons; • Lack of statistics on overall confiscations meant that it was not possible to assess effectiveness as to confiscation in cases other than ML.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	**LC**	• No specific provision on third parties reliance to allow financial institutions to obtain necessary information on their customers.
5. Customer due diligence	**PC**	• The legislation does not cover full CDD requirements when carrying out occasional transactions that are wire transfers equal to or exceeding €1,000;[45] • Financial institutions are required to verify the customer identity on the basis of documents and information from a public source, but not specifically from reliable and independent sources; • There is no clear requirement to identify the beneficial owner, since financial institutions are only required to attempt to identify the beneficial owner; • There is no requirement to verify whether any person purporting to act on behalf of a legal person is so authorised; • When conducting on-going due diligence on the business relationship there is no requirement to establish, where necessary, the source of funds; • The provisions dealing with simplified CDD permit financial institutions to waive all CDD measures, except for on-going monitoring; • There is no prohibition against applying simplified

[45] The obligation to carry out full CDD only applies to wire transfers exceeding 15,000 EUR.

		CDD when there is a suspicion of ML/FT; • There is no requirement to complete verification of identity as soon as reasonably practicable in those cases where verification is not carried out before the establishment of a business relationship; • Article 9b permits financial institutions to open an account without performing full CDD; **Effectiveness:** • Some financial institutions met on-site maintain a business relationship despite the fact that the ultimate beneficial owner is unknown.
6. Politically exposed persons	**LC**	• The PEP definition does not cover important political party officials or persons entrusted with a prominent public function by a foreign jurisdiction who are resident in Poland; • No requirement to apply enhanced CDD if the beneficial owner is a PEP; • No specific requirement to obtain senior management approval to continue a business relationship where the customer subsequently is found to be or becomes PEP; • There is no requirement to conduct enhanced on-going monitoring on the entire business relationship with a PEP.
7. Correspondent banking	**LC**	• The requirements regarding correspondent banking relationships are limited to respondent institutions located in a state not imposing equivalent AML/CFT obligations; • No requirement to establish the reputation of the respondent and to determine whether it has been subject to a ML/FT investigation or regulatory action; • No requirement to ascertain that the AML/CFT measures implemented by a respondent institution are adequate and effective.
8. New technologies and non face-to-face business	**PC**	• No requirement to have policies and procedures in place to prevent the misuse of technological developments in ML/FT schemes; • No requirement to have policies and procedures to address the specific risks associated with non face-to-face business relationships when conducting on-going due diligence.
9. Third parties and introducers	**PC**	• Partial requirement to immediately obtain from a third party the necessary information concerning certain elements of the CDD process; • Partial requirement to take adequate steps to ensure

		that that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay; • No clear requirement to ensure that the third party is regulated and supervised and has measures in place to comply with the CDD requirements; • No measures to determine under Article 9h of the AML/CFT Act whether the country in which the third party is based adequately applies the FATF Recommendations.
10. Record keeping	**LC**	• There is no requirement empowering competent authorities to request financial institutions to extend the record-keeping period beyond 5 years; • The commencement of the record-keeping period under the AML/CFT Act in relation to customer data is not linked to the date of the termination of an account or a business relationship; • No requirement to retain business correspondence.
11. Unusual transactions	**LC**	• There is no specific requirement to make transaction records available to auditors; **Effectiveness:** • The manner in which Article 8a paragraph 1 is drafted could potentially detract the focus from complex, unusual large transactions or unusual patterns of transactions.
12. DNFBPS – R.5, 6, 8-11	**PC**	• Company Service Providers are not covered by the AML/CFT Act; • Legal professionals are exempted from the obligation to identify the beneficial owner of the client and certain other CDD requirements; • Not all the activities of notaries fall within the scope of the AML/CFT Act; ***Applying Recommendation 5*** • DNFBP are required to verify the customer identity on the basis of documents and information from a public source, but not specifically from reliable and independent sources; • There is no requirement to verify whether any person purporting to act on behalf of a legal person is so authorised; • When conducting on-going due diligence on the business relationship there is no requirement to establish, where necessary, the source of funds; • The provisions dealing with simplified CDD permit DNFBP to waive all CDD measures, except for on-

		going monitoring; • There is no prohibition to apply simplified CDD when there is a suspicion of ML/FT; • There is no requirement to complete verification of identity as soon as reasonably practicable in those cases where verification is not carried out before the establishment of a business relationship; **Effectiveness:** • The understanding and awareness of the obligations dealing with the identification beneficial owners of DNFBP does not appear to be adequate; ***Applying Recommendation 6*** • The PEP definition does not cover persons entrusted with a prominent public function by a foreign jurisdiction who are resident in Poland; • No requirement to apply enhanced CDD if the beneficial owner is a PEP; • There is no requirement to conduct enhanced on-going monitoring on the entire business relationship with a PEP; ***Applying Recommendation 8*** • No requirement to have policies and procedures in place to prevent the misuse of technological developments in ML/FT schemes; • No requirement to have policies and procedures to address the specific risks associated with non face-to-face business relationships when conducting on-going due diligence; ***Applying Recommendation 9*** • No requirement to immediately obtain from the third party the necessary information concerning certain elements of the CDD process; • Partial requirement to take adequate steps to ensure that that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay; • No requirement to ensure that the third party is regulated and supervised and has measures in place to comply with the CDD requirements; • No measures to determine whether the country in which the third party is based adequately applies the FATF Recommendations; ***Applying Recommendation 10*** • There is no requirement empowering competent authorities to request DNFBP to extend the record-keeping period beyond 5 years;

		• The commencement of the record-keeping period under the AML/CFT Act in relation to customer data is not linked to the date of the termination of a business relationship; • No requirement to keep the business correspondence; ***Applying Recommendation 11*** • There is no specific requirement to make transaction records available to competent authorities and auditors; **Effectiveness:** • The manner in which Article 8a paragraph 1 is drafted could potentially detract the focus from complex, unusual large transactions or unusual patterns of transactions.
13. Suspicious transaction reporting	**PC**	• The scope of the reporting requirement is only linked to transactions related to ML/TF and does not extend to the reporting of "*funds"* suspected to be the proceeds of a criminal activity; • The FT reporting obligation is limited to *"transactions"* related to FT and does not extend to *"funds"*; • The deficiencies identified with respect to Recommendation 1 and Special Recommendation II restrict the scope of the reporting requirement; • Possible confusion between reporting obligations under Articles 8.3, 11.1 and 16 (e.g. attempted transactions are not covered under Article 11.1).
14. Protection and no tipping-off	*Largely Compliant*	• *It should be clarified that all civil and criminal liability is comprehensively covered;* • *The tipping-off provision should cover related information.*
15. Internal controls, compliance and audit	*Largely Compliant*	• *There is no provision concerning timely access of the AML/CFT compliance officer and other appropriate staff to CDD and other relevant information;* • *Not all financial institutions (apart from the banking and securities sectors) are obligated to have internal audit function, which also covers AML/CFT policies;* • *There is no legal obligation on financial institutions to establish screening procedures to ensure high standards when hiring employees.*

16. DNFBPS – R.13-15 & 21[46]	**PC**	• Not all the activities of notaries fall within the scope of the AML/CFT Act; • Company Service Providers are not covered by the AML/CFT Act; ***Applying Recommendation 13*** • The scope of the reporting requirement is only linked to transactions related to ML/TF and does not extend to the reporting of "*funds"* suspected to be the proceeds of a criminal activity; • The FT reporting obligation is limited to *"transactions"* related to FT and does not extend to *"funds"*; • The deficiencies identified with respect to Recommendation 1 and Special Recommendation II restrict the scope of the reporting requirement; • Possible confusion between reporting obligations under Articles 8.3, 11.1 and 16 (e.g. attempted transactions are not covered under Article 11.1); ***Applying Recommendation 21*** • There is no requirement to give special attention to business relationships with persons from or in countries which do not or insufficiently apply the FATF Recommendations; • There is no requirement to make written findings available to assist to competent authorities and auditors; • There is no requirement to apply appropriate counter-measures; **Effectiveness:** • Low level of STRs submitted DNFBPs; • No reporting from the real estate sector despite the fact that the real estate market is considered to be particularly vulnerable to money laundering in Poland.
17. Sanctions	**LC**	**Effectiveness:** • No sanctions imposed on directors and senior management.
18. Shell banks	**C**	

[46] The review of Recommendation 16 has taken into account the findings from the 3rd round report on Recommendations 14 and 15.

19. Other forms of reporting	*Compliant*	
20. Other DNFBPS and secure transaction techniques	*Compliant*	
21. Special attention for higher risk countries	**PC**	• There is no requirement to give special attention to business relationships with persons from or in countries which do not or insufficiently apply the FATF Recommendations; • There is no requirement to make written findings available to assist auditors; • There is no requirement to apply appropriate counter-measures; **Effectiveness:** • The effectiveness of the measures which are in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries is debatable.
22. Foreign branches and subsidiaries	**LC**	• There is no explicit obligation for branches and subsidiaries of Polish financial institutions established in a foreign jurisdiction to apply higher standards when the AML/CFT requirements of home and host countries differ; • There is no requirement to inform the home country supervisor where it is impossible to apply AML/CFT measures which are at least equivalent to those in force in Poland.
23. Regulation, supervision and monitoring	**LC**	• There is no registration or licensing system for Cooperative Savings and Credit Unions.
24. DNFBPS - Regulation, supervision and monitoring	**LC**	• No supervision over TCSPs; • Certain activities of notaries are not subject to AML/CFT obligations; **Effectiveness:** • Insufficient focus on the supervision of the real estate agents; • The number of sanctions imposed for breaches of the AML/CFT Act by DNFBPs is very low.
25. Guidelines and Feedback	*Largely Compliant*	• *Consideration could be given to some case specific feedback;* • *Sector-specific AML/CFT guidance issued by the financial supervisors is missing*
Institutional and other measures		

26. The FIU	**LC**	• Out-dated guidance on the manner of reporting; • There are no provisions to ensure that the General Inspector maintains confidential any information received in the performance of his functions following the termination of his appointment.
27. Law enforcement authorities	**PC**	**Effectiveness:** • Over focus on fiscal ML cases; • Low number of ML investigations by LEA in major proceeds-generating cases; • Insufficiently proactive approach by LEA in ML investigations; • Insufficient utilisation of FIU information by LEAs.
28. Powers of competent authorities	*Compliant*	
29. Supervisors	**LC**	**Effectiveness:** • Insufficient number of on-site inspections, prior to implementation of the RBA; • The level of appreciation of ML/FT risks by NSCCU appears to be low, thereby having an impact on the effectiveness of on-site inspections.
30. Resources, integrity and training[47]	**PC (composite rating)**	• The Analytical Units of the Department of Financial Information appear to be understaffed; • High fluctuation of experienced and specially skilled Police staff; • Concern over training in relation to conducting modern financial investigations by all LEAs involved in combating ML/TF, not only Police; • Insufficient number of AML/CFT inspectors within the Control Unit of the GIFI and the PFSA.
31. National co-operation	**LC**	• There is no mechanism for facilitating a regular and joint review of the AML/CFT system and its effectiveness by competent authorities; • No central coordinating body at policy level in the area of AML/CFT.

[47] The review of Recommendation 30 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on resources integrity and training of law enforcement authorities and prosecution agencies.

32. Statistics[48]	**LC (composite rating)**	• Lack of detailed statistics kept by LEAs; • No statistics on confiscation of proceeds of crime which are not ML or TF related; • Insufficient review of effectiveness of the AML/CFT systems on regular basis; • Lack of detailed statistics on information exchanged between domestic law enforcement bodies and their foreign counterparts.
33. Legal persons – beneficial owners	**PC**	• Polish Law, although requiring some transparency with respect to immediate ownership, does not require adequate transparency concerning beneficial ownership and control of legal persons. Access to information on beneficial ownership and control of legal persons, when there is such access, is not always timely; • No real measures in place to guard against abuse in the context of R. 33 of bearer shares of private companies.
34. Legal arrangements – beneficial owners	**N/A**	
International Co-operation		
35. Conventions	**PC**	*Vienna and Palermo Conventions* • The physical elements of money laundering offence do not fully correspond to the Vienna and Palermo Conventions, in particular conversion, concealment, disguise, acquisition, possession or use are not covered in all circumstances (R.1); • Not all essential criteria are provided for in the Polish legislation, e.g. association with or conspiracy as an ancillary offence (R.1); • The confiscation of instrumentalities is discretionary (R.3); • Confiscation regime does not cover instrumentalities transferred to third parties (R.3); *Convention for the Suppression of the Financing of Terrorism* • Funding terrorist organisation for "any purpose" not fully criminalised (SR.II);

[48] The review of Recommendation 32 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendations 37, 38, 39 and SR.IX.

		• The funding of an individual terrorist is not criminalised in all circumstances (SR.II); • Terrorist Financing abroad is not fully covered (SR.II); • There are purposive supplementary elements for some of the acts constituting offences in the treaties annexed of the Convention (SR.II); • Limited scope of terrorist financing offence potentially affects the scope of confiscation and provisional measures especially with regard to "legal" activities of terrorist organisations and individual terrorists (R.3).
36. Mutual legal assistance (MLA)[49]	**C**	
37. Dual criminality	*Largely Compliant*	• *Poland has indicated that it takes a wide view of dual criminality, but the absence of statistical data means there is a reserve on effectiveness;* • *As terrorist financing is not an autonomous offence, the requirement of dual criminality for extradition means that for non-EU countries, not all kinds of financing of terrorism offences are extraditable.*
38. MLA on confiscation and freezing	*Largely Compliant*	• *There are provision in place which comply with international Convention obligations and separate procedures within the European Union recognition of foreign freezing orders;* • *The absence of statistical data means there is a reserve on effectiveness in relation to freezing, seizing, and confiscation (property and value).*
39. Extradition	*Largely Compliant*	• *In the absence of statistics it is not possible to determine whether extradition requests are handled without undue delay.*
40. Other forms of co-operation	**LC**	**<u>Effectiveness:</u>** • Effectiveness issues regarding law enforcement authorities.
Nine Special Recommendations		
SR.I Implement UN instruments	**PC**	*Convention for the Suppression of the Financing of Terrorism* • Funding terrorist organisation for "any purpose" not fully criminalised (SR.II);

[49] The review of Recommendation 36 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendation 28.

		• The funding of an individual terrorist is not criminalised in all circumstances (SR.II); • Terrorist Financing abroad is not fully covered (SR.II); • There are purposive supplementary elements for some of the acts constituting offences in the treaties annexed of the Convention (SR.II); • Deficiencies under SR.III.
SR.II Criminalise terrorist financing	**PC**	• Funding terrorist organisation for "any purpose" not fully criminalised; • The funding of an individual terrorist is not criminalised in all circumstances; • Terrorist Financing abroad is not fully covered; • There are purposive supplementary elements for some of the acts constituting offences in the treaties annexed of the Convention.
SR.III Freeze and confiscate terrorist assets	**PC**	***Implementation of S/RES/1267*** • The EU or Polish Legislation do not cover the freezing of funds derived from funds owned or controlled directly or indirectly by persons acting on their behalf or at the direction of designated persons or entities; • The time taken to amend the EU regulations following amendments made to the list published by the 1267 Committee is relatively long; in this respect the obligation to freeze terrorist funds without delay is not observed; • The freezing mechanism under Article 20d of the AML/CFT Act excludes movable and immovable property, which restricts the scope of the obligations imposed by EU Council Regulation 881/2002; • Reliance on a criminal proceedings in order to freeze terrorists funds is not fully in line with the requirements of UNSCR 1267 since the requirement to freeze assets could be limited in time according to the Criminal Procedure Rules; ***Implementation of S/RES/1373*** • Poland has not yet taken specific measures to cover "EU internals"; • The freezing mechanism under Article 20d of the AML/CFT Act excludes movable and immovable property, which restricts the scope of the obligations imposed by EU Council Regulation 2580/2001; • Reliance on a criminal proceedings in order to

		freeze terrorists funds is not fully in line with the requirements of UNSCR 1373 since the requirement to freeze assets could be limited in time according to the Criminal Procedure Rules; *Other deficiencies:* • No communication system between the authorities and DNFBP; **Effectiveness:** • Concerns over the effectiveness due to conflicting provisions in the EU Regulations and Polish legislation.
SR.IV Suspicious transaction reporting	**PC**	• The FT reporting obligation is limited to *"transactions"* related to FT and does not extend to *"funds"*; • The deficiencies identified with respect to Special Recommendation II restrict the scope of the reporting requirement; • Possible confusion between reporting obligations under Articles 8.3, 11.1 and 16 (e.g. attempted transactions are not covered under Article 11.1).
SR.V International co-operation	**LC (composite rating)**	• 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; • Deficiencies under SR.II have a negative impact; **Effectiveness:** • Effectiveness issues regarding law enforcement authorities.
SR.VI AML requirements for money/value transfer services	**LC**	• Deficiencies in the AML/CFT Law relating to preventive measures, particularly on CDD, apply to MVT operators; **Effectiveness:** • Effectiveness could not be demonstrated since the system for the licensing and supervision of MVT operators is still being set up.
SR.VII Wire transfer rules	**C**	
SR.VIII Non-profit organisations	**PC**	• Limited review of the risks in the NPO sector has been undertaken; • 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 this sector.

SR.IX Cross Border declaration and disclosure	*Largely Compliant*	• *More targeted co-operative enquiries are encouraged;* • *More sensitisation to terrorist financing issues is required.*

9. TABLE 2: RECOMMENDED ACTION PLAN TO IMPROVE THE AML/CFT SYSTEM

AML/CFT System	Recommended Action (listed in order of priority)
1. General	**No text required**
2. Legal System and Related Institutional Measures	
2.1 Criminalisation of Money Laundering (R.1)	Article 299 should be amended to ensure that conversion, concealment, disguise, acquisition, possession and use, as well all types of property, are fully covered by legislation in accordance with the Vienna and Palermo Conventions. The financing of terrorism in all its forms, as explained in the Interpretative Note to SR.II, should be clearly covered as a predicate offence to money laundering. The clarification should be provided (either by legislation or by binding interpretative mechanism) that the subject matter of money laundering offence covers property obtained directly through the commission of an offence. Association with or conspiracy to commit money laundering should be recognised as a criminal offence. Guidance should be issued to clarify that the predicate base of money laundering extends to conduct which occurs in another country but which is not an offence in that country, but would be an offence if it occurs in Poland. Knowledge that such property is proceeds - as widely defined in the Palermo and Council of Europe Convention – is impliedly covered by Article 299, but it should be formally set out in the legislation. Guidance should be issued to clarify that knowledge (the intentional element) can be inferred from objective factual circumstances. The Polish authorities may also wish to consider an alternative lower mental element, like suspicion for Article 299 (1), with appropriately lower penalties, to cover situations where knowledge cannot clearly be proved. Equally, introducing the concept of negligent money laundering will also assist the prosecutorial effort. Greater emphasis needs to be placed on autonomous prosecution of money laundering by third parties. To achieve this, it is necessary for the Polish authorities to address the issue of the evidence required to establish the predicate

	criminality in autonomous money laundering cases. It should be made clear in legislation or guidance that the underlying predicate criminality can be proved by inferences drawn from objective facts and circumstances in money laundering cases brought in respect of both domestic and foreign predicate offences, and to give more guidance generally to prosecutors on the amount of evidence needed to establish underlying predicate offence (for example, that it may be sufficient to establish that e.g. drug trafficking has occurred, but not drug trafficking on a specific date or time, etc.).
2.2 Criminalisation of Terrorist Financing (SR.II)	Legislation should be amended to bring it in line with Article 2 (1) (a) of the TF Convention which doesn't require any specific common purpose for those acts constituting offences in the treaties annexed of the Convention. The Polish authorities are strongly encouraged to urgently address the shortcomings identified in the TF regime, especially with regard to criminalisation of funding terrorist organisation and individual terrorists for "any purpose".
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	The Polish confiscation regime should allow confiscating of instrumentalities, especially when owned by third parties. The discretionary character of the confiscation of instrumentalities raises concerns. The Polish authorities should remedy the deficiencies identified in the TF offence (see supra c.II.1) that potentially affect the scope of confiscation and provisional measures especially with regard to "legal" activities of terrorist organisations and individual terrorists. The Polish authorities should put more emphasis on confiscation and devote additional resources to financial investigation in order to improve the current results.
2.4 Freezing of funds used for terrorist financing (SR.III)	Polish authorities should apply mechanism set out under section 20d of the AML/CFT Act that provides a clear legal mechanism, which would potentially cover designations in Poland in respect of EU citizens or named persons not covered by the EU clearing house list proposed by other countries. Consideration should be given to the merits of a more general administrative procedure for handling SR.III in its entirety, subject to proper safeguards (especially with regard to bona fide third parties). Movable and immovable property should be included in the freezing mechanisms in place pursuant to Article 20(d) of the AML/CFT Law. The Polish authorities may consider amending its national legislation in order to cover deficiencies under the EU Regulations. The Polish authorities should establish an effective system of

	communication with the DNFBP sector in respect of the obligations under SR.III.
2.5 The Financial Intelligence Unit and its functions (R.26)	The AML/CFT Act should be reviewed to address a number of remaining technical shortcomings related to Recommendation 26. In particular, the AML/CFT Act should clearly provide for the manner in which the functions and responsibilities of the General Inspector are to be delegated to the Department on Financial Information. The Guidance on the manner of reporting should be brought up to date to bring it in line with the amended AML/CFT Act. Among other things, the guidance should expressly include a reference to the reporting of FT transactions and reporting under Articles 16 and 17. Although the GIFI regularly disseminates analytical reports to competent authorities (other than the public prosecutor), the legal basis for this procedure appears to be rather ambiguous. A clear provision dealing with this issue should be included in the AML/CFT Act. The General Inspector should be required to maintain confidential any information received in the performance of his functions following the termination of his appointment.
2.6 Law enforcement, prosecution and other competent authorities (R.27)	More emphasis should be placed on ML investigations by LEA in major proceeds-generating cases. ML and TF offences should be on the list of offences for which special investigative techniques can be applied in the investigation. LEA should be sufficiently proactive in ML investigations.
3. Preventive Measures – Financial Institutions	
3.1 Risk of money laundering or terrorist financing	
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)	**Recommendation 5** A provision should be included in the AML/CFT Act expressly requiring financial institutions to carry out customer due diligence measures when carrying out occasional transactions that qualify as a wire transfer amounting to or exceeding €1,000. Financial institutions should be required to verify customer identity on the basis of document, data or information obtained from a reliable and independent source. Financial institutions should be required to identify the beneficial owner, where applicable, and not simply attempt to identify the beneficial owner. Additionally, there should be a clear provision to explicitly prohibit financial institutions from

	establishing (or continuing) a business relationship with a customer in those instances where the ultimate beneficiary owner cannot be determined. Financial institutions should be required to ensure that a person acting on behalf of a legal person is so authorised. Financial institutions should be required when conducting on-going due diligence on the business relationship to establish, where necessary, the source of funds. Financial institutions should not be permitted to waive the application of CDD measures entirely when dealing with low risk customers and products. Additionally, the application of simplified CDD should not be accepted whenever there is a suspicion of ML/FT. Financial institutions should be required to complete the verification of identity as soon as reasonably practicable in those cases where verification is not carried out before the establishment of a business relationship. Additionally, financial institutions should not be permitted to open an account without performing full CDD measures, since the relevant criterion merely refers to the postponement of verification and not full CDD. Financial institutions should be required to conduct CDD measures to existing customers, including those customers holding an anonymous account. **Recommendation 6** The PEP definition should be extended to cover persons entrusted with prominent public functions in a foreign country irrespective of their residence. Financial institutions should be required to apply enhanced CDD measures when the beneficial owner is a PEP. Financial institutions should be required to obtain senior management approval to continue the business relationship where the customer or beneficial owner subsequently becomes or is found to be a PEP after having been accepted as a client. Financial institutions should be required to conduct enhanced on-going monitoring on the entire business relationship and not just transactions. **Recommendation 7** Article 9e (3) of the AML/CFT Act should apply to respondent institutions located in any foreign jurisdictions. Financial institutions should be required to determine the reputation of the respondent institution and whether it has been subject to a money laundering or terrorist financing investigation or regulatory action. Financial institutions should be required to ascertain that the

	AML/CFT measures implemented by a respondent institution are adequate and effective. **Recommendation 8** A requirement to have policies and measures to prevent the misuse of technological developments in ML/FT schemes should be introduced. Financial institutions should be required to have policies and procedures to address the specific risks associated with non face-to-face business relationships when conducting on-going due diligence.
3.3 Reliance on third parties (R.9)	The provisions on reliance should be entirely amended to be brought in line with the different criteria set out under Recommendation 9. In particular, the following requirements should be provided for: • Immediately obtain from the third party the necessary information concerning certain elements of the CDD process (Criteria 5.3 to 5.6); • Take adequate steps to ensure that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay; • Satisfy themselves that the third party is regulated and supervised and has measures in place to comply with the CDD requirements.
3.4 Financial institution secrecy or confidentiality (R.4)	Polish authorities should take the necessary steps to introduce provisions in the AML/CFT Act to cover reliance on third parties, specifically with respect to obtaining information from them.
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	***Recommendation 10*** Legislation should explicitly empower competent authorities to request financial institutions to extend the record-keeping period beyond five years. The record-keeping period for identification data under the AML/CFT Act should commence on the date of the termination of an account or a business relationship. Financial institutions should be required to maintain records of business correspondence.
3.6 Monitoring of Transactions and Relationship Reporting (R. 11 and R. 21)	***Recommendation 11*** The Polish authorities should introduce a specific requirement to pay special attention to all complex or unusual transactions and unusual patterns of transactions. Moreover, a requirement to make transaction records available

	to and auditors should also be included in the law. ***Recommendation 21*** The Polish authorities should revise the provisions dealing with Recommendation 21. In particular, a specific requirement to give special attention to business relationships with persons from or in countries which do not or insufficiently apply the FATF Recommendations should be introduced. The written findings in relation to the analysis of transactions that have no apparent economic or visible lawful purpose should be available to assist auditors. Competent authorities should be empowered to apply appropriate counter-measures. The PFSA and GIFI should provide further assistance to financial institutions regarding the practical implementation of the requirements under Recommendation 21.
3.7 Suspicious transaction reports and other reporting (R.13 & SR.IV)	***Recommendation 13 and Special Recommendation IV*** The scope of the ML reporting requirement should be extended to the reporting of "funds" suspected to be the proceeds of a criminal activity. The FT reporting obligation should be extended to "funds" as required under Criterion 13.2. The reporting requirement under Article 11 paragraph 1 should expressly provide for attempted transactions. The Polish authorities should revise the legal text of the entire reporting regime to remove any overlaps between the requirements under Article 11 and 16, to provide for a clear legal basis for the reporting of suspicious activity reports.
3.8 Foreign Branches (R.22)	***Recommendation 22*** The Polish authorities should introduce a requirement for foreign branches and subsidiaries of Polish financial institutions to apply higher standards when the AML/CFT requirements of home and host countries differ. Financial institutions should be required to inform the home country supervisor where it is impossible to apply AML/CFT measures which are at least equivalent to those in force in Poland.
3.9 Shell banks (R.18)	The Polish authorities should consider amending the definition of a "shell bank" to specify that a shell bank will qualify as such if, *inter alia*, it is not part of a financial group which is subject to effective consolidated supervision.

3.10 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17)	***Recommendation 23*** The Polish authorities should introduce a licensing system as defined in the Basel Core Principles for Cooperative Savings and Credit Unions. ***Recommendation 17*** The Polish authorities should apply sanctions to directors and senior management when appropriate. ***Recommendation 29*** More AML/CFT supervisory on-site visits should be conducted. The authorities should take measures to ensure that the NSCCU is properly apprised of the ML/FT risks within its sectors.
3.11 Money or value transfer services (SR. VI)	The Polish authorities should consider taking steps to ensure that a public list of branches and agents of EU payment institutions is included in the register.
4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	The Polish authorities should review the exemption applicable to legal professionals from certain CDD requirements set out in the AML/CFT Act Article 10d. The Polish authorities should review the definition set out under Article 2.1.n of the AML/CFT Act to ensure that no ambiguities arise with respect to the scope of application of AML/CFT obligations to the activities of notaries. The Polish authorities should include company service providers within the scope of application of the AML/CFT Act. ***Applying Recommendation 5*** DNFBP should be required to verify customer identity on the basis of document, data or information obtained from a reliable and independent source. DNFBP should be required to identify the beneficial owner, where applicable, and not simply attempt to identify the beneficial owner. Legal professionals should be not exempted from the requirement to identify the beneficiary owner. Additionally, there should be a clear provision to explicitly prohibit DNFBP from establishing (or continuing) a business relationship with a customer in those instances where the ultimate beneficiary owner cannot be determined.

	DNFBP should be required to ensure that a person acting on behalf of a legal person is so authorised. DNFBP should be required when conducting on-going due diligence on the business relationship to establish, where necessary, the source of funds. DNFBP should not be permitted to waive the application of CDD measures entirely when dealing with low risk customers and products. DNFBP should be required to complete the verification of identity as soon as reasonably practicable in those cases where verification is not carried out before the establishment of a business relationship. ***Applying Recommendation 6*** The PEP definition should be extended to cover persons entrusted with prominent public functions in a foreign country irrespective of their residence. DNFBP should be required to apply enhanced CDD measures when the beneficial owner is a PEP. DNFBP should be required to conduct enhanced on-going monitoring on the entire business relationship and not just transactions. ***Applying Recommendation 8*** A requirement to have policies and measures to prevent the misuse of technological developments in ML/FT schemes should be introduced. DNFBP should be required to have policies and procedures to address the specific risks associated with non face-to-face business relationships when conducting on-going due diligence. ***Applying Recommendation 9*** The provisions on reliance should be entirely amended to be brought in line with the different criteria set out under Recommendation 9. ***Applying Recommendation 10*** The Polish legislation should explicitly empower competent authorities to request DNFBP to extend the record-keeping period beyond five years. The record-keeping period for identification data under the AML/CFT Act should commence on the date of the termination of a business relationship. Additionally, DNFBP should be required to maintain records of business correspondence. ***Applying Recommendation 11*** The Polish authorities should consider introducing a specific

	requirement to pay special attention to all complex or unusual transactions and unusual patterns of transactions. Moreover, a requirement to make transaction records available to competent authorities and auditors should also be included in the law.
4.2 Suspicious transaction reporting (R.16)	The Polish authorities should identify reasons for the complete absence of reporting by the real estate sector and implement measures to rectify the situation. ***Applying Recommendation 13*** The scope of the ML reporting requirement should be extended to the reporting of "funds" suspected to be the proceeds of a criminal activity. The FT reporting obligation should be extended to "funds" as required under Criterion 13.2. The reporting requirement under Article 11 paragraph 1 should expressly provide for attempted transactions. The Polish authorities should revise the legal text of the entire reporting regime to remove any overlaps between the requirements under Article 11 and 16, to provide for a clear legal basis for the reporting of suspicious activity reports and to include an obligation to refrain from conducting a suspicious transaction before reporting it to the GIFI. ***Applying Recommendation 21*** The Polish authorities should introduce a specific requirement to give special attention to business relationships with persons from or in countries which do not or insufficiently apply the FATF Recommendations. The written findings in relation to the analysis of transactions that have no apparent economic or visible lawful purpose should be available to assist competent authorities and auditors. Competent authorities should be empowered to apply appropriate counter-measures. The PFSA and the GIFI should provide further assistance to DNFBPs regarding the practical implementation of the requirements under Recommendation 21.
4.3 Regulation, supervision and monitoring (R.24)	The Polish authorities should take measures to ensure that all DNFBP, especially real estate agents, are subject to effective supervision. The sanctioning regime for DNFBP should be reviewed to determine whether it is being effectively applied.
5. Legal Persons and Arrangements & Non-Profit	

Organisations	
5.1 Legal persons – Access to beneficial ownership and control information (R.33)	Poland should review its commercial, corporate and other laws with a view to taking measures to provide adequate transparency with respect to beneficial ownership. Measures should be put in place to guard against abuse in the context of R. 33 of bearer shares.
5.2 Legal arrangements – Access to beneficial ownership and control information (R.34)	
5.3 Non-profit organisations (SR.VIII)	The Polish authorities should: • Undertake a formal analysis of threats posed by this sector as a whole and to identify its risks. • Review the existing system of relevant laws and regulations in order to assess the adequacy of the current legal framework with respect to criterion VIII.1. • Review the effective and proportional oversight of the NPO sector, the issuing of guidance to financial institutions on the specific risks of this sector and consideration of whether and how further measures need to be taken in the light of the Best Practices Paper for SR.VIII. In particular, programme verification and direct field audits should be considered in identified vulnerable parts of the NPO sector. Consideration might usefully be given as to whether and how any relevant private sector watchdogs could be utilised. • Provide assistance to raise awareness for SR.VIII among existing control bodies engaged with the NPO sector so that they also could fully take account of SR VIII issues in their oversight.
6. National and International Co-operation	
6.1 National co-operation and coordination (R.31)	A central coordinating body in the area of combating ML/FT should be established in order to coordinate AML/CFT at policy level. More efficient mechanism for domestic cooperation and coordination should be established in order to enhance the effective utilisation of the GIFI information.
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	**Recommendation 35** Poland should take necessary measures to remedy identified deficiencies under Recommendations 1 and 3 and Special Recommendation II to fully implement the Vienna, Palermo

	and TF Conventions. **Special Recommendation I** The Polish authorities should take steps to address the deficiencies identified under SR.III to fully implement the requirements of the UNSCRs, in particular implement the mechanism set out in Chapter 5a of the AML/CFT Act.
6.3 Mutual Legal Assistance (R.36 & SR.V)	Poland should fully cover the TF offence to remove any potential impact on the provision of mutual legal assistance.
6.5 Other Forms of Co-operation (R.40 & SR.V)	It is recommended that procedures are set out in place to centrally record and monitor all international cooperation requests on matters related to ML and TF.
7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	***Recommendation 30*** <u>FIU</u> The Polish authorities should allocate further resources to the analytical units of the Department of Financial Information of the GIFI. <u>Law enforcement</u> The Polish authorities should take steps to tackle the fluctuation of experienced and especially skilled Police staff. More training should be provided in relation to conducting modern financial investigations by all LEAs involved in combating ML/TF, not only the Police. More continuous specialised training for prosecution authorities in the area of combating ML/FT should be provided. <u>Supervisory authorities</u> The Polish authorities should allocate further human resources for compliance monitoring purposes to the Control Unit of the GIFI and the PFSA. ***Recommendation 32*** A mechanism for reviewing effectiveness of the AML/CFT systems on a regular basis should be established. The GIFI should maintain relevant statistics on requests made to obligated institutions according to Article 13a of the AML/CFT Act. More detailed statistics should be kept by the Polish authorities to demonstrate the effectiveness of the AML/CFT

	regime overall, in particular on ML cases and their underlying predicate offences. Statistics on confiscation of proceeds of crime which are not ML or TF related should be kept. The Polish authorities should keep MLA statistics regarding offences other than ML or TF leaving. Law enforcement authorities should keep detailed statistics on the exchange of information with foreign counterparts.
7.2 Other relevant AML/CFT measures or issues	
7.3 General framework – structural issues	

10. TABLE 3: AUTHORITIES' RESPONSE TO THE EVALUATION (IF NECESSARY)

RELEVANT SECTIONS AND PARAGRAPHS	COUNTRY COMMENTS
Section 3.7 – suspicious transaction reports and other reporting (R. 13 and SR.IV), paragraph 758	The Polish authorities would like to point out that the definition of transaction in the AML Act is broad (and related to any economic/legal relationship between reporting entity and customer) and includes any transfer of funds or asset values and that reporting entities' obligation to analyse circumstances of transactions has no limits in time. Thus, if reporting entity possesses new information about relation between funds and criminal activities, it has a legal base to report transaction related to these funds to the FIU, even if it was carried out in the past. Moreover, if newly available information indicating relation to criminal activities was not included into the analysis of transaction circumstances, and if that fact was noticed during inspection, the supervisory authorities would point it out in post-control protocol. In practice financial institutions submit reports to the GIFI when a transaction is suspected to be related to criminal activity, even though this is not prescribed by the AML/CFT Act.
Section 3.7 – suspicious transaction reports and other reporting (R. 13 and SR.IV), paragraph 764	The Polish authorities would like to stress that despite of some technical deficiencies in the reporting requirement under R.13, in practice the STR regime in Poland is comprehensively and accurately established. This conclusion includes the question of a lack of formal obligation to report "funds" suspected to be the proceeds of a criminal activity in AML Act. From the point of view of effectiveness this deficiency is compensated by common understanding between reporting entities and the FIU and, following the information gathered by evaluation team during the on-site visit, in practice financial institutions submit reports to the GIFI when a transaction is suspected to be related to criminal activity, even though this is not prescribed by the AML/CFT Act.

V. COMPLIANCE WITH THE 3RD EU AML/CFT DIRECTIVE

Poland has been a member country of the European Union since 2004. It has implemented **Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing** (hereinafter: "the Directive") and the **Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis**.

The following sections describe the major differences between the Directive and the relevant FATF 40 Recommendations plus 9 Special Recommendations.

1.	**Corporate Liability**
Art. 39 of the Directive	Member States shall ensure that natural and legal persons covered by the Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive.
FATF R. 2 and 17	Criminal liability for money laundering should extend to legal persons. Where that is not possible (i.e. due to fundamental principles of domestic law), civil or administrative liability should apply.
Key elements	The Directive provides no exception for corporate liability and extends it beyond the ML offence even to infringements which are based on national provisions adopted pursuant to the Directive. What is the position in your jurisdiction?
Description and Analysis	Natural and legal persons can be held liable for infringements of Polish national legislation. Corporate criminal liability is covered by the Act of 28 October 2002 on the Liability of Collective Entities for Acts Prohibited under Penalty, which sets out the basic principles governing procedures to be followed in matters of such liability. According to Art 3 of the Act of 28 October 2002 on Liability of Collective Entities for Acts Prohibited Under Penalty legal persons and organisational units without legal personality are liable for a prohibited act being the behaviour of a natural person acting on behalf of the collective entity or who is an entrepreneur. The sanctions for legal persons are set out in Articles 7,8 and 9 of this Act, i.e. forfeiture, fine up to 10 % of the revenue, ban on promoting the business activities and ban on using grants from public funds -as well as ban on applying for public procurements, ban on conducting basic or secondary economic activity and making the sentence publicly known It was understood that a company could now be prosecuted on the basis of vicarious liability, but this would not preclude employees being charged

	individually. Pursuant to the provisions of Art. 6 of the Act, the individual liability of the perpetrator employed in a collective entity is not excluded even if such entity does not incur liability provided by the Act. In addition, Chapter 7a of the AML/CFT Act contains pecuniary sanctions applicable to legal persons for a breach of this Act. According to provisions set out in sectoral laws there is a range of sanctions which refer to natural and legal persons. With respect to legal persons the supervisors are enabled to issue recommendations, cautions and orders, to impose fine and to revoke the license or delete from register.
Conclusion	Criminal liability for money laundering extends to legal persons.
Recommendations and Comments	Not applicable

2.	**Anonymous accounts**
Art. 6 of the Directive	Member States shall prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks.
FATF R. 5	Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.
Key elements	Both prohibit anonymous accounts but allow numbered accounts. The Directive allows accounts or passbooks on fictitious names but always subject to full CDD measures. What is the position in your jurisdiction regarding passbooks or accounts on fictitious names?
Description and Analysis	Article 19 of the Act of 25 June 2009 amending the AML/CFT Act by implementing the Third AMLD requires that any contracts allowing anonymous accounts to be kept, shall be deemed null and void by law, after 12 months of this act entering into force. Also the obliged institutions shall immediately take actions to identify such account holders and to inform them of the provisions of paragraph 1.
Conclusion	Polish AML/CFT regime does not directly prohibit the opening and maintaining of anonymous accounts or accounts in fictitious names. There is an indirect prohibition of keeping anonymous passbooks (the institutions are obliged to identify their clients and verify their identity).
Recommendations and Comments	There should be a direct prohibition not to open anonymous counts and accounts in fictitious names.

3.	Threshold (CDD)
Art. 7 b) of the Directive	The institutions and persons covered by the Directive shall apply CDD measures when carrying out occasional transactions amounting to €15,000 or more.
FATF R. 5	Financial institutions should undertake CDD measures when carrying out occasional transactions above the applicable designated threshold.
Key elements	Are transactions and linked transactions of €15,000 covered?
Description and Analysis	Para 4 (2) of Article 8b of the AML/CFT Act requires the application of CDD measures before carrying out occasional transactions of the equivalent of more than €15,000, regardless of whether the transaction is carried out as a single operation or as several operations if the circumstances indicate that they are linked.
Conclusion	Transaction and linked transactions amounting to €15,000 are covered.
Recommendations and Comments	Not applicable

4.	Beneficial Owner
Art. 3(6) of the Directive (see Annex)	The definition of 'Beneficial Owner' establishes minimum criteria (percentage shareholding) where a natural person is to be considered as beneficial owner both in the case of legal persons and in the case of legal arrangements
FATF R. 5 (Glossary)	'Beneficial Owner' refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or legal arrangement.
Key elements	Which approach does your country follow in its definition of "beneficial owner"? Please specify whether the criteria in the EU definition of "beneficial owner" are covered in your legislation.
Description and Analysis	The definition of beneficial owner, contained in Article 2 (1a) of the AML/CFT Act, is as follows: • natural person or natural persons who are owners of a legal entity or exercise control over a client or have an impact on a natural person on whose behalf a transaction or activity is being conducted. • natural person or natural persons who are stakeholders or shareholders or have the voting right at the level of above 25% within such a legal entity, therein by means of block of registered shares • natural person or natural persons who exercises control over at

	least 25% of the asset values in the case of entities entrusted with the administration of asset values and the distribution of with the exception of the entities carrying out activities referred to in Article 69 item 2 point 4 of the Act of 29 July 2005 on trading in financial instruments.
Conclusion	The definition of beneficial owner in AML/CFT Act corresponds to the definition provided by the Directive and also to the FATF definition.
Recommendations and Comments	Not applicable

5.	**Financial activity on occasional or very limited basis**
Art. 2 (2) of the Directive	Member States may decide that legal and natural persons who engage in a financial activity on an occasional or very limited basis and where there is little risk of money laundering or financing of terrorism occurring do not fall within the scope of Art. 3(1) or (2) of the Directive. Art. 4 of Commission Directive 2006/70/EC further defines this provision.
FATF R. concerning financial institutions	When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially (2004 AML/CFT Methodology para 23; Glossary to the FATF 40 plus 9 Special Recs.).
Key elements	Does your country implement Article 4 of Commission Directive 2006/70/EC?
Description and Analysis	Polish legislation does not implement this optional provision given by the Directive. Therefore the AML/CFT Act does not provide exemptions for persons and entities who engage in a financial activity on occasional or a very limited basis and where there is a little risk of ML or FT. However, under Para 5 of Article 9 of AML/CFT Act the Minister Competent for Financial Institutions may set forth categories of persons or activities which are related to low risk of money laundering or terrorist financing. Up to now no relevant regulation has been issued.
Conclusion	Poland did not implement Art. 4 of the Directive.
Recommendations and Comments	Not applicable

6.	Simplified Customer Due Diligence (CDD)
Art. 11 of the Directive	By way of derogation from the relevant Article the Directive establishes instances where institutions and persons may not apply CDD measures. However the obligation to gather sufficient CDD information remains.
FATF R. 5	Although the general rule is that customers should be subject to the full range of CDD measures, there are instances where reduced or simplified measures can be applied.
Key elements	Is there any implementation and application of Art. 3 of Commission Directive 2006/70/EC which goes beyond the AML/CFT Methodology 2004 criterion 5.9?
Description and Analysis	According to Article 9d of the AML/CFT Act the obligated institutions may apply reduced CDD measures: • when the client is: o an entity providing financial services and established in the territory of a Member State or an equivalent country o government body, local government authority and execution body o a company whose securities are admitted to public trading on a regulated market in at least one European Union member state or in an equivalent country • in relation to: o life insurance policies with the thresholds laid down in the Directive o electronic money, within the meaning of the Act of 12 September 2002 on electronic payment instruments, if the maximum amount stored in the device does not exceed the threshold laid down in the Directive In respect of financial institutions, government bodies and life insurance policies under threshold the obligated institution shall collect information to determine whether a client meets the requirements of the AML/CFT Act. In addition, Article 9d(1) completely exempts financial institutions from carrying out CDD measures with respect to the above categories of clients and products According to Para 5 of Art. 9d the Minister competent for Financial Institutions may determine, by regulation, other categories of persons or activities where, is a low risk of ML or FT, and may be apply reduced CDD measures.
Conclusion	The Polish legislation implements Article 11 of the Directive with the

	exception of paragraph 2 letter b and paragraph 5 letter c.
Recommendations and Comments	Financial institutions should not be allowed to waive all CDD measures in case of simplified customer due diligence. The Directive specifically requires: where institutions and persons may not apply CDD measures, the obligation to gather sufficient CDD information remains.

7.	**Politically Exposed Persons (PEPs)**
Art. 3 (8), 13 (4) of the Directive *(see Annex)*	The Directive defines PEPs broadly in line with FATF 40 (Art. 3(8)). It applies enhanced CDD to PEPs residing in another Member State or third country (Art. 13(4)). Directive 2006/70/EC provides a wider definition of PEPs (Art. 2) and removal of PEPs after one year of the PEP ceasing to be entrusted with prominent public functions (Art. 2(4)).
FATF R. 6 and Glossary	Definition similar to Directive but applies to individuals entrusted with prominent public functions in a foreign country.
Key elements	Does your country implement Art. 2 of Commission Directive 2006/70/EC, in particular Art. 2(4), and does it apply Art. 13(4) of the Directive?
Description and Analysis	The definition of PEPs is provided in the paragraph 1f of Art. 2 of the AML/CFT Act and broadly follows the definition of the Directive and the Commission Directive 2006/70. Para 4 of Art 9e of the AML/CFT Act requires obligated institutions to include the application of risk based procedures to determine whether the customer is a PEP, obtain the approval of senior management, take adequate measures to establish the source of funds, and maintain constant monitoring od conducted transitions.
Conclusion	Poland has partially implemented Article 2(4) of Commission Directive 2006/70/EC and Article 13(4) of the Directive.
Recommendations and Comments	Poland should take legislative measures to implement a requirement to establish the source of wealth of a PEP as well as a requirement to conduct enhanced on-going monitoring on the entire business relationship with a PEP.

8.	**Correspondent banking**
Art. 13 (3) of the Directive	For correspondent banking, Art. 13(3) limits the application of Enhanced Customer Due Diligence (ECDD) to correspondent banking relationships with institutions from non-EU member countries.

FATF R. 7	Recommendation 7 includes all jurisdictions.
Key elements	Does your country apply Art. 13(3) of the Directive?
Description and Analysis	Poland applies Article 13 (3) of the Directive through Para 3 of Art. 9e of the AML/CFT Act, which limits the application of enhanced due diligence to cross-border relationships with institutional correspondents from countries other than EU member states and equivalent countries.
Conclusion	The requirements provided by the AML/CFT Act are in line with Article 13 (3) of the Directive.
Recommendations and Comments	Not applicable

9.	**Enhanced Customer Due Diligence (ECDD) and anonymity**
Art. 13 (6) of the Directive	The Directive requires ECDD in case of ML or TF threats that may arise from products or transactions that might favour anonymity.
FATF R. 8	Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity [...].
Key elements	The scope of Art. 13(6) of the Directive is broader than that of FATF R. 8, because the Directive focuses on products or transactions regardless of the use of technology. How are these issues covered in your legislation?
Description and Analysis	According to Article 9g of the AML/CFT Act obligated institutions are required to "apply appropriate measures of financial security in order to prevent money laundering or terrorist financing, which may arise from products or transactions allowing to maintain anonymity".
Conclusion	Poland has implemented Article 13 (6) of the Directive
Recommendations and Comments	Not applicable

10.	**Third Party Reliance**
Art. 15 of the Directive	The Directive permits reliance on professional, qualified third parties from EU Member States or third countries for the performance of CDD, under certain conditions.
FATF R. 9	Allows reliance for CDD performance by third parties but does not specify particular obligated entities and professions which can qualify

	as third parties.
Key elements	What are the rules and procedures for reliance on third parties? Are there special conditions or categories of persons who can qualify as third parties?
Description and Analysis	According to Article 9h of the AML/CFT Act each obligated institution may rely on other entities in so far as the implementation of CDD measures required by the law, furthermore the responsibility for such an implementation shall remain with the obligated institution. According to Article 9i obligated institutions may rely on the result of CDD measures executed by another entity providing financial services from EU Member State or equivalent countries when conducting a transaction on the basis of an order or a disposition. Article 9h permits reliance on third parties from non-equivalent third countries, furthermore there are no requirements for professional registration and supervision.
Conclusion	With the exception of the execution of transactions based on order of another financial institution the Polish AML/CFT Act does not require reliance on professional, qualified third parties from the EU Member States or third countries for CDD purposes, under certain conditions.
Recommendations and Comments	The authorities need to consider implementing all requirements set out in Article 15 of the Directive.

11.	**Auditors, accountants and tax advisors**
Art. 2 (1)(3)(a) of the Directive	CDD and record keeping obligations are applicable to auditors, external accountants and tax advisors acting in the exercise of their professional activities.
FATF R. 12	CDD and record keeping obligations: 1. do not apply to auditors and tax advisors; 2. apply to accountants when they prepare for or carry out transactions for their client concerning the following activities: • buying and selling of real estate; • managing of client money, securities or other assets; • management of bank, savings or securities accounts; • organisation of contributions for the creation, operation or management of companies; • creation, operation or management of legal persons or arrangements, and buying and selling of business entities (2004 AML/CFT Methodology criterion 12.1(d)).
Key elements	The scope of the Directive is wider than that of the FATF standards but does not necessarily cover all the activities of accountants as described by criterion 12.1(d). Please explain the extent of the scope

	of CDD and reporting obligations for auditors, external accountants and tax advisors.
Description and Analysis	The scope of AML/CFT Act covers entities operating in so far as accounts bookkeeping services, expert auditors and tax advisers (Para 1 n) and o) of Art. 2). They are required to identify their customers when entering into business relationship, when carrying out occasional transactions amounting to €15,000 or more, when there are doubts about the veracity or adequacy of previously obtained customer identification data and in all cases when there is reasonable doubt for money laundering or terrorism financing. According to Para 1 of Art. 11 and Para 1 of Art. 16 of the AML/CFT Act the obliged institutions are required to provide STR to the GIFI when may arise the suspicion of ML/TF or criminal offence. The AML/CFT Act does not provide threshold for reporting obligations.
Conclusion	The AML/CFT Act covers accountants, auditors and tax advisors in line with the Directive. CDD and reporting obligations are the same as for all obliged entities under the scope of the AML/CFT Act.
Recommendations and Comments	Not applicable

12.	**High Value Dealers**
Art. 2(1)(3)e) of the Directive	The Directive applies to natural and legal persons trading in goods where payments are made in cash in an amount of €15,000 or more.
FATF R. 12	The application is limited to those dealing in precious metals and precious stones.
Key elements	The scope of the Directive is broader. Is the broader approach adopted in your jurisdiction?
Description and Analysis	According to Subpara t) Art. 2 of the AML/CFT Act each entrepreneurs receiving payment for commodities in cash of the value equal to or exceeding the equivalent of €15,000, also when the payment for a given product is made by more than one operation, is subject to AML rules. According to Para 1 of Art. 11 and Para 1 of Art. 16 of the AML/CFT Act obligated institutions are required to submit STRs to the GIFI when may arise the suspicion of ML/TF or criminal offence.
Conclusion	The AML/CFT Act adopted the broader approach of the Directive.
Recommendations and Comments	Not applicable

13.	Casinos
Art. 10 of the Directive	Member States shall require that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of €2 000 or more. This is not required if they are identified at entry.
FATF R. 16	The identity of a customer has to be established and verified when he or she engages in financial transactions equal to or above €3 000.
Key elements	In what situations do customers of casinos have to be identified? What is the applicable transaction threshold in your jurisdiction for identification of financial transactions by casino customers?
Description and Analysis	According to Art. 9c of The AML/CFT Act it is required to conduct identification of the clients and verification of their identity in casino or cash bingo room at entry. There is no threshold prescribed for identification and verification purposes in case of casino or bingo room customers. According to para 1a Article 8 of the AML/CFT Act casino operators are required to register all transactions in relation to purchase or sale of gambling chips with a value amounting €1 000 or more.
Conclusion	The scope of the AML/CFT Act covers all customers entering a casino. It is required that all casino customers are identified and their identity verified at entry regardless of the value of the gambling chips purchased for gambling.
Recommendations and Comments	Not applicable

14.	Reporting by accountants, auditors, tax advisors, notaries and other independent legal professionals via a self-regulatory body to the FIU
Art. 23 (1) of the Directive	This article provides an option for accountants, auditors and tax advisors, and for notaries and other independent legal professionals to report through a self-regulatory body, which shall forward STRs to the FIU promptly and unfiltered.
FATF Recommendations	The FATF Recommendations do not provide for such an option.
Key elements	Does the country make use of the option as provided for by Art. 23 (1) of the Directive?
Description and Analysis	According to para 4 Art 11 of the AML/CFT Act STRs may be forwarded to the GIFI through the agency of a territorially competent body of professional self-management of notaries, attorneys, legal advisers and foreign lawyers, if a national body of such a self-

	management body adopts a resolution determining detailed rules and a course of provision of such information. The national self-management body submits the list of persons responsible for providing such information to the GIFI.
Conclusion	The Polish AML/CFT legislation makes use of the option provided by Art. 23 (1) of the Directive.
Recommendations and Comments	Not applicable

15.	**Reporting obligations**
Arts. 22 and 24 of the Directive	The Directive requires reporting where an institution knows, suspects, or has reasonable grounds to suspect money laundering or terrorist financing (Art. 22). Obligated persons should refrain from carrying out a transaction knowing or suspecting it to be related to money laundering or terrorist financing and to report it to the FIU, which can stop the transaction. If to refrain is impossible or could frustrate an investigation, obligated persons are required to report to the FIU immediately afterwards (Art. 24).
FATF R. 13	Imposes a reporting obligation where there is suspicion that funds are the proceeds of a criminal activity or related to terrorist financing.
Key elements	What triggers a reporting obligation? Does the legal framework address *ex ante* reporting (Art. 24 of the Directive)?
Description and Analysis	According to Para 3 of Art. 8 of the AML/CFT Act the obliged institutions required to register transactions which may arise the suspicion of ML or TF. Pursuant to para 2 Article 12 those transactions in the case of which there is a suspicion of ML or TF should be reported to GIFI. The para 2 point 2 of Article 12 requires that such report should be sent immediately. The para 1 of Article 16 also requires to report the transactions which may be related to the criminal offence. The para 4 of Article 16 of the AML/CFT Act requires the reporting entities - with the exception of notaries, attorneys, legal advisers and foreign lawyers - to suspend the suspicious transaction for the 24 hours after GIFI confirmation of the receipt of STR. GIFI may extend the suspension for up to 72 additional hours. According to Art. 17, where the refrain is not possible, obligated institutions shall provide a STR immediately after the completion of a transaction. Para 1 Art 18 stipulates that in the case when the report follows the execution of suspicious transaction, the GIFI may provide a written request to suspend the transaction or block the account for no more than 72 hours and shall notify the competent public prosecutor on a suspicion of having committed a crime.
Conclusion	The general principle of forwarding the STRs on registered

	transactions - which had been carried out - is stipulated by the AML/CFT Act. However the act foresees also the *ex-ante* reporting, which triggers the procedure of postponing the transaction or blocking the account. The applied exceptions for notaries, attorneys, legal advisers and foreign lawyers on suspension requirements are not in line with Art. 24 of the Directive.
Recommendations and Comments	The authorities need to consider implementing all requirements set out in Art. 24 of the Directive.

16.	**Tipping off (1)**
Art. 27 of the Directive	Art. 27 provides for an obligation for Member States to protect employees of reporting institutions from being exposed to threats or hostile actions.
FATF R. 14	No corresponding requirement (directors, officers and employees shall be protected by legal provisions from criminal and civil liability for "tipping off", which is reflected in Art. 26 of the Directive)
Key elements	Is Art. 27 of the Directive implemented in your jurisdiction?
Description and Analysis	In order to protection of employees Polish authorities apply Art. 184 of Code of Criminal Procedure, which provides the mechanism of protecting anonymity of witnesses. These provisions do not cover the requirements laid down in Art. 27 of the Directive. Furthermore there is no requirement that the name or other personal data of the person who initially noticed the suspicious information is kept anonym. Also the AML/CFT Act does not provide specific provisions to protect employees of reporting institutions from being exposed to threats or hostile actions.
Conclusion	Poland does not implement Art 27 of the Directive.
Recommendations and Comments	The authorities need to consider implementing the requirements set out in Art. 27 of the Directive.

17.	**Tipping off (2)**
Art. 28 of the Directive	The prohibition on tipping off is extended to where a money laundering or terrorist financing investigation is being or may be carried out. The Directive lays down instances where the prohibition is lifted.
FATF R. 14	The obligation under R. 14 covers the fact that an STR or related information is reported or provided to the FIU.

Key elements	Under what circumstances are the tipping off obligations applied? Are there exceptions?
Description and Analysis	Pursuant to Art. 34 of AML/CFT Act any disclosure of information to unauthorized parties, including the parties of the transaction or the account holders; on the fact that the FIU has been informed about the suspicious transactions or on the accounts of entities for which there is a reasoned suspicion that they have a connection with terrorist financing; or on transactions made by these entities, is prohibited.
Conclusion	The AML/CFT Act does not provide provision for extension of prohibition on tipping off where a money laundering or terrorist financing investigation is being or may be carried out.
Recommendations and Comments	The authorities need to consider implementing all the requirements set out in Art. 27 of the Directive.

18.	**Branches and subsidiaries (1)**
Art. 34 (2) of the Directive	The Directive requires credit and financial institutions to communicate the relevant internal policies and procedures where applicable on CDD, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication to branches and majority owned subsidiaries in third (non EU) countries.
FATF R. 15 and 22	The obligations under the FATF 40 require a broader and higher standard but do not provide for the obligations contemplated by Art. 34 (2) of the EU Directive.
Key elements	Is there an obligation as provided for by Art. 34 (2) of the Directive?
Description and Analysis	According to Para. 1 of Art 9j the financial institutions with its branches and subsidiaries operating in third countries are obliged to apply the financial security measures set out in AML/CFT Act in those branches and subsidiaries. The Para 3 Art 9j requires that the financial institutions shall inform its branches and subsidiaries on the introduced internal AML/CFT related procedures.
Conclusion	Poland has implemented Art. 34(2) of the Directive.
Recommendations and Comments	Not applicable

19.	Branches and subsidiaries (2)
Art. 31(3) of the Directive	The Directive requires that where legislation of a third country does not permit the application of equivalent AML/CFT measures, credit and financial institutions should take additional measures to effectively handle the risk of money laundering and terrorist financing.
FATF R. 22 and 21	Requires financial institutions to inform their competent authorities in such circumstances.
Key elements	What, if any, additional measures are your financial institutions obligated to take in circumstances where the legislation of a third country does not permit the application of equivalent AML/CFT measures by foreign branches of your financial institutions?
Description and Analysis	Pursuant to Para 2 and 3 of Art. 9j where there is no possibility to comply with the obligation set out in AML/CFT Act the financial institutions required to apply additional measures to effectively prevent money laundering and financing of terrorism, and shall inform the branches and affiliates about the introduced AML/CFT policies and internal procedures. Pursuant to Para 3 of Art. 10a the financial institutions required to conduct analysis to determine the geographical risk. So they are obliged to take particular account on risk sensitive basis when conducting a business activity in a country with insufficient AML/CFT regime. To inform the home country supervisor when the application of AML/CFT measures which are at least equivalent to those in force in Poland is not possible, is not reflected in the Polish legislation.
Conclusion	Art. 31 (3) of the EU Directive has been partially implemented by Poland. However it is not required to inform competent authorities about that, the legislation of a third country does not permit the application of equivalent AML/CFT measures by foreign branches.
Recommendations and Comments	Poland should take legislative measures to implement Article 31(3) of the EU Directive

20.	Supervisory Bodies
Art. 25 (1) of the Directive	The Directive imposes an obligation on supervisory bodies to inform the FIU where, in the course of their work, they encounter facts that could contribute evidence of money laundering or terrorist financing.
FATF R.	No corresponding obligation.
Key elements	Is Art. 25(1) of the Directive implemented in your jurisdiction?
Description and	According to Para 1 Art 15a the government and local government authorities, the other public organizational units, the NBP, the PFSA and

Analysis	the Supreme Chamber of Control within their statutory authority immediately notify the GIFI on any suspicion involving committing money laundering and terrorist financing. These "cooperating units" are required to set up and use written procedures for transmission of such information.
Conclusion	Art. 25 (1) of the EU Directive has been implemented in Poland.
Recommendations and Comments	Not applicable

21.	**Systems to respond to competent authorities**
Art. 32 of the Directive	The Directive requires credit and financial institutions to have systems in place that enable them to respond fully and promptly to enquires from the FIU or other authorities as to whether they maintain, or whether during the previous five years they have maintained, a business relationship with a specified natural or legal person.
FATF R.	There is no explicit corresponding requirement but such a requirement can be broadly inferred from Recommendations 23 and 26 to 32.
Key elements	Are credit and financial institutions required to have such systems in place and effectively applied?
Description and Analysis	According to Art. 13a of the AML/CFT Act at the written request of the GIFI, the financial institutions shall immediately disclose any information about the transactions covered by the provisions of the act. This information has to contain the information about the parties to the transaction, the balances and turnover of their accounts and the copies of other relevant documents. The General Inspector may request to be provided with the information electronically. Art. 9k of the AML/CFT Act provides for obligation to keep record of CDD and ECDD measures applied for 5 years from the first day of the year following the year in which the transaction was carried out. From the requirement to keep records on customer transactions to be produced immediately may be inferred that information on the name and nature of the business relationship with the customer in question is promptly available. It is not required by AML/CFT Act or any other law to store such information longer than 5 years upon the request of the GIFI or other competent authority.
Conclusion	Art. 32 of the EU Directive has been implemented in Poland.
Recommendations and Comments	Not applicable

22.	Extension to other professions and undertakings
Art. 4 of the Directive	The Directive imposes a *mandatory* obligation on Member States to extend its provisions to other professionals and categories of undertakings other than those referred to in A.2(1) of the Directive, which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes.
FATF R. 20	Requires countries only to consider such extensions.
Key elements	Has your country implemented the mandatory requirement in Art. 4 of the Directive to extend AML/CFT obligations to other professionals and categories of undertaking which are likely to be used for money laundering or terrorist financing purposes? Has a risk assessment been undertaken in this regard?
Description and Analysis	The provisions of the AML/CFT Act have been extended to other professionals and categories of undertakings than those referred to in Article 2 (1) of the Directive, namely: • entrepreneurs engaged in auction houses, • antique shops, • business factoring, • trading in metals or precious/semi-precious stones, • commission sale or real estate brokerage, • foundations, • associations with corporate personality.
Conclusion	Art. 4 of the EU Directive has been implemented in Poland.
Recommendations and Comments	Not applicable

23.	Specific provisions concerning equivalent third countries?
Art. 11, 16(1)(b), 28(4),(5) of the Directive	The Directive provides specific provisions concerning countries which impose requirements equivalent to those laid down in the Directive (e.g. simplified CDD).
FATF R.	There is no explicit corresponding provision in the FATF 40 plus 9 Recommendations.
Key elements	How, if at all, does your country address the issue of equivalent third countries?
Description and Analysis	According to the definition provided by AML/CFT Act the equivalent country is a third country which applies provisions on ML and FT in line with the AML/CFT regulation of the EU.

	The Para 1 and 2 Art 9d of the AML/CFT Act permits to apply SCDD measures when the client is an entity providing financial services and established in an equivalent third country, furthermore a company whose securities are admitted to public trading on a regulated market in at least one Member State or in an equivalent country. According to Art. 9i the obligated institution may rely on the result of CDD measures executed by another entity providing financial services from equivalent countries when conducting a transaction on the basis of an order or a disposition. The Polish AML/CFT Act addresses the third equivalent countries as far as it regards the concept of the beneficial owner in case of corporate entities Poland is a member to the Member States Common Understanding on the Procedure and Criteria for the Recognition of Third Countries' Equivalence. In full compliance with Common Understanding according to Para 6 of Art. 9d of the AML/CFT Act the Minister of Finance has issued the list of equivalent third countries.
Conclusion	The Polish AML/CFT provisions on equivalent third countries are in line with the Directive.
Recommendations and Comments	Not applicable

Annex to Compliance with 3rd EU AML/CFT Directive Questionnaire

Article 3 (6) of EU AML/CFT Directive 2005/60/EC (3rd Directive):

(6) "beneficial owner" means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:

(a) in the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25 % plus one share shall be deemed sufficient to meet this criterion;

(ii) the natural person(s) who otherwise exercises control over the management of a legal entity:

(b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:

(i) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity;

(ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(iii) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity;

Article 3 (8) of the EU AML/CFT Directive 2005/60EC (3rd Directive):

(8) "politically exposed persons" means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons;

Article 2 of Commission Directive 2006/70/EC (Implementation Directive):

Article 2

Politically exposed persons

1. For the purposes of Article 3(8) of Directive 2005/60/EC, "natural persons who are or have been entrusted with prominent public functions" shall include the following:

(a) heads of State, heads of government, ministers and deputy or assistant ministers;

(b) members of parliaments;

(c) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

(d) members of courts of auditors or of the boards of central banks;

(e) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(f) members of the administrative, management or supervisory bodies of State-owned enterprises.

None of the categories set out in points (a) to (f) of the first subparagraph shall be understood as covering middle ranking or more junior officials.

The categories set out in points (a) to (e) of the first subparagraph shall, where applicable, include positions at Community and international level.

2. For the purposes of Article 3(8) of Directive 2005/60/EC, "immediate family members" shall include the following:

(a) the spouse;

(b) any partner considered by national law as equivalent to the spouse;

(c) the children and their spouses or partners;

(d) the parents.

3. For the purposes of Article 3(8) of Directive 2005/60/EC, "persons known to be close associates" shall include the following:

(a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in paragraph 1;

(b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in paragraph 1.

4. Without prejudice to the application, on a risk-sensitive basis, of enhanced customer due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning of paragraph 1 of this Article for a period of at least one year, institutions and persons referred to in Article 2(1) of Directive 2005/60/EC shall not be obligated to consider such a person as politically exposed.

VI. LIST OF ANNEXES

Annex 1. Details of all Bodies met on the on-site visit

Ministries and other Government Authorities

Ministry of Finance

Ministry of Foreign Affairs

Ministry of Justice

Ministry of Economic Affairs

Ministry for Labour and Social Policy

Ministry for Administration and Digitisation

Ministry of Interior

Investigation and Law Enforcement Bodies and Public Prosecutor' Office

Department for Organized Crime and Corruption of the Prosecutor General's Office

Central Bureau of Investigation of the National Police Headquarters

Division for Fighting Organized Economic Crime

Criminal Office - Division for Fighting Economic Crimes

Asset Recovery Department

Financial Sector Bodies

Polish Financial Supervision Authority

Central Bank of Poland

National Savings and Credit Cooperative Union

Other Government Bodies

Central Anticorruption Bureau

Internal Security Agency (including the Counter-Terrorist Centre)

Inter-ministerial Committee of Financial Security

Inter-ministerial Team for Terrorist Threats (including Task Force – Permanent Group of Experts

Central Records and Information on Economic Activity

National Court Register

Private Sector Representatives and Associations

Polish Bank Association

Polish Insurance Association

National Chamber of Statutory Auditors

National Council of Notaries

Stock Exchange Company

Private Banks

Currency exchange services providers

Post office

Auditors and accounts

Lawyers and notaries

Casinos

Real estate agents

Annex 2. Key Laws, Regulations and other Documents

ACT on COUNTERACTING MONEY LAUNDERING AND TERRORISM FINANCING

of 16th November 2000

Chapter 1

General Provisions

Article 1. The Act lays down principles of and procedures for counteracting money laundering, counteracting terrorist financing, application of specific restrictive measures against persons, groups and entities, and obligations of entities involved in financial transactions in so far as collection and disclosure of information.

Article 2. Whenever the Act refers to:

1) obligated institution, it shall mean:

a) branches of a credit institution as defined in the Act of 29 August 1997 - Banking Law (Journal of Laws of 2002 No. 72 item 665, as amended)
b) any financial institution having its registered office in the territory of the Republic of Poland, branches of a financial institutions not having its registered office in the territory of the Republic of Poland as defined in the Act of 29 August 1997 - Banking Law,
c) national banks, branches of foreign banks as defined in the Act of 29 August 1997 – Banking Law,
d) the National Bank of Poland - in so far as the maintenance of bank accounts for legal entities, sale of coins, banknotes and numismatic items for collection and other purposes, gold buying and exchange of damaged legal tender under the Act of 29 August 1997 on the National Bank of Poland (Journal of Laws of 2005 No. 1 item 2, as amended)
e) electronic money institutions, branches of a foreign electronic money institution and any clearing agent operating under the Act of 12 September 2002 on electronic payment instruments (Journal of Laws No. 169 item 1385, as amended),
f) investment companies, custodian banks, as defined in the Act of 29 July 2005 on trading in financial instruments (Journal of Laws No. 183 item 1538, as amended),
g) foreign legal entities carrying out brokerage activities and commodity brokerage houses in the territory of the Republic of Poland as defined in the Act of 26 October 2000 on commodity exchanges (Journal of Laws of 2005 No. 121 item 1019, as amended), and any commercial companies referred to in Article 50a of the Act,
h) the National Depository for Securities S.A. – in so far as the maintenance of securities accounts or omnibus accounts,
i) entity operating in the field of games of chance, mutual betting and automatic machine games and automatic machines games of low prizes,
j) insurance companies in so far as life insurance, including any domestic insurer, main branches of an insurer from a non-EU member country, branches of an insurer from a EU-member country, life insurance intermediaries unless an insurer is responsible for their operations,
k) investment funds, investment fund management companies , as defined in the Act of 27 May 2004 on investment funds (Journal of Laws No. 146 item 1546, as amended)
l) cooperative savings and credit unions,

m) public operator within the meaning of the Act of 12 June 2003 - Postal Law (Journal of Laws of 2008 No. 189 item 1159; and of 2009 No. 18 item 97),
n) notaries in so far as notary's operations concerning trading in asset values, attorneys performing their profession, legal advisers practicing his profession outside their employment relationship with agencies providing services to the government authorities and local government units, foreign lawyers providing legal services apart from his employment, expert auditors, active tax advisers,
o) entities operating in so far as accounts bookkeeping services,
p) entities providing currency exchange operations,
q) entrepreneurs engaged in: auction houses, antique shops, business factoring, trading in metals or precious/semi-precious stones, commission sale or real estate brokerage,
r) foundations,
s) associations with corporate personality established under the Act of 7 April 1989 - Law of Associations (Journal of Laws of: 2001 No. 79 item 855; of 2003: No. 96 item 874; of 2004: No. 102 item 1055; and of 2007: No. 112 item 766) and receiving payments in cash of the total value equal to or exceeding the equivalent of 15.000 EURO, originating also from more than one operation,
t) entrepreneurs within the meaning of the Act of 2 July 2004 on freedom of economic activity (Journal of Laws of 2007 No. 155 item 1095, as amended), receiving payment for commodities in cash of the value equal to or exceeding the equivalent of 15.000 EURO, also when the payment for a given product is made by more than one operation,
u) payment institutions, branches of EU payment institutions, agencies of payment institutions and their agents within the meaning of the Act of 19 August 2011 on payment services (Journal of Laws No 199, pos. 1175);

1a) beneficial owner, it shall mean:

a) a natural person or natural persons who are owners of a legal entity or exercise control over a client or have an impact on a natural person on whose behalf a transaction or activity is being conducted,
b) a natural person or natural persons who are stakeholders or shareholders or have the voting right at shareholders meetings at the level of above 25% within such a legal entity, therein by means of block of registered shares, with the exception of companies whose securities are traded within the organised trading, and are subject to or apply the provisions of the European Union laws on disclosure of information, and any entities providing financial services in the territory of a EU-Member State or an equivalent state in the case of legal entities,
c) a natural person or natural persons who exercises control over at least 25% of the asset values - in the case of entities entrusted with the administration of asset values and the distribution of, with the exception of the entities carrying out activities referred to in Article 69 item 2 point 4 of the Act of 29 July 2005 on trading in financial instruments.

1b) entity providing financial services, it shall mean any obligated institution or another organization that has its legal address outside the territory of the Republic of Poland and which - on its own behalf and for its own account - under the authorization of a competent state-owned body exercising the supervision over such an entity, carries on business activities which include:

a) acceptance of deposits or other repayable funds,
b) granting credits,
c) conclusion of financial lease agreements,
d) granting guarantees and securities,
e) trading - on its own account or on its client's account - in money market instruments, foreign exchange, options and future contracts,
f) participation in issuing financial instruments and provision of services related to such issues ,

g) advisory services provided to companies on capital structure, industrial strategy and on mergers and acquisitions,
h) brokerage in the money market,
i) portfolio management or investment advisory services,
j) storage and administration of financial instruments,
k) rental of safe deposit boxes;

1c) shell bank, it shall mean an entity providing financial services or engaged in equivalent activities, established in the territory of a country in which it does not have any legal address, in such a manner that its actual management and administration are performed, and where such an entity is not affiliated with any financial group operating legitimately;

1d) economic relations, it shall mean any relations of the obligated institutions with clients related to economic activities within the meaning of the Act of 2 July 2004 on freedom of economic activity, and which - at the time of their establishment - indicate long-term cooperation;

1e) carry out a transaction, it shall imply to the execution of orders or instructions of a client by the obligated institution;

1f) politically exposed persons, it shall mean the following natural persons:

a) heads of state, heads of government, ministers, deputy ministers or assistant ministers, members of parliament, judges of supreme courts, constitutional tribunals and other judicial bodies whose decisions are not subject to further appeal with the exception of extraordinary measures, members of the court of auditors, members of central bank management boards, ambassadors, chargés d'affairs and senior officers of armed forces, members of management or supervisory bodies of state-owned enterprises – who hold or held these public functions, within a year since the day they ceased to meet the conditions specified in these provisions,
b) spouses of persons referred to in point (a), or persons staying with them in cohabitation, parents and children of the persons referred to in point (a) and the spouses of those parents and children or other persons staying in cohabitation with them,
c) who remain or remained in close professional or business co-operation with the persons referred to in point (a) and, or are co-owners of legal entities, and only ones entitled to assets of legal entities if they have been established for the benefit of those persons

- domicile outside the territory of the Republic of Poland;

2) transactions, it shall mean performing – on someone's own or on someone else's behalf, on someone's own or someone else's account:

a) deposits and withdrawals in cash or non-cash, including transfers of funds within the meaning of Article 2 point 7 of the Regulation No. 1781/2006, commissioned both in the territory of the Republic of Poland, and beyond it,
b) buying and selling foreign currency,
c) transfers of the ownership or transfers of possession of asset values, including putting such values into consignment or as colaterall , and transfer of asset values between bank accounts belonging to the same client
d) a claim for shares a claim for stock swap.

3) asset values, it shall mean means of payment, financial instruments within the meaning of Article 2, item 1 of the Act of 29 July 2005 on trading in financial instruments, as well as other securities or foreign exchange, property rights, movable asset values and immovable estate;

4) account, it shall mean any bank account, any account maintained at a financial institution, payment account in a payment institution, any account held in a credit institution, any account in a cooperative savings and credit union, any securities account and any omnibus account also any cash account within the meaning of the Act of 29 July 2005 on trading in financial instruments

used for their service, any registry of fund participants, any record of participants of an investment fund;

5) transaction suspension, it shall mean any temporary restrictions on administering and using asset values, preventing from the performance of a specific transaction by the obligated institution;

6) account blockage, it shall mean temporary restrictions on administering and using all the asset values collected on the account, therein also by the obligated institution, in case of the omnibus account the blockage might apply to certain asset values collected on the account;

6a) account freeze, it shall mean prevention against transmission, conversion and use of asset values or carrying out transactions in a manner that might change their volume, value, location, ownership, possession, nature, destination or against any other change which may enable using such asset values;

7) (revoked);

8) cooperating units – it shall mean any government and local government authorities and other public organizational units, as well as the National Bank of Poland, the Polish Financial Supervision Authority and the Supreme Chamber of Control;

9) money laundering, it shall mean any deliberate action such as:

a) conversion or transfer of asset values derived from criminal activity or from participation in such activity in order to conceal or disguise the illicit origin of asset values, or granting assistance to a person who participates in such activities in order to avoid legal consequences of actions undertaken by such a person,

b) concealment or disguise of the true nature of asset values or property rights associated with them, of their source, location, disposition and an event of their dislocation, being aware that these values are derived from criminal activity or participation in such activity,

c) acquisition, taking possession or use of asset values derived from criminal activity or participation in such an activity,

d) complicity, attempt to commit, aiding or abetting - in the cases of behaviour referred to in a) - c);

– even if the activities leading to attain those asset values were conducted in the territory of another country than the Republic of Poland;

10) terrorism financing, it shall mean an act referred to in Article 165a of the Act of 6 June 1997 - Penal Code (Journal of Laws No. 88 item 553, as amended);

11) equivalent country, it shall mean any country which is not a EU-member but applies provisions on money laundering and terrorist financing in line with the European Union law;

12) Regulation No 1781/2006, it shall mean the EC Regulation No. 1781/2006 of the European Parliament and the Council of 15 November 2006 on information on the payer accompanying transfers of funds (OJ L 345 of 08.12. 2006 point 1).

Article 2a. When determining the equivalent in EURO - as referred to in the Act – one shall apply the average rate announced by the National Bank of Poland for the currency in question at the day of the transaction or the day of disposal or the day of orderdering the transaction.

Chapter 2

Competent authorities responsible for counteracting money laundering and terrorist financing

Article 3. 1. A competent government authorities responsible for counteracting money laundering and terrorist financing, hereinafter referred to as "financial information authorities", shall be:

1) a minister competent for financial institutions as the supreme authority of financial information;
2) the General Inspector of Financial Information, hereinafter referred to as the "General Inspector".

2.The General Inspector shall be appointed and dismissed by the Prime Minister at the request of the minister competent for financial institutions.

3.The General Inspector is an Under-Secretary of State at the Ministry of Finance.

4.The General Inspector shall perform his duties with the assistance of an organizational unit established for this purpose within the structure of the Ministry of Finance.

5.The provisions of paragraph 1 do not infringe the provisions of the Act of 24 May 2002 on the Internal Security Agency and Intelligence Agency (Journal of Laws No. 74 item 676; and of 2003: No. 90 item 844, No. 113 item 1070 and No. 130 item 1188) defining duties of the Internal Security Agency and Intelligence Agency.

Article 4. 1. Duties of the General Inspector involve acquiring, collecting, processing and analysing information in the manner prescribed by law, and undertaking actions aimed at counteracting money laundering and terrorist financing, particularly:

10) investigation of the course of transaction, which has raised reasoned suspicions of the General Inspector;
11) carrying out of the procedure for transaction suspension or bank account blocking;
12) adjudicating on the release of frozen asset values;
13) disclosure of information on transaction or requesting for it;
14) submission of documentation supporting suspicion on the commitment for criminal offense to legitimate bodies;
15) initiating and undertaking other measures to counteract money laundering and financing terrorism, including training provided to the personnel of the obligated institutions within the responsibilities imposed on these institutions;
16) monitoring of compliance with legal regulations on counteracting money laundering and terrorist financing;
17) cooperation with foreign institutions and international organizations dealing with anti-money laundering or combating terrorist financing;
18) impose penalties as referred to in the Act.

2. Responsibilities of the authority referred to in Article 15 items 2 and 3 of the Regulation No. 1781/2006, are executed by the General Inspector.

Article 4a. 1. The General Inspector submits an annual report on his activities to the Prime Minister within 3 month after the end of the year in question which is subject to the report.

2. The report referred to in paragraph 1, includes in particular: the number of transaction reported by the obligated institutions, a description of actions undertaken in response to such notifications and the number of cases for which the proceeding was carried out, the number of persons who faced the allegation on having committed the crime referred to in Article 165a or Article 299 of the Penal Code, and number of persons convicted of crimes, with and without legal validity referred to in Article 165a and Article 299 of the Penal Code, and the evaluation of asset values in respect of

which either freezing, blockage, or suspension of transactions has been performed, or property seizure, confiscation or forfeiture has been adjudicated.

3. The Minister of Justice shall provide information to the General Inspector on the number of criminal prosecutions, the number of persons in respect to the proceedings instituted and convicted of crimes, with and without legal validity, referred to in Article 165a and Article 299 of the Penal Code, and on asset values in respect to which freezing, blocking, and suspension of a transaction has been performed, or property seizure, confiscation or forfeiture has been adjudicated - within 2 months after the end of the year in question and subject to the report.

4. After having submitted the report referred to in paragraph 1 to the Prime Minister, it shall be published by the minister competent for financial institutions on the website of the Public Information Bulletin of the Ministry of Finance.

Article 4b.1.The General Inspector shall be exempted from performing his responsibilities referred to in Article 18 and 18a, and Article 21 paragraph 1, if there appears a circumstance of such nature that it could raise doubts as to his impartiality.

2. Such an exclusion takes place at the written request of the General Inspector submitted to the minister competent for financial institutions.

3. In the event of such an exclusion of the General Inspector, his responsibilities are taken over by the minister competent for financial institutions.

Article 5. 1. The minister competent for internal affairs and the Head of the Internal Security Agency, in consultation with the minister competent for financial institutions, may delegate employees or officers of the subordinate units and bodies, or under their supervision, to work in a unit referred to in Article 3 paragraph 4.

2. Detailed terms and conditions for so delegated employees and officers of the units and bodies subordinate to the competent minister of internal affairs, or being under his supervision, are governed by separate regulations.

3. The Minister of National Defence, in consultation with the minister competent for the financial institutions, may designate regular soldiers to be on duty in a unit referred to in Article 3, paragraph 4.

4. The Prime Minister shall determine, by regulation, detailed terms and conditions on delegating officers of the Internal Security Agency, therein data which should be included in the application that the General Inspector moves for to delegate an officer taking under consideration: the position assigned to the person delegated; the scope of his/her duties and responsibilities on this position and the proposed salary; data that such an order for the secondment of personnel should include, therein conditions and time-limits of delegation; and also types of powers and welfare benefits available to the officer delegated, along with the arrangements for payment of salary and other monetary claims determining the distribution of salaries and monetary claims paid either by the organizational unit of the Internal Security Agency or the organizational unit to which the officer is assigned.

5. The minister competent for internal affairs, in consultation with the minister responsible for financial institutions, shall determine, by regulation, detailed terms and conditions of the deployment of employees of the bodies and authorities subordinate to him/her, therein data which should be included in the application that the General Inspector moves for to delegate an employee taking under consideration: the position assigned to the person delegated; the scope of his/her duties and responsibilities on this position and the proposed salary; data that such an order for the secondment of personnel should include, therein conditions and time-limits of delegation; and also types of powers and welfare benefits available to the officer delegated, along with the arrangements for payment of salary and other monetary claims determining the distribution of salaries and monetary claims paid

either by the organizational unit of the Internal Security Agency or the organizational unit to which the officer is assigned.

6. Detailed rules and procedures on the designation of regular soldiers to be on duty in a unit referred to in Article 3 paragraph 4, as well as detailed rules for granting salaries and other benefits inherent at the time of service in this unit are defined in the Act of 11 September 2003 on the military service of regular soldiers (Journal of Laws No. 179, item 1750).

Article 6. (revoked)

Article 7. 1. When an audit proceeding is being carried out under the scope and according to the principles defined by the Supreme Chamber of Control, the General Inspector provides the auditors with the information obtained within the course of execution of the duties referred to in Article 4, on the grounds of a separate authorization of the President of the Supreme Chamber of Control.

2. In the event of the audit carried out the Supreme Chamber of Control, Article 34 shall apply.

Chapter 3

Responsibilities of the obligated institution

Article 8. 1. Any obligated institution conducting a transaction exceeding the equivalent of 15.000 EURO is required to register such a transaction, also if it is carried out by more than one single operation but the circumstances indicate that they are linked and that they were divided into operations of less value with the intent to avoid the registration requirement.

1a. In case of casino operators under the provisions of the Gambling Act of 19 November 2009 (Journal of Laws, No. 201, item 1540) , the obligation referred to in paragraph 1 involves purchase or sale of gambling chips of the value equivalent to at least 1.000 EUR.

1b.The transactions referred to in paragraph 1a shall apply to the regulations on the transactions referred to in paragraph 1 accordingly.

1c. (revoked)

1d.(revoked)

1e.The obligation referred to in paragraph 1 shall not apply to:

1) transfers from a deposit account to a time deposit account belonging to the same client at the same obligated institution;
2) transfers to a deposit account from a time deposit account belonging to the same client at the same obligated institution;
3) incoming transfers with the exception of bank transfers from abroad;
4) transactions related to the internal management of the obligated institutions;
5) transactions concluded on the interbank market;
6) events defined in Articles 9d paragraph 1;
7) banks associating cooperative banks, provided the transaction has been registered in the associated co-operative bank;
8) transactions of temporary lien to secure asset values, conducted for the duration of the lien contract with the obligated institution.

2. (revoked)

3. Any obligated institution conducting a transaction, the circumstances of which may suggest that it was related to money laundering or terrorist financing, is required to register such a transaction, regardless of its value and character.

3a. In the event that the obligated institution does not accept the disposition or order to conduct a transaction, the obligation referred to in paragraph 3 shall also apply if this institution is aware of or - with due diligence - should be aware of such a transaction in regard to the contract with its client.

3b. Any obligated institutions that are attorneys, legal advisers and foreign lawyers shall exercise the obligation referred to in paragraph 3 when they participate in transactions related to the provision of assistance to their clients, which is planning or carrying out transactions relating to:

1) buying and selling real estate or business entities ;
2) money management, securities or other asset values;
3) opening accounts or their management;
4) arrangements of payments and extra payments to the initial or share capital, arrangements of contributions to create or conduct business operations of companies or for their administration;
5) creation and operation of entrepreneurs in a different form of business organization, and also the management of.

4. The register of transactions referred to in paragraphs 1 and 3 shall be stored for a period of 5 years, calculating from the first day of the year following the year in which transactions were recorded. In the event of liquidation, merger, division and transformation of any obligated institution, the provisions of Article 76 of the Act of 29 September 1994 on accounting (Journal of Laws of 2009 No. 152 item 1223, No. 157 item 1241 and No. 165 item 1316) shall be applied in regard to keeping records and documentation.

4a. Any information on the transactions carried out by the obligated institution and documents related to such a transaction are stored for a period of 5 years calculating from the first day of the year following the year in which the last record associated with the transaction took place.

4b. Provisions of paragraphs 4 and 4a shall apply to the information recorded under paragraphs 3a and 3b accordingly.

5. [(45)] The registration of transactions referred to in paragraph 1 shall not apply to the companies operating within real estate brokerage, electronic money institutions, foreign divisions of electronic money institutions, cash pool leaders, attorneys, legal advisers and foreign lawyers, and also auditors and tax consultants.

Article 8a. 1. Any obligated institution shall carry out ongoing analysis of the transactions carried out. Results of those analyses should be documented in paper or electronic form.

2. All the results of such analyses shall be kept for a period of 5 years, calculating from the first day of the year following the year in which they were conducted. In the event of liquidation, merger, division and transformation of any institution obligated to keep records, the provisions of Article 76 of the Act of 29 September 1994 on accounting shall apply accordingly.

Article 8b. 1. Any obligated institution shall apply financial security measures for its clients. Their scope is determined on the basis of risk assessment as for money laundering and terrorist financing, hereinafter referred to as "risk assessment", resulting from the analysis, taking into account in particular type of a client, economic relationships, products or transactions.

2. Financial security measures are not applied by:

1) the National Bank of Poland,
2) public operator referred to in Article 2 point 1 letter m) in the course of providing money transfer services.

3. Financial security measures referred to in paragraph 1, consist of:

1) client identification and verification of his identity on the basis of documents or information publicly available;
2) making attempts, with due diligence, in order to identify a beneficial owner and apply verification measures to identify the identity of, dependent on appropriate risk assessment, in order to provide the obligated institution with data required on the actual identity of a beneficial owner, including the determination of the ownership structure and dependence of the client;
3) obtaining information regarding the purpose and the nature of economic relationships intended by a client;
4) constant monitoring of current economic relationships with a client, therein surveying transactions carried out to ensure that transactions are in accordance with the knowledge of the obligated institution on the client and the business profile of his operations and with the risk; and, if possible, surveying the origins of assets and constant update of documents and information in possession.

4. Financial security measures are applied, in particular:

1) when concluding a contract with a client;
2) when carrying out transaction with a client with whom the obligated institution has not previously concluded any agreements of the equivalent of more than 15.000 EURO, regardless of whether the transaction is carried out as a single operation or as several operations if the circumstances indicate that they are linked;
3) when there is a suspicion of money laundering or terrorist financing regardless of the value of such a transaction, its organizational form and the type of a client;
4) when there are doubts raised that the previously received data referred to in Article 9 are authentic and complete.

5. In the event the obligated institution cannot perform its duties referred to in paragraph 3 points 1-3, it does not carry out the transaction, it does not sign the contracts with a client or it terminates the previously concluded contracts, and submits to the General Inspector, in accordance with the predetermined form, information about such client, along with the information on the specific transaction, , where appropriate, taking into account the risk of money laundering and terrorist financing.

6. Any obligated institution – at the request of the financial information authority and the authorities referred to in Article 21 paragraph 3 - presents its financial security measures applied in regard to the risk of money laundering and terrorist financing.

Article 9. 1. The identification, referred to in Article 8b paragraph 3 point 1, includes:

1) in case of natural persons and their representatives: determination and recording of the features of such a document confirming on the basis of separate provisions the identity of the person: the first and last name, nationality and address of the person performing the transaction; furthermore, his/her PESEL; or, if the person has no PESEL number, his/her date of birth or the number of an identity document confirming the identity of an alien, or a country code if it was a passport presented;
2) in case of a corporation: recording of current data from the extract of the Court Register or another document indicating the (company's) name and organizational form of such a legal entity, its registered office and address, its tax identification number along with the first and last name and the PESEL number of the person representing this legal entity - or in the case of a person with no PESEL number, his/her date of birth;
3) in the case of organizational units without legal status: recording of current data from a document indicating the name, the organizational form, the registered office and address, tax identification

number along with the first name, the last name and the PESEL number of the person representing this unit - or in the case of a person with no PESEL number, his/her date of birth;

2. The identification, referred to in Article 8b paragraph 3 point 1, shall also apply to transaction parties which are no clients and it includes determination and recording of their (companies') names or the first and last name and address, to the extent to which these data may be determined with due diligence by the obligated institution.

3. The identification, referred to in Article 8b paragraph 3 point 2, includes determination and record of the first and last name and address, along with other identifiers, referred to in paragraph 1 point 1, to the extent to which the obligated institution is able to determine it.

Article 9a. 1. The verification, referred to in Article 8b paragraph 3 points 1 and 2, consists of verifying and confirming data referred to in Article 9 paragraphs 1 and 3, and is performed before entering into a contract with a client or prior to the transaction.

2. The verification, referred to in Article 8b paragraph 3 points 1 and 2, may be completed after having established an economic relationship only if it is necessary to ensure further business operations and where there is little risk of money laundering or terrorist financing determined on the basis of relevant analysis performed.

3. In the case of insurance operations, within life insurance, the verification of identity of a policy's beneficiary or a policy's holder may be performed at the time of payment or prior to effecting it or when such a beneficiary or such a holder intends to exercise his/her rights under such an insurance policy.

Article 9b. 1. In justified cases, it is possible to open an account without satisfying the requirement referred to in Article 8b paragraphs 1-4.

2. In the case referred to in paragraph 1, effecting any transaction by means of an account is acceptable after the conclusion of a contract on conducting this account.

Article 9c. In the case of a casino operator or an entity running cash bingo room, within the meaning of the Gambling Act of 19 November 2009, the measures referred to in Article 8b paragraph 3 point 1 shall be applied at the entrance of a client to the casino or cash bingo room regardless of the value of gambling chips or cards purchased for gaming.

Article 9d. 1. Any obligated institution, taking into account the risk of money laundering or terrorist financing, may waive the application of Article 8b paragraph 3 points 1-3:

1) when its client is an entity providing financial services and established in the territory of a EU-Member State or an equivalent country;
2) in relation to:
   a) government bodies, local government authorities and execution bodies,
   b) life insurance policies, where an annual premium shall not exceed the equivalent of 1.000 EURO, or a single premium shall not exceed the equivalent of 2.500 EURO,
   c) an insurance policy consolidated with retirement insurance, provided that the terms and conditions of such a policy do not include a surrender clause , and that such a policy may not be used as a collateral for a loan or loans,
   d) electronic money, within the meaning of the Act of 12 September 2002 on electronic payment instruments, if the maximum amount stored in the device does not exceed:
      – the equivalent of 150 EURO - in the case of a device that cannot be recharged, or
      – the equivalent of 2.500 EURO per calendar year in question - in case of a device which can be recharged, provided that the redemption amount is at least the equivalent of 1.000 EURO per calendar year in question,

e) transactions where a payee is able by means of a unique reference number to monitor back to the payer the transfer of funds from a legal person, an organizational unit without legal status or a natural person, who has entered into agreement with a receipient for the supply of goods and services, even if transaction amount does not exceed the equivalent of 1000 EURO;

2. In the event that a client is a company whose securities are admitted to public trading on a regulated market in at least one European Union member state or in an equivalent country, the obligated institutions - taking into account the risk of money laundering or terrorist financing - may abridge the application of financial security measures to the cases and the measures set out in Article 8b paragraph 3 point 1 and paragraph 4 points 1 and 3.

3. In the cases referred to in paragraph 1 point 1 and points 2a and 2b, the obligated institution shall collect information to determine whether a client meets the requirements of these regulations.

4. To collect information, referred to in paragraph 3, Article 9k shall apply accordingly.

5. The minister competent for financial institutions may determine, by regulation, other categories of persons or activities than those specified in paragraphs 1 and 2, which are related to low risk of money laundering or terrorist financing, and for which it is possible not to apply the provisions of Article 8b paragraph 3 points 2-4 and paragraph 4 points 2 and 4, taking under consideration proper execution of required financial security measures by the obligated institution.

6. The minister competent for financial institutions shall define, by regulation, the list of equivalent countries, taking into account the necessity of ensuring correct implementation of security measures by the obligated institutions and of the assessment in so far as conformity of the state standards with money laundering and terrorist financing, established by international organizations.

Article 9e. 1. Any obligated institution shall apply - on the basis of risk analysis - increased security measures against a client in the events which may involve a higher risk of money laundering or terrorist financing and particularly in the cases referred to in paragraphs 2-5.

2. If the client is absent, the obligated institutions - for the purposes of identification – shall apply at least one of the following measures in order to reduce the risk:

1) establishment of the identity of the client on the basis of additional documents or information;
2) additional verification of the authenticity of the documents or attestation of their compliance with the original copies by a notary public, a government body, a local government authority or an entity providing financial services;
3) ascertainment of the fact that the first transaction was conducted via the client's account in the entity providing financial services.

3. In terms of cross-border relations with institutional correspondents from countries other than the EU-member states and equivalent countries, any obligated institutions being a provider of financial services shall:

1) collect information allowing to determine the scope of operations, and whether a provider of financial services is supervised by the state;
2) assess measures taken by a provider of financial services who is a correspondent in so far as counteracting money laundering and terrorist financing;
3) prepare documentation defining the scope of responsibilities of each provider of financial services;
4) ascertain with respect to payable-through accounts - that a provider of financial services, who is a correspondent, conducted the verification of identity and has taken appropriate actions under procedures on the application of financial security measures in relation with clients having direct access to such a correspondent's bank accounts and that it is able to provide, on demand of the correspondent, any data related to the application of financial security measures in regard to a client;

5) establish cooperation, with the prior consent of a board of directors or a designated member of such a board or a person designated by such a board; or a person designated in accordance with Article 10b paragraph 1.

4. With regard to the politically exposed persons, the obligated institutions:

1) implement procedures based on risk assessment to determine whether such client is a person holding a politically exposed position;
2) apply measures, adequate to the risk determined by this obligated institution, in order to establish the source of asset values introduced to trading;
3) maintain constant monitoring of conducted transactions;
4) conclude a contract with a client after having obtained the consent of the board, the designated member of the management board or a person designated by the board or a person responsible for the activities of the obligated institution.

5. The obligated institutions may collect written statements on whether a client is a person holding a politically exposed position, which are given under the penal liability for providing data incompatible with the facts.

Article 9f. 1. No obligated institution, which is a provider of financial services, shall establish and maintain cooperation within correspondent banking with a shell bank.

2. No obligated institutions shall establish and maintain cooperation within correspondent banking with any obligated institution which is a provider of financial services concluding contracts on accounts with a shell bank.

Article 9g. Any obligated institutions shall apply appropriate measures of financial security in order to prevent money laundering or terrorist financing, which may arise from products or transactions allowing to maintain anonymity.

Article 9h. Each obligated institutions may rely on other entities in so far as the implementation of the obligations set out in Article 8b paragraph 3 points 1-3. The responsibility for such an implementation shall remain with the obligated institution.

Article 9i. 1. Any obligated institution conducting a transaction on the basis of an order or a disposition accepted or received by an entity providing financial services - having its legal address within the territory of the EU-member state or an equivalent country - may recognise the obligations referred to in Article 8b paragraph 3 points 1-3 as executed provided that it has assured the submission of copies of documents or information confirming the application of financial security measures at each request of the obligated institution.

2. At the request of the institution conducting the transaction, the obligated institution accepting an order or disposition makes copies of the documents and information referred to in paragraph 1 immediately accessible.

3. The obligated institution shall not apply the provisions of paragraph 1, where financial security measures have been implemented by an entity providing financial services connected to the transfer of funds.

4. In order to disclose the information referred to in paragraph 1, the provisions limiting disclosure of information covered by secrecy protected by law and resulting from relevant provisions because of the type of operations carried out by the obligated institution shall not apply.

Article 9j. 1. Any obligated institution with its branches and subsidiaries in the territory of non-EU member states shall apply the financial security measures defined in the Act in those branches and subsidiaries.

2. In the absence of the possibility to fulfil obligation referred to in paragraph 1, any obligated institution shall carry out all the activities in order to effectively counteract money laundering and terrorist financing as provided for in the legislation of the countries referred to in paragraph 1.

3. Any obligated institution shall inform its subsidiaries and affiliates, referred to in paragraph 1, on any introduced internal procedures focused on counteracting money laundering and terrorist financing.

Article 9k. Information obtained as the result of the application of the measures referred to in Articles 8b and 9e is stored for a period of 5 years from the first day of the year following the year in which the transaction was carried out with the client. In the event of liquidation, merger, division or transformation of an obligated institution, the provisions of Article 76 of the Act of 29 September 1994 on accounting shall apply to the storage of documentation.

Article 10 (revoked).

Article 10a. 1. Any obligated institutions shall introduce a written internal procedure on counteracting money laundering and terrorist financing.

2. Such an internal procedure, referred to in paragraph 1, should contain, in particular, the determination of how the financial security measures shall be implemented, transactions registered, analyses performed and risk assessed, transaction information transmitted to the General Inspector, the suspension of transactions, account blocking and account's freezing carried out, and the manner in which the statements referred to in Article 9e point 5 received, if they are received, and how the information is stored.

3. When conducting analysis to determine risk value, any obligated institution should , in particular, include the criteria of the following nature:

1) economic - involving assessment of client's transaction in terms of its business activity;
2) geographic - involving performance of transactions unwarranted by the nature of business activity, concluded with the operators of the countries where there is a high risk of money laundering and terrorist financing;
3) objective - involving business activities of high-risk conducted by the client in terms of vulnerability to money laundering and terrorist financing;
4) behavioural - involving unusual behaviour of the client, in the situation in question.

4.Any obligated institution assures the participation of the employees, who perform duties related to counteracting money laundering and terrorist financing in this obligated institution, in training programs related to these duties.

Article 10b. 1. Any obligated institutions designates persons responsible for fulfilling the obligations specified in the Act. In the obligated institutions that are commercial capital companies, cooperative or state banks, the person responsible for fulfilling the obligations specified in the Act is a board member appointed by the management board, and in the obligated institutions, which are branches of foreign banks or credit institutions, it is a director of the branch.

2. When the obligated institutions exercises its business activity individually, a person responsible is a person performing this activity.

3. The provision of Article 10a shall apply accordingly to any obligated institution exercising its business activities individually.

Article 10c. 1. The provisions of Regulation No 1781/2006 shall not apply where a payment service provider of the recipient is able - by means of a unique reference number - to monitor back all the transfers of funds to the payer originating from a legal entity, an organizational unit without legal

personality or a natural person, who has concluded a contract for the supply of goods and services with the recipient, even if amount of such a transaction does not exceed the equivalent of 1.000 EURO.

2. The provision of Art. 5 of Regulation No 1781/2006 shall not apply to a payment service provider having their legal address in the territory of the Republic of Poland with reference to transfers of funds to non-profit organizations, exercising charitable, religious, cultural, educational, social, scientific activities, if the transfer of funds does not exceed the equivalent of 150 EURO and takes place only in the territory of the Republic of Poland.

Article 10d.(64) Any obligated institution which are attorneys, legal advisers or foreign lawyers shall not apply the provisions of Article 8a, Article 8b paragraph 3 point 2-4, Article 9e paragraphs 1-3, Articles 9f-9j, Article 10a paragraphs 1-3, Articles 10b paragraph 1, and of Article 10c.

Chapter 4

Principles for providing information to the General Inspector

Article 11. 1. Any obligated institution provides information on transactions registered in accordance with Article 8 paragraphs 1 and 3 to the General Inspector. Such a provision involves sending or delivering data from the register of transactions referred to in Article 8 paragraph 4, also using computer data storage carriers.

2. (revoked).

3. Such information on transactions referred to in Article 8 paragraph 1 may be forwarded to the General Inspector through the agency of chambers of commerce associating obligated institutions and banks associating co-operative banks.

4. Information on the transactions referred to in Article 8, may be forwarded to the General Inspector through the agency of a territorially competent body of professional self-management of notaries, attorneys, legal advisers and foreign lawyers, if a national body of such a self-management body adopts a resolution determining detailed rules and a course of provision of such information to the General Inspector. Then the national self-management body submits the list of persons responsible for providing such information to the General Inspector.

5. The obligation to provide information on transactions covered by the provisions of the Act does not apply if lawyers, legal advisers and foreign lawyers, auditors and tax advisers represent their client on the basis of a power of attorney related to proceedings pending or provide advice for the purpose of such a proceeding.

Article 12 1. Information on the transactions recorded in accordance with Article 8 paragraphs 1 and 3 shall include in particular the following data:

1) trade date;
2) identification data of the parties to the transactions referred to in Article 9 paragraphs 1 and 2;
3) the amount, currency and type of the transaction;
4) numbers of account used to conduct the transaction if the transactions involved such accounts;
5) (revoked);
6) (revoked);
7) substantiation along with the place, date and manner of placing disposition in the event of providing information on the transactions referred to in Article 8, paragraph 3.

2. Information on the transaction registered in accordance with Article 8 paragraph 1 and 3, containing information specified in paragraph 1, shall be forwarded to the General Inspector:

1) within 14 days after the end of each calendar month - in the case of the transactions referred to in Article 8, paragraph 1;
2) immediately - in the case of the transactions referred to in Article 8, paragraph 3.

3. The provision of paragraphs 1 point 2 shall not apply to the transactions conducted on the regulated marked within the meaning of the Act of 29 July 2005 on trading in financial instruments, with respect to the identification data of the party not being a client of this transactions.

Article 12a. In the case of transactions referred to in Article 8 paragraph 3, the obligated institution shall provide additional data in its possession about the parties of transactions, including information on their personal accounts and related to their business activity, not used in the subject transaction.

Article 13 The minister competent for financial institutions, in consultation with the minister competent for internal affairs, and after consultation with the President of the National Bank of Poland, determines, by regulation:

1) the form of the register referred to in Article 8 paragraph 4, the method of its conducting and the procedure for delivery of data from the register to the General Inspector;
2) the procedure for providing information on the transactions referred to in Article 8 paragraphs 1 and 3 to the General Inspector, when using computerized data storage carriers.

Article 13a. 1. At the written request of the General Inspector, any obligated institution shall immediately disclose any information about the transactions covered by the provisions of the Act. Such a disclosure consists in particular the provision of information about the parties of transaction, the content of documents, including the balances and turnovers on the account, provision of certified copies of theirs, or a disclosure of relevant documents for insight of the authorized employees of the unit referred to in Article 3 paragraph 4 in order to produce notes or copies.

2. The information referred to in paragraph 1, shall be forwarded to the General Inspector free of charge.

3. The General Inspector may request to be provided with the information referred to in paragraph 1 in an electronic manner.

Article 14. 1. (revoked).

2. The Prosecution Office, the Internal Security Agency, the Central Anticorruption Bureau and the units subordinated to the minister competent for internal affairs and supervised by him shall immediately inform the General Inspector, within the limits of its statutory authority, on all the cases involving:

1) receipt of information indicating suspicion of crimes having been committed as referred to in Article 165a and Article 299 of the Penal Code, in the form of a summary statement, not later than the end of the month following the month in which the information was obtained;
2) presentation of charges relating to the commitment of the crime referred to in Article 165a and Article 299 of the Penal Code;
3) initiation and completion of proceedings on the crime referred to in Article 165a and Article 299 of the Penal Code.

3. The information, referred to in paragraph 2, must indicate, in particular, the circumstances relating to the commitment of the crime and to the persons participating in it.

4. The General Inspector shall immediately notify the authorities referred to in paragraph 2 of the circumstances indicating the connection between the information obtained in the manner specified in this provision, and information on the transactions referred to in Article 8 paragraph 3, Article 16 paragraphs 1 and 1a, and Article 17.

Article 15 At the request of the General Inspector, all the cooperating units are obliged to provide, within their statutory authority, any information necessary to carry out his tasks in the field of prevention as referred to in Article 165a and Article 299 of the Penal Code.

Article 15a. 1. Within their statutory authority, the cooperating units, with the exception of the bodies referred to in Article 14 paragraph 2, are obliged to cooperate with the General Inspector within the prevention of the crimes referred to in Article 165a and Article 299 of the Penal Code, and to:

1) immediately notify the General Inspector on any suspicion involving committing money laundering and terrorist financing;
2) submit certified copies of documents relating to the transactions for which there is a suspicion that they are related to the commitment of crimes referred to in Article 165a and Article 299 of the Penal Code, along with the information on the parties of such transactions.

2. Any cooperative units are required to develop a manual of procedures to be carried out in the cases referred to in paragraph 1.

3. An fiscal control authorities, tax authorities and customs authorities shall immediately notify the General Inspector of any circumstances disclosed in the course of their business operations that may indicate activities aimed at the commitment of crimes referred to in Article 165a and Article 299 of the Penal Code.

4. The notification referred to in paragraph 1 point 1 and paragraph 3 should include, in particular, a description of the circumstances disclosed, along with the reasons why the notifier concluded that they might have been involved in carrying out activities aimed at the commitment of a crime referred to in Article 165a and Article 299 of the Penal Code.

5. The Border Guard and the Customs authorities shall provide the General Inspector with the information referred to in Article 5 of 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 (OJ L 309, 25.11.2005, point 9), and with the information contained in the declaration referred to in the regulations issued under Article 21 of the Act of 27 July 2002 - Foreign Exchange Law (Journal of Laws No. 141 item 1178, as amended). This information is provided accordingly through the agency of the Chief Commander of the Border Guard or the Head of the Customs Service within 14 day of the month following the month in which the import of cash in the territory of the Republic of Poland, or export of funds from the territory of the Republic of Poland, has been performed.

6. The minister competent for financial institutions shall define, by regulation, the form and the manner of providing the information referred to in paragraph 5, taking into account the necessity for efficient provision of information collected by the Border Guard and the Customs Authorities to the General Inspector.

Article 15b. In reasoned cases, the General Inspector may request the tax authorities or the fiscal control authorities to investigate the legality of origin of certain asset values. The information on the results of the activities conducted shall be submitted to the General Inspector without delay.

Chapter 5

Procedure for transaction suspension and account blockage

Article 16. 1. Any obligated institution which received a disposition or an order of the transactions, or carried out such a transaction, or has any information about the intention to carry out such a transaction, for which there is a reasoned suspicion that it may be related to the criminal offense referred to in Article 165a and Article 299 of the Penal Code, is obliged to inform to the General Inspector in writing by passing all the data referred to in Article 12 paragraph 1 and Article 12a along with the indication of prerequisites in favour of suspension of the transaction or blockage of the account, and to indicate the expected date of the implementation. The provision of Article 11 paragraph 4 shall not be applied.

1a. Where the obligated institution, making the notification pursuant to paragraph 1, is not the institution which is to carry out the transaction, the notice shall also indicate the institution, which is to transact.

2. Upon the receipt of the notice, the General Inspector shall promptly confirm the receipt thereof in writing, stating the date and the time of collection of the notice.

3. Such a notification and a confirmation referred to in paragraphs 1 and 2 may be also provided on the information storage carrier.

4. Pending such a receipt of the request referred to in Article 18 paragraph 1, but no longer than for 24 hours after the confirmation of the receipt of the notification referred to in Article 16 paragraph 2, the obligated institution shall not carry out the transaction covered by the notice.

Article 16a. (revoked).

Article 17. If the notice, referred to in Article 16 paragraph 1, can not be made before performing - or during performing - a disposition or an order to carry out the transactions, the obligated institution shall provide the information about the transaction immediately after its completion, giving the reasons for the prior absence of such a notice.

Article 18. 1. If from the notice referred to in Article 16 paragraph 1, it follows that the transaction to be carried out may be related to any criminal offense referred to in Article 165a and Article 299 of the Penal Code, The General Inspector may - within 24 hours of the date and time indicated on the confirmation referred to in Article 16 paragraph 2 - provide the obligated institution with a written request to suspend the transaction or block the account for no more than 72 hours from the date and time indicated on the confirmation thereof. At the same time, the General Inspector shall notify the competent public prosecutor on a suspicion of having committed a crime and shall provide him with any information and documents concerning the suspended transaction or the account blocked.

2. The request to suspend the transactions or to block the account may be issued only by the General Inspector, or a total of two employees of the unit, as referred to in Article 3 paragraph 4, authorized by the General Inspector in writing.

3. The transaction is suspended or the account blocked by the obligated institution immediately upon the receipt of the request referred to in paragraph 1.

4. The suspension of the transactions or the blockage of the account by the obligated institution, in the manner specified in paragraphs 1 and 3, shall not arouse any disciplinary, civil, criminal, or otherwise specified responsibility defined by separate provisions.

5. Saturdays, Sundays and public holidays shall not be included in the time limits referred to in paragraph 1.

Article 18a. 1. The General Inspector may submit a written request to the obligated institution to suspend a transaction or block the account without having previously received the notification referred to in Article 16 paragraph 1, if the information in possession of which he is indicates the conduct of activities aimed at money laundering or terrorist financing.

2. In the case referred to in paragraph 1, the General Inspector may request the suspension of a transaction or block the account for no more than 72 hours after the receipt of the request by the obligated institution.

3. The provisions of Articles 18, 19 and 20 shall apply accordingly.

Article 19 1. In the event that the General Inspector receives the notification referred to in Article 18 paragraph 1 second sentence, the prosecutor may order, by decision, to suspend this transaction or block the account for a definite period, but no longer than 3 months from the day of the receipt of this notification.

2. In the decision referred to in paragraph 1, the General Inspector defines the scope, manner and time-limits of the suspension of the transaction or the blockage of the account. The decision may be appealed to the court competent to hear the case.

3. (revoked).

4. The suspension of transactions or the blockage of the account falls if before the expiry of 3 months from the receipt of the notification referred to in Article 18 paragraph 1 second sentence, a decision on asset values freezing will not be issued.

5. In the matters regarding suspension of transactions or account blocking not regulated by the Act, the provisions of the Code of Criminal Procedure shall apply.

Article 20 In the event that the account has been blocked or the transaction has been suspended with the breach of the law, the liability for damages resulting from it is borne by the Treasury under the terms defined in the Civil Code.

Article 20a. (revoked).

Article 20b. The provisions of Articles 19 and 20 also apply accordingly to pending criminal proceedings brought for a crime listed in Article 165a of the Criminal Code, when the notification received by the prosecutor comes from other sources.

Article 20c. Any obligated institution, at the request of the party ordering the transaction or of the account holder, can inform the party about the suspension of the transaction or the account blockage and indicate the authority which has requested for it.

Chapter 5a

Specific restrictive measures against persons, groups and entities

Article 20d. 1. Any obligated institution shall perform freezing of the asset values with due diligence, with the exception of movable and immovable property, on the basis of:

3) the European Union legislature imposing specific restrictive measures directed against certain persons, groups or entities, and

4) regulations issued pursuant paragraph 4.

2. Any obligated institution, while performing such freezing, submits all the data in its possession and related to the freezing of asset values to the General Inspector, electronically or in paper form.

3. The provision of Article 20 shall apply accordingly for freezing asset values.

4. The minister competent for financial institutions - in consultation with the minister competent for foreign affairs - may indicate, by regulation, persons, groups or entities which are subject to such freezing as referred to in paragraph 1, taking into account the necessity to comply with the obligations under international agreements or resolutions of international organizations binding the Republic of Poland, and bearing in mind the necessity of combating terrorism and counteracting terrorism financing.

5. Hereby, the Inter-Ministerial Committee of Financial Security is established, hereinafter referred to as "the Committee", acting under the auspices the General Inspector. The Committee acts as a consultative and advisory body within the scope of application of specific restrictive measures against persons, groups and entities.

6. The objective of the Committee shall be, in particular, to present proposals on the inclusion or removal of persons, groups or entities from the list of persons, groups or entities referred to under paragraph 4.

7. The Committee shall consist of the representatives of:

1) the minister competent for financial institutions;
2) the minister competent for public finance,
3) the minister competent for foreign affairs,
4) the Minister of Justice,
5) the Minister of National Defence;
6) the minister competent for internal affairs;
7) the minister competent for economy;
8) the President of the Polish Financial Supervision Authority;
9) the President of the National Bank of Poland,
10) the Head of Internal Security Agency;
11) the Head of the Central Anti-Corruption Bureau;
12) the General Inspector.

8. The bylaw on the operating mode and work procedures of the Committee shall be set out by the Committee.

9. Any person, group or entity on the list, provided under paragraph 4, may step forward with a justified motion to the minister competent for financial institutions, for the removal from the list. Such a motion is subject to the opinion given at the immediate meeting of the Committee.

10. In the case of freezing asset values based on the list of persons, groups or entities referred to under paragraph 4, the General Inspector shall - if it is possible - immediately inform the person, the group or the entity whose asset values has been frozen on the fact. Such information should include justification of the act of freezing funds as well as an instruction on how to take further actions in order to be removed from the list, appeal or nullify freezing of asset values.

Article 20e. 1. In the event of freezing asset values, any person, group or entity which:

1) is not mentioned in the acts of the European Union implementing specific restrictive measures or on the list of persons, groups or entities referred to under Article 20d paragraph 4, or
2) is in a difficult life or material situation

- such a person, group or entity may request the General Inspector to be released from freezing of asset values.

2. In the event referred to in paragraph 1 point 1 the total release from freezing asset values shall be determined.

3. In the event referred to paragraph 1 point 2, provided the minister responsible for foreign affairs does not object, and after consulting the Committee, the General Inspector may determine a total or a partial release from freezing asset values, if it is not contrary to the binding resolutions of international organizations.

4. The objection referred to in paragraph 3, is filed, by decision, within 14 days since the receipt of the argument of the General Inspector. In particularly substantiated cases, the General Inspector, at the request of the minister for foreign affairs, extends the deadline for motion filing to 30 days from the date of the receipt of the argument from the General Inspector.

5. In the case referred to in paragraph 1 point 1, the General Inspector shall decide on the release from freezing asset values ex officio.

6. In order to establish the facts and circumstances referred to in paragraph 1, all the cooperating units are required to provide all their assistance, including the submission of the copies of any necessary documents.

7. The decision on the release from freezing asset values shall be by decision of the General Inspector.

8. The appeal against the decision of the General Inspector referred to in paragraph 7, shall be filed to the minister competent for financial institutions within 14 days after the receipt of the notification about this decision.

9. The proceedings shall unfold according to the provisions of the Code of Administrative Procedure.

10. The decision made by the minister competent for financial institutions may be appealed at the administrative court.

Chapter 6

Control of obligated institutions

Article 21. 1. The control of compliance of the obligated institutions – except from the National Bank of Poland – with the obligations within counteracting money laundering and terrorist financing is exercised by the General Inspector.

2. Such an control shall be carry out by employees of the unit, referred to in Article 3 paragraph 4, hereinafter referred to as "inspectors", authorized in writing by the General Inspector, following the presentation of an auditor business identification card, hereinafter referred to as the "inspector's ID", and a written authorization.

3. The control referred to in paragraph 1 may also be carried out, within the frameworks of the surveillance and control performed on terms and procedures specified in separate provisions, by:

1) the President of the National Bank of Poland - in relation to currency exchange operators;
2) the Polish Financial Supervision Authority;
3) the competent heads of custom offices - in relation to operators organizing and exercising games of chance, mutual bets, and operations involving automatic machine games and automatic machine games of low prizes;
4) presidents of appeal courts – in relation to notaries public;

5) the National Savings and Credit Cooperative Union;
6) competent voivods and governors - in relation to associations;
7) tax audit authorities.

3a. Imposing penalties relating to the violations identified by the control, referred to in paragraph 3, falls within the jurisdiction of the General Inspector.

3b. Any entity, mentioned in point 3, submits its schedules of controls to the General Inspector within two weeks following their completion.

3c. At the request of the minister competent for public finance, the General Inspector shall carry out control as referred to in paragraph 1- in relation to obligated institution applying for license or permit, provided for in Gambling Act of 19 November 2009.

4. A written report about the results of the control referred to in paragraph 3, within compliance with the provisions of the Act, shall be forwarded to the General Inspector within 14 days following its completion.

4a. The General Inspector may request the entities listed in paragraph 3, to provide certified copies of the documentation collected during an audit.

5. The minister competent for financial institutions shall stipulate, by regulation, the standard pattern form of the inspector's ID and shall determine the rules for its issuance and replacement.

Article 22. 1. At the request of an inspector, any obligated institution is required to disclose all the documents and materials necessary within the course of the audit referred to in Article 21 paragraph 1, with the exception of documents and materials containing classified information.

2. Any obligated institution shall provide proper conditions for carrying out a control, in particular: the immediate presentation of the documents requested and materials for their inspection and timely delivery of explanations by the staff of the unit.

3. The inspectors shall be entitled to:

1) access the facilities and premises of the obligated institution in the presence of the body under inspection;
2) have insight to documents and to other evidence documentation covered by the scope of the control and to obtain their certified copies;
3) demand oral and written explanations, within the range of the control, from the employees of the obligated institution.

4. The inspectors, in the course of performing control activities, have right to the protection provided for in the Penal Code for public servants.

Article 23. Each inspector is authorized to move freely within the premises of the obligated institution without having to obtain a pass and is not subject to personal control.

Article 24. 1. The director of the unit, referred to in Article 3 paragraph 4, presents, in a post-control protocol, the results of the control to the head of the obligated institution or a person authorized by the latter within 30 days from the date of the control completion.

1a. Prior to the presentation of the final post-control protocol, the director of the unit, referred to in Article 3 paragraph 4, may apply to the obligated institution to submit, within the prescribed period of time, additional clarification in writing in regard to any irregularities found during the inspection.

1b. The period specified in paragraph 1 does not include the period from the date of dispatch of the letter referred to in paragraph 1a, to the date of the receipt of additional explanation.

2. Such a post-control protocol includes findings of fact, evaluation of the controlled operations, including any irregularities concluded and the indication of persons responsible for them, and conclusions and recommendations following the control.

Article 25. 1. Any obligated institution is entitled to notify the General Inspector of any reasoned objections to the findings contained in the post-control protocol.

2. Any objections shall be reported in writing to the General Inspector within 14 days after the receipt of the post-control protocol.

3. After having considered the objections, the General Inspector shall submit his written opinion to the applicant of such an objection within 30 days since the receipt thereof.

4. The obligated institution shall send to the director of the unit referred to in Article 3 paragraph 4, within the term indicated in the post-control protocol, the information on the manner the post-audit recommendations have been executed or reasons for their failure indicating the anticipated date of their execution.

5. In the case any objections under paragraph 1 have been lodged, the deadline referred to in paragraph 4 is calculated from the date of the receipt of the opinion of General Inspector.

Article 26. (deleted).

Article 27. The written information on the results of the control referred to in Article 21 paragraph 1 shall be submitted by the General Inspector to:

1) the authorities exercising supervision over the obligated institutions;
2) the authority appointed to prosecute crimes and offenses, in the event of any reasoned suspicion of the commitment a crime or an offense.

Chapter 7

Protection and disclosure of collected data

Article 28. (revoked).

Article 29. In order to disclose any information in the manner and extent provided by the Act to the General Inspector, the regulations restricting the disclosure of confidential information shall not apply to, except the classified information.

Article 30. Any information received and provided by the financial information authority, as provided for in the Act, shall be subject to the protection as required by separate laws governing the rules for their protection.

Article 30a. 1. The financial information authority, employees and persons performing activities for the unit referred to in Article 3 paragraph 4, are required to maintain the confidentiality of the information that was disclosed to them in the course of their operations in accordance with the principles and procedures specified in separate regulations.

2. Maintenance of confidentiality referred to in paragraph 1 applies even after the termination of the employment in the unit referred to in Article 3 paragraph 4, and even if the activities were performed on its behalf on the basis of civil law contracts.

Article 31. 1. If the suspicion of having committed any crime referred to in Article 165a and Article 299 of the Penal Code, results from the information in possession of the General Inspector, its

processing or analysis, the General Inspector shall notify the public prosecutor on a suspicion of crime commitment and at the same time shall provide him with the evidence supporting this suspicion.

2. Where the basis of the notification referred to in paragraph 1 had been the information on the transaction - as referred to in Article 8 paragraph 3, Article 16 paragraph 1, or Article 17 - provided by the obligated institution or a cooperating unit, as referred to in Article 15a paragraph 1, the General Inspector shall submit the information on that fact to it, no later than within 90 days from the submission of this notification.

Article 32. 1. Any information collected in the manner and within the scope of the provisions of the Act is disclosed for the purposes of criminal proceedings to the courts and prosecutors - at their written request - by the General Inspector.

2. In order to verify data contained in the notification related to the suspicion of a crime commitment, referred to in Article 165a and Article 299 of the Penal Code, the prosecutor may request the General Inspector to provide information protected by law, including bank or insurance secrecy, also during the verifying proceeding conducted pursuant to Article 307 of the Code of Criminal Procedure.

3. If the General Inspector is not in possession of information enough to let the prosecutor issue the order in the subject matter of the initiation of preliminary proceedings relate to the case of a crime referred to in Article 165a and Article 299 of the Penal Code, the request referred to in paragraph 2 can be directed to the obligated institution.

Article 33 1. The General Inspector shall submit, with reservation to paragraph 1a, the information in his possession on the written and reasoned request of:

1) the minister competent for internal affairs or persons authorized by him,

1a) the Head of the Customs Service or persons authorized by him – only to the extent of performing duties of the Customs Service,

2) the Heads: the Internal Security Agency, the Intelligence Agency, the Military Counter-Intelligence Service, the Military Intelligence Service and the Central Anti-Corruption Bureau or any persons authorized by them

- in terms of their statutory powers.

1a. The information referred to in Article 8 paragraph 1 is submitted by the General Inspector to the minister competent for internal affairs and the Heads: the Internal Security Agency, the Intelligence Agency, the Military Counter-Intelligence Service, the Military Intelligence Service and the Central Anti-Corruption Bureau, at their written and reasoned request made with the consent of the Attorney General.

2. Information about the transactions covered by the provisions of the Act may be disclosed by the General Inspector at the written and reasoned request of:

1) the General Inspector of Fiscal Control, directors of fiscal chambers and the directors of the fiscal control offices - only to the extent of their statutory duties;

1a) the Head of Custom Service or any persons authorized –only to the extent of Custom Service duties;

2) the President of the Polish Financial Supervision Authority or persons authorized by him - only in matters related to the exercise of banking supervision, in matters relating to the exercise of supervision over the insurance activities and investment firms and custodian banks - within the meaning of the Act of 29 July 2005 on trading in financial instruments, foreign legal entities performing brokerage activities in the territory of the Republic of Poland in the field of trading in

stock exchange commodities of commodity brokerage houses for the purposes of the Act of 26 October 2000 on commodity exchanges, in relation to investment funds, investment fund management companies and the National Depository for Securities S.A., and in relation to payment institutions, branches of EU payment institutions, agencies of payment services and their agents, within the meaning of the Act of 19 August 2011 on payment services;,

3) directors of customs chambers - only in matters concerning the enforcement of customs debt and tax liabilities resulting from the economic exchange with foreign countries;
4) (revoked);
5) (revoked);
6) (deleted);
7) the President of the National Savings and Credit Cooperative Union or persons authorized by him - only in matters related to the exercise of supervision over the activities of cooperative savings and credit funds;
8) (revoked);
9) (deleted);
10) the President of the Supreme Chamber of Control – to the extent necessary to carry out auditing procedures.

3. In the events defined in paragraphs 1 and 2, the General Inspector may provide information on the transactions covered by the provisions of the Act, on his own initiative.

4. In terms of information covered by banking secrecy, the General Inspector shall provide and disclose information to the bodies referred to in paragraph 2 in accordance with the scope of powers and the procedure set out in the Act of August 29, 1997 - Banking Law (Journal of Laws of 2002: No. 72 item 665, No. 126 item 1070, No. 141 item 1179, No. 144 item 1208, No. 153 item 1271, No. 169 items 1385 and 1387, and No. 241 item 2074; and of 2003: No. 50 item 424, No. 60 item 535 and No. 65 item 594).

5. Information relating to the introduction of asset values originating from money laundering and terrorist financing to the financial system may be disclosed by the General Inspector for foreign institutions referred to in Article 4 paragraph 1 point 8, on a reciprocal basis, in the manner specified in bilateral agreements concluded by the General Inspector, and also by a computerized data storage carriers.

6. Anyone who came into possession of information obtained pursuant to paragraphs 1-3 is required to protect the information protected by law, according to the principles and procedures laid down in separate regulations. Maintenance of confidentiality also applies after employment termination, performing activities under the contract or termination of civil service.

7. The obligation to maintain the confidentiality about the information obtained on the basis of the Act, to which the provisions of separate laws governing the protection do not apply, also covers the personnel of the obligated institutions, commerce chambers associating the obligated institutions, banks associating cooperative banks and all the persons performing activities on their behalf under civil law contracts. Maintenance of confidentiality also applies after termination of employment or cessation of activities based on civil law contracts.

Article 34 Any disclosure of information to unauthorized parties, including the parties of the transaction or the account holders; on the fact that the General Inspector has been informed about the transactions, the circumstances of which indicate that asset values may be derived from money laundering; or on the accounts of entities for which there is a reasoned suspicion that they have a connection with terrorist financing; or on transactions made by these entities, is prohibited.

Chapter 7a

Pecuniary penalties

Article 34a. Any obligated institution, with the exception of the National Bank of Poland, which:

1) fails to register the transaction referred to in Article 8 paragraph 1, fails to provide the General Inspector with the documents relating to this transactions or fails to store the records of the transactions or documents relating to this transaction for the required period of time,
2) fails to carry out risk analysis essential for the application of appropriate financial security measures,
3) fails to apply financial security measures,
4) fails to store documented results of the analysis for the required period of time,
5) fails to meet the obligation to provide the participation of employees in a training program,
6) fails to timely comply within the post-audit conclusions or recommendations,
7) establishes and maintains cooperation with a shell bank.

- shall be subject to pecuniary penalties.

Article 34b. 1. Any obligated institution that contrary to the following provisions of Regulation No 1781/2006:

1) Articles 5-7, does not ensure that the transfer of funds is accompanied by complete information on the payer,
2) Article 8, does not have effective procedures in place to detect the absence of information on the payer
3) Article 9, does not inform the General Inspector on the fact of regular neglecting to provide relevant information on the payer by payment service provider of the recipient,
4) Article 12, when acting as go-between as a payment service provider, does not preserve all the information accompanying transfers of funds received on the payer,
5) Article 14, does not respond completely to the request of the General Inspector on the information on the payer accompanied with transfers of funds, and does not provide the General Inspector with the relevant documents requested by him.

- shall be subject to pecuniary penalties.

2. The obligated institution is subject to the same penalty if - contrary to Article 20d paragraph 1 – it does not freeze the asset values of a person, group or entity or does not provide the General Inspector with all the data available to reasoning the freezing of asset values.

Article 34c. 1. The penalty shall be imposed by decision of the General Inspector at the amount not higher than 750.000 PLN, and in the event of a breach referred to in Article 34a point 5 not higher than 100.000 PLN.

2. When determining the amount of such a pecuniary penalty, the General Inspector shall take into account the nature and the extent of violations, the previous operation of the obligated institution and its financial capacity.

3. Pecuniary penalty is the revenue of the state budget.

4. If the violation referred to in Article 34a is found by the General Inspector in the course of the control, only one pecuniary penalty may be imposed.

5. Proceedings on inflicting pecuniary penalty are carried out under the provisions of the Code of Administrative Procedure.

6. The decision of the General Inspector may be appealed against to the minister competent for financial institutions within 14 days of its receipt.

7. Pecuniary penalties are subject to the enforcement of payment under the provisions of the enforcement procedure in the administration within the scope of the enforcement of pecuniary obligations.

8. In any undetermined matter, the provisions of Section III of the Act of August 29, 1997 - Tax Ordinance (Journal of Laws of 2005 No. 8 item 60, as amended) shall be applied accordingly for the pecuniary penalty.

9. The information about the pecuniary penalty imposed shall be communicated to the institution supervising the activities of the obligated institution.

Chapter 8

Penal provisions

Article 35 1. Any person who acts on behalf of or in the interest of the obligated institution contrary to the provisions of the Act fails to:

1) register a transaction, to submit documentation relating to this transaction to the General Inspector or to store the register of such transactions or documentation relating to this transaction for the required period of time,
2) maintain financial security measures, in accordance with the procedure referred to in Article 10a paragraph 1, or to store information obtained in connection with the implementation of financial security measures,
3) notify the General Inspector about the transactions referred to in Article 16 paragraph 1,
4) suspend a transaction or block an account,
5) introduce the internal procedure referred to in Article 10a paragraph 1,
6) designate a person responsible in accordance with Article 10b paragraph 1,

shall be subject to the punishment of imprisonment of up to 3 years.

2. Anyone who, contrary to the provisions of the Act, discloses the information collected in accordance with the authorization of the Act to any unauthorized persons, any account holder or any person to whom the transaction relates to or uses this information in any other manner inconsistent with the provisions of the Act shall be subject to the same punishment.

3. If the perpetrator of an act referred to in paragraphs 1 or 2 acts unintentionally, he/she shall be subject to a fine.

Article 36. Anyone acting on behalf of or in the interest of the obligated institution, contrary to the provisions of the Act:

1) refuse to submit information or documents to the General Inspector,
2) submits false data to the General Inspector or hides real data on transactions, accounts or persons,

shall be subject to the punishment of imprisonment from 3 months to 5 years.

Article 37. Who commits an act described in Article 35 paragraphs 1 or 2, or in Article 36 causing substantial damage, shall be subject to the punishment of imprisonment from 6 months to 8 years.

Article 37a. 1. Whoever hinders or obstructs exercising control activities referred to in Chapter 6 shall be subject to a fine.

2. (revoked).

Chapter 9

Amendments to existing regulations. Transitional and final provisions.

Article 38. The Act of 28 July 1990 on insurance activities (Journal of Laws of 1996: No. 11 item 62; of 1997: No. 43 item 272, No. 88 item 554, No. 107 item 685, No. 121 item 769 and 770, and No. 139 item 934; of 1998: No. 155 item 1015; of 1999: No. 49 item 483, No. 101 item 1178 and No. 110 item 1255; and of 2000: No. 43 item 483; No. 48, item 552; No. 70 item 819 and No. 114 item 1193) is amended as follows: (changes omitted).

Article 39. In the Act of 14 February 1991 - The Notary Law (Journal of Laws No. 22 item 91; of 1997: No. 28 item 153; of 1999: No. 101 items 1178; and of 2000: No. 48 item 551 and No. 94 item 1037), § 4 of the following content has been added to Article 18:

"§ 4 The obligation to maintain confidentiality does not apply to the information disclosed pursuant to the provisions on counteracting the introduction of asset values originating from illegal or undisclosed sources into financial trading"

Article 40. In the Act of 28 September 1991 on fiscal control (Journal of Laws of 1999 No. 54 item 572 and No. 83 item 931; and of 2000: No. 70 item 816 and No. 104, item 1103), point 1a of the following content has been added to Article 34a item 1:

"1a) the General Inspector of Financial Information - in accordance with the provisions on counteracting the introduction of asset values originating from illegal or undisclosed sources into financial trading."

Article 41. In the Act of 29 July 1992 on games of chance, mutual wagering and slot machine games (Journal of Laws of 1998: No. 102 item 650, No. 145 item 946, No. 155 item 1014 and No. 160 item 1061; and of 2000: No. 9 item 117 and No. 70 item 816), in Article 11 item 6 after the words "of the minister competent for public finances" the words "of the General Inspector of Financial Information" have been added;

Article 42. In the Act of 13 October 1995 on the terms of registration and identification of taxpayers and tax remitters (Journal of Laws No. 142 item 702; of 1997: No. 88 item 554; of 1998: No. 162 item 1118; and of 1999: No. 83 item 931) item 6 of the following content has been added to in Article 15 item 2:

"6) to the General Inspector of Financial Information - to perform his duties arising from the provisions on counteracting the introduction of asset values originating from illegal or undisclosed sources into financial trading."

Article 43. In the Act of 6 June 1997 - Penal Code (Journal of Laws No. 88 item 553 and No. 128 item 840; of 1999: No. 64 item 729 and No. 83 item 931; and of 2000: No. 48 item 548 and No. 93 item 1027), in Article 299: (changes omitted).

Article 44. In the Act of 21 August 1997 - Law on Public Trading in Securities (Journal of Laws No. 118 item 754, No. 141 item 945; of 1998: No. 107 item 669, No. 113 item 715; and of 2000: No. 22 item 270, No. 60 items 702 and 703, No. 94 item 1037, No. 103 item 1099, No. 114 item 1191) item 5 of the following content has been added to Article 161:

"5. The scope and the principles for the provision of confidential information and constituting professional secrecy disclosed to the General Inspector of Financial Information by the Commission, is governed by a separate act"

Article 45. The Act of August 29, 1997 - Banking Law (Journal of Laws No. 140 item 939; of 1998: No. 160 item 1063 and No. 162 item 1118; of 1999: No. 11 item 95 and No. 40 item 399; and of 2000: No. 93 item 1027, No. 94 item 1037 and No. 114 item 1191) is amended as follows: (changes omitted).

Article 46. In the Act of August 29, 1997 - Tax Ordinance (Journal of Laws No. 137 item 926 and No. 160 item 1083; of 1998: No. 106 item 668; of 1999: No. 11 item 95 and No. 92 item 1062; and of 2000: No. 94 item 1037) item 2a of the following content has been added to Article 297 in § 1 after point 2:

„2a) to the General Inspector of Financial Information – according to the provisions on counteracting the introduction of asset values originating from illegal or undisclosed sources into financial trading"

Article 47. In the Act of August 29, 1997 on the protection of personal data (Journal of Laws No. 133 item 883; and of 2000: No. 12 item 136 and No. 50 item 580) point 2a of the following content has been added in Article 43 item 1, after point 2:

"2a) processed by the General Inspector of Financial Information,"

Article 47a. Within the period from 31 March, 2002, to 31 December, 2002, the provisions of the Act shall also apply to the exchange of the parred media of exchange in national currencies for media of exchange parred in EURO, made under the provisions of the Act of 25 May 2001 on the consequences associated with introducing common EURO currency in some Member States of the European Union (Journal of Laws No. 63 item 640), including the National Bank of Poland.

Article 47b. Within the period from 1 December 2002 to 31 December 2003, the obligation to register the transactions referred to in Article 8 item 1 shall not apply.

Article 48. (Deleted).

Article 49. The Act shall enter into force after 6 months from the date of the notice, except:

1) Articles 3-6, Article 13 and Article 15 which shall enter into force after 14 days from the date of the notice;
2) (deleted);
3) Article 45 point 3 letter b in so far as considering Article 106 items 4 and 5, which shall enter into force on 31 December 2003.

[1)] Within the scope of its regulation, this Act shall implement the following directives of the European Communities:

1) Directive 91/308/EEC of 10 June 1991 on the prevention of use of the financial system for the purpose of money laundering (OJ L 166 of 28.06.1991),
2) Directive 2001/97/EC of 4 December 2001 amending Directive 91/308/EEC on the prevention of the use of the financial system for the purposes money laundering - Commission Declaration (OJ L 344, 18.12.2001).

Data considering publishing of the European Union juristic acts, included in this law, since the day of the accession of the Republic of Poland to the European Union, relate to the publications of those acts in the Official Journal of the European Union (special edition). (134)

Annex 3. List of Key Law, Regulations and Other materials provided to Evaluation Team

See MONEYVAL(2013)2ANN

Annex 4. Status of Implementation of the Vienna Convention, the Palermo Convention and the UN International Convention for the Suppression of the Financing of Terrorism

Implementation of the Vienna Convention

Provisions of the Vienna Convention	Polish legislative acts and regulations that cover requirements of the Vienna Convention
Article 3 (Offences and Sanctions)	Articles 53-68 of the Act of 29 July 2005 on Counteracting Drug Addiction Articles 18, 64, 65, 78, 101, 115, 258, 291, 299 of the CC Chapters 27 and 28 of the CPC
Article 4 (Jurisdiction)	Articles 5, 109-113 of the CC
Article 5 (Confiscation) - with regard to confiscation of proceeds derived from offences involving illicit trafficking of narcotic drugs or psychotropic substances; - with regard to seizure of property (assets); - with regard to rendering mutual legal assistance.	Articles 44-45,52 of the CC Article 32 of the AML/CFT Act Art.299 § 7 CC Articles 585 and 588 of the CPC Article 69 of the Act of 29 July 2005 on Counteracting Drug Addiction Bilateral and multilateral agreements signed by Poland
Article 6 (Extradition)	Article 55 of the Constitution Chapter 65 of the CPC Bilateral and multilateral agreements signed by Poland Institution of European Arrest Warrant regulated by Chapter 65a of the CPC
Article 7 (Mutual Legal Assistance)	Article 585 and 588 of the CPC
Article 8 (Transfer of Proceedings)	Chapter LXIII of the CCP
Article 9 (Other Forms of Cooperation and Training)	Bureau of International Cooperation of the Polish National Police Interpol Europol In the international MLA agreements signed by Poland
Article 10 (International Cooperation and Assistance for Transit States)	United Nations Council of Europe

	OSCE European Union In the international agreements signed by Poland
Article 11 (Controlled Delivery)	Article 11 of the Act on the Police of 6 April 1990 Act of 24 May 2002 on Internal Security Agency and Intelligence Agency Act of 12 October 1990 on Border Guard Act of 28 September 1991on Fiscal control
Article 15 (Commercial Carriers)	
Article 17 (Illicit Traffic by Sea)	
Article 19 (The Use of the Mails)	

Implementation of the Palermo Convention

Provisions of the Palermo Convention	**Polish legislative acts and regulations that cover requirements of the Palermo Convention**
Article 5 (Criminalisation of Participation in an Organized Criminal Group)	Articles 18 and 258 of the CC
Article 6 (Criminalisation of the Laundering of Proceeds of Crime)	Articles 291 and 299 of the CC
Article 7 (Measures to Combat Money-Laundering)	AML/CFT Act
Article 10 (Liability of Legal Persons)	Act on Liability of Collective Entities for Acts Prohibited under Penalty of 28 October 2002
Article 11 (Prosecution, Adjudication and Sanctions)	Articles 78 and 101 of the CC Chapters 27 and 28 of the CPC
Article 12 (Confiscation and Seizure)	Articles 44-45 of the CC
Article 13 (International Cooperation for Purposes of Confiscation)	Articles 585 and 588 of the CPC
Article 14 (Disposal of Confiscated Proceeds of Crime or Property)	Articles 585 and 588 of the CPC
Article 15 (Jurisdiction)	Articles 5, 109-113 of the CC
Article 16 (Extradition)	Article 55 of the Constitution Chapter 65 of the CPC Bilateral and multilateral agreements signed by

	Poland Institution of European Arrest Warrant regulated by Chapter 65a of the CPC
Article 18 (Mutual Legal Assistance)	Articles 585 and 588 of the CPC
Article 19 (Joint Investigations)	Article 589b of the CPC
Article 20 (Special Investigative Techniques)	Articles 237 and 241 of the CCP Act on Polish National Police (Articles 19a, 19b and 20a)
Article 24 (Protection of Witnesses)	Article 184 of the CPC
Article 25 (Assistance to and Protection of Victims)	Polish Chart on Victims' Rights
Article 26 (Measures to Enhance Cooperation with Law Enforcement Authorities)	Article 259 of the CC
Article 27 (Law Enforcement Cooperation)	Article 589b, c, d, e, f
Article 29 (Training and Technical Assistance)	United Nations Council of Europe OSCE European Union
Article 30 (Other Measures: Implementation of the Convention through Economic Development and Technical Assistance)	In different part of Polish legislation
Article 31 (Prevention)	AML/CFT Act
Article 34 (Implementation of the Convention)	

Implementation of the UN International Convention for the Suppression of the Financing of Terrorism

Provisions of the UN International Convention for the Suppression of the Financing of Terrorism	**Polish legislative acts and regulations that cover requirements of the UN International Convention for the Suppression of the Financing of Terrorism**
Article 2	Articles 15, 18, 165a, 258 of the CC
Article 3	Article 165a of the CC

Article 4	Article 165a of the CC
Article 5	Act on Liability of Collective Entities for Acts Prohibited under Penalty of 28 October 2002
Article 6	
Article 7	Articles 5 and 10 of the CC Art. 109-113 CC
Article 8	Articles 44 and 45 of the CC Article 20d of the AML/CFT Act
Article 9	Art.110 §2 CC Art.303 of the CCP Art.243-265 CCP
Article 10	Articles 602 and 605 of the CPC
Article 11	Article 55 of the Constitution Chapter 65 of the CPC Bilateral and multilateral agreements signed by Poland Institution of European Arrest Warrant regulated by Chapter 65a of the CPC
Article 12	Article 585 of the CPC Article 32 of the AML/CFT Act
Article 13	Art.602-607 of the CCP
Article 14	
Article 15	Art.604 of the CCP
Article 16	
Article 17	Art.207-223a of the Code of Execution of Penalties (CEP)
Article 18	Articles 1, 16, 18, 255a of the CC Article 32 of the AML/CFT Act

Annex 5 Status of Implementation of the UN Security Council Resolutions

Resolution 1267 (1999)

Provisions of the Resolution 1267 (1999)	Polish legislative acts and regulations that cover requirements of the Resolution 1267 (1999)
subparagraph "a" of paragraph 4	Council Regulation (EC) No 467/2001 of 6 March 2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan, and repealing Regulation (EC) No 337/2000. Act on the Border Guard
subparagraph "b" of paragraph 4	Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan. AML/CFT Act

Resolution 1333 (2000)

Provisions of the Resolution 1333 (2000)	Polish legislative acts and regulations that cover requirements of the Resolution 1333 (2000)
subparagraphs "a", "b", and "c" of paragraph 5	See above.
subparagraphs "a", "b", and "c" of paragraph 7	See above.
subparagraphs "a", "b" and "c" of paragraph 8	See above.
subparagraphs "a" and "b" of paragraph 10	See above.

subparagraphs “a” and “b” of paragraph 11	See above.
subparagraphs “a” and “b” of paragraph 14	See above.

Resolution 1363 (2001)

Provisions of the Resolution 1363 (2001)	Polish legislative acts and regulations that cover requirements of the Resolution 1363 (2001)
paragraph 8	AML/CFT Act Order No 117 of the President of the Council of Ministers of 14 November 2003 on the establishment of the Inter-ministerial Team for International Sanctions

Resolution 1373 (2001)

Provisions of the Resolution 1373 (2001)	Polish legislative acts and regulations that cover requirements of the Resolution 1373 (2001)
subparagraphs “a”, “b” and “c” of paragraph 1	Article 165a of Penal Code Article 115 paragraph 20 of the Penal Code Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism
Paragraph 2	Council Common Position of 27 December 2001 on combating terrorism (2001/930/CFSP) Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism Council Decision 2005/211/JHA of 24 February

	2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism Council Decision 2007/801/ECof 6 December 2007 on the full application of the provisions of the *Schengen acquis* in the Czech Republic, the Republic of Estonia, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime Penal Code Code of Criminal Procedure Act on the Border Guard

Resolution 1390 (2002)

Provisions of the Resolution 1390 (2002)	Polish legislative acts and regulations that cover requirements of the Resolution 1390 (2002)
subparagraphs "a", "b" and "c" of paragraph 2	See above. Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan. AML/CFT Act Act on the Border Guard

Resolution 1455 (2003)

Provisions of the Resolution 1455 (2003)	Polish legislative acts and regulations that cover requirements of the Resolution 1455 (2003)
paragraph 1	Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan. AML/CFT Act Act on the Border Guard

paragraph 5	See above. Order No 117 of the President of the Council of Ministers of 14 November 2003 on the establishment of the Inter-ministerial Team for International Sanctions.
paragraph 6	Order No 117 of the President of the Council of Ministers of 14 November 2003 on the establishment of the Inter-ministerial Team for International Sanctions.

Resolution 1526 (2004)

Provisions of the Resolution 1526 (2004)	**Polish legislative acts and regulations that cover requirements of the Resolution 1526 (2004)**
paragraph 4	Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan. Regulation (EC) No 1781/2006 of the European Parliament and the Council of 15 November 2006 on information on the payer accompanying transfers of funds Penal Code AML/CFT Act
paragraph 5	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

	The Customs Service Act Act on the Border Guard
Paragraph 17	Order No 117 of the President of the Council of Ministers of 14 November 2003 on the establishment of the Inter-ministerial Team for International Sanctions.
paragraph 22	Order No 117 of the President of the Council of Ministers of 14 November 2003 on the establishment of the Inter-ministerial Team for International Sanctions.

Annex 6. International agreements signed by Poland

On mutual legal assistance and legal relations

Mutual legal assistance (MLA) is provided by Poland either on the basis of international multi - and bilateral treaties that Poland is a party to or upon reciprocity principle under domestic law: Part XIII - Procedure in criminal cases in international relations - of the Code of Criminal Procedure.

Mutual legal assistance may also be afforded under the self-executing provisions of certain conventions and treaties:

1. Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on Financing of Terrorism of 16 May 2005 (CETS 198)
2. European Convention on mutual assistance in criminal matters of 20 April 1959 (CETS 30),
3. Additional Protocol to the European Convention on mutual assistance in criminal matters of 17 March 1978 (CETS 099),
4. Second Additional Protocol to the European Convention on mutual assistance in criminal matters of 8 November 2001 (CETS 182),
5. The Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000,
6. Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 16 October 2001,
7. the Convention implementing the Schengen Agreement 1990.

Poland has also signed numerous bilateral agreements concerning MLA:

1. Agreement between the Republic of Poland and the People's Democratic Republic of Algeria on legal transactions in civil and criminal matters, signed on 9.11.1976;
2. Agreement between the Republic of Poland and the Commonwealth of Australia on extradition**,** signed on 03.06.1998;
3. Agreement between the Republic of Poland and the Republic of Belarus on legal assistance in civil, family, labour and criminal matters, signed on 26.10.1994;
4. Agreement between the Republic of Poland and the Arab Republic of Egypt on legal assistance in criminal matters, trasferring the sentenced persons and extradition, signed on 17.05.1992;
5. Agreement between the Republic of Poland and the Republic of Iraq on legal assistance in
6. civil and criminal matters, signed on 29.10.1988;
7. Agreement between the Republic of Poland and the Republic of India on extradition , signed on 17.02.2003;
8. Agreement between the Republic of Poland and the Democratic People's Republic of Korea on legal assistance in civil, family and criminal matters, signed on 28.09.1986;
9. Agreement between the Republic of Poland and the Republic of Cuba on legal assistance in civil, family and criminal matters, signed on 18.11.1982;

10. Agreement between the Republic of Poland and the Great Socialist People's Libyan Arab Jamahiriya on legal assistance in civil, commercial, family and criminal matters, signed on 02.12.1985;
11. Agreement between the Republic of Poland and the Kingdom of Morocco on legal assistance in civil and criminal matters, signed on 21.05.1979;
12. Agreement between the Republic of Poland and Mongolia on legal assistance in civil, family, labour and criminal matters, signed on 19.10.1998;
13. Agreement between the Republic of Poland and the United States of America on extradition, signed on 10.07.1996;
14. Agreement between the Republic of Poland and the Syrian Arab Republic on legal assistance in civil and criminal matters, signed on 16.02.1985;
15. Agreement between the Republic of Poland and the Tunisian Republic on legal assistance in civil and criminal matters, signed on 22.03.1985;
16. Agreement between the Republic of Poland and the Socialist Republic of Vietnam on legal assistance in civil, family and criminal matters, signed on 22.03.1993.

On extradition

Poland is a party to numerous multi- and bi-lateral agreements in this area, notably the Convention of 10 March 1995 on simplified extradition procedure between the Member States of the European Union (1995 EU Extradition Convention) and the European Union the Convention of 27 September 1996 relating to extradition between the Member States of the European Union (1996 EU Extradition Convention). Furthermore Poland has ratified:

1. Council of Europe Convention on Extradition (ETS 24)
2. Additional Protocol to the European Convention on Extradition of (ETS 86)
3. Second Additional Protocol to the European Convention on Extradition (ETS 98)
4. Convention implementing the Schengen Agreement of 19 June 1990.

With respect to European Union countries, Poland has simplified some of its extradition provisions implementing the European Union Framework Decision of 2002 on the European Arrest Warrant and Surrender Procedures between Member States.

On cooperation in combating organized crime, international terrorism and other especially dangerous crimes

Armenia

Agreement between the Government of the Republic of Poland and the Government of the Republic of Armenia on Cooperation in combating Crime

Signed: 2004-09-06

Entered into force: 2005-04-07

Published: J oL.2005 No 125, item 1046

 **Austria**

Agreement between the Government of the Republic of Poland and the Government of the Republic of Austria in prevention and combating Crime

Signed: 2002-06-10

Entered into force 2003-12-01

Published: J oL.2004 No 41, item 377

 **Belgium**

Agreement between the Government of the Republic of Poland and the Government of the Kingdom of Belgium on Cooperation in combating Organized Crime

Signed: 2000-11-13

Entered into force: 2004-01-01

Published: J oL.2004 No 36, item 329

 **Belarus**

Agreement between the Government of the Republic of Poland and the Government of the Republic of Belarus on Cooperation in combating Crime

Signed: 2003-12-08

Entered into force: 2005-03-05

Published: J oL.2005 No 125, item 1044

 **Brazil**

Agreement between the Government of the Republic of Poland and the Government of the Federative Republic of Brazil on Cooperation in combating Organized Crime and Other Crimes

Signed: 2006-10-09

Bulgaria

Agreement between the Government of the Republic of Poland and the Government of the Republic of Bulgaria on Cooperation in combating Crime

Signed: 2002-06-19

Entered into force: 2003-11-28

Published: J oL.2004 No 154, item 1619

Chile

Agreement between the Government of the Republic of Poland and the Government of the Republic of Chile on Cooperation in combating Organized Crime

Signed: 2006-10-13

Entered into force: 2007-09-12

Published: J oL.2007 No 229, item 1688

Croatia

Agreement between the Ministry of Internal Affairs of the Republic of Poland and the Ministry of Internal Affairs of the Republic of Croatia on Cooperation in prevention and detecting Criminal Offences

Signed: 1994-11-08

Entered into force: 1994-11-08

Agreement between the Government of the Republic of Poland and the Government of the Republic of Croatia on Cooperation in combating Crime

Signed: 2010-07-09

Entered into force: 2010-07-09

Cyprus

Agreement between the Government of the Republic of Poland and the Government of the Republic of Cyprus on Cooperation in combating Organized Crime and Other Crimes

Signed: 2005-02-18

Entered into force: 2006-02-17

Published: J oL.2006 No 88, item 611

 **Czech Republic**

Agreement between the Government of the Republic of Poland and the Government of the Czech Republic on Cooperation in combating Crime, Protection of the Public Order and Cooperation in the Border Territories

Signed: 2006-06-21

Entered into force: 2007-08-02

Published: J oL.2007 No 177, item 1246

 **Egypt**

Agreement between the Government of the Republic of Poland and the Government of the Arab Republic of Egypt on Cooperation in Security issues

Signed: 1996 10 17

Entered into force: 1998 10 17

 **Estonia**

Agreement between the Government of the Republic of Poland and the Government of the Republic of Estonia on Cooperation in combating Organized Crime and Other Crimes

Signed: 2003- 06 -26

Entered into force: 2004 -02-07

Published: J oL.2004 No 216, item 2195

Agreement in the form of an Exchange of aide-mémoire between the Government of the Republic of Poland and the Government of the Republic of Estonia on Addendum to Article 2 of the Agreement between the Government of the Republic of Poland and the Government of the Republic of Estonia on Cooperation in combating Organized Crime and Other Crimes signed at Warsaw on June 26, 2003

Signed: 2006-12-05

Published: J oL.2008 No 12, item 71

Finland

Agreement between the Government of the Republic of Poland and the Government of the Republic of Finland on Cooperation in counteracting and combating Organized Crime and Other Crimes

Signed: 1999-11-04

Entered into force: 2003-11-20

Published: J oL.2004 No 41, item 379

France

Agreement between the Government of the Republic of Poland and the Government of the Republic of France on Cooperation in Internal Affairs

Signed: 1996-09-12

Entered into force: 1998-03-01

Germany

Agreement between the Government of the Republic of Poland and the Government of the Federal Republic of Germany on Police and Border Guard Cooperation in the Border Territories

Signed: 2002- 02-17

Entered into force: 2003 06 26

Published: J oL.2005 No 223, item 1915

Agreement between the Government of the Republic of Poland and the Government of the Federal Republic of Germany on Cooperation in combating Organized Crime and Other Serious Crimes

Signed: 2002-06-18

Entered into force: 2004-09-18

Published: J oL.2004 No 248, item 2486

Greece

Agreement between the Government of the Republic of Poland and the Government of the Republic of Greece on Cooperation between the Ministry of Internal Affairs of the Republic of Poland and the Ministry of Public Order of the Republic of Greece on Cooperation in their competences

Signed: 1993 06 18

Georgia

Agreement between the Government of the Republic of Poland and the Government of Georgia on Cooperation in combating Organized Crime and Other Crimes

Signed: 2007-05-31

Entered into force: 2008-05-03

Published: J oL.2008 No 146, item 925

Iran

Agreement between the Government of the Republic of Poland and the Government of the Islamic Republic of Iran on Cooperation in combating Illegal Drug, Psychotropic Substances and their Precursors Trafficking

Signed: 2005-07-11

Ireland

Agreement between the Government of the Republic of Poland and the Government of Ireland on Cooperation in combating Organized Crime and Other Crimes

Signed: 2001-05-12

Entered into force: 2006-03-18

Published: J oL.2006 No 103, item 701

Italy

Agreement between the Government of the Republic of Poland and the Government of the Italian

Republic in combating Organized Crime and Other Crimes

Signed: 2007-06- 04

Entered into force: 2009-06-25

Published: J oL.2009 No 133, item 1093

Kazakhstan

Agreement between the Government of the Republic of Poland and the Government of the Republic of Kazakhstan on Cooperation in combating Organized Crime and Other Crimes

Signed: 2002-05-24

Entered into force: 2005-03-30

Published: J oL.2005 No 156, item 1312

Lithuania

Agreement between the Government of the Republic of Poland and the Government of the Republic of Lithuania on Cooperation in combating Organized Crime and Other Crimes and Cooperation in the Border Territories

Signed: 2006-03-14

Entered into force: 2007-07-08

Published: J oL.2007 No 177, item 1244

Latvia

Agreement between the Ministry of Internal Affairs of the Republic of Poland and the Ministry of Internal Affairs of the Republic of Latvia on Cooperation in combating Crime

Signed: 1994-07-14

Entered into force: 1994-07-14

Macedonia

Agreement between the Government of the Republic of Poland and the Government of the Republic of Macedonia on Cooperation in combating Organized Crime and Other Crimes

Signed: 2008-06-16

Entered into force: 2009-02-21

Published: J oL.2009 No 46, item 378

Morocco

Agreement between the Ministry of Internal Affairs of the Republic of Poland and the Ministry of Internal Affairs of the Kingdom of Morocco on Cooperation in combating Crime, Terrorism and Drug Trafficking

Signed: 1995-06-26

Entered into force: 1995 06 26

Mexico

Agreement between the Government of the Republic of Poland and the Government of the United States of Mexico on Cooperation in combating Organized Crime and Other Crimes

Signed: 2002-11-25

Entered into force: 2003-11-27

Published: J oL.2004 No 154, item 1623

Agreement in the form of an Exchange of aide-mémoire between the Government of the Republic of Poland and the Government of the United States of Mexico on Addendum to Article 2 of the Agreement between the Government of the Republic of Poland and the Government of the United States of Mexico Cooperation in combating Organized Crime and Other Crimes signed at City of Mexico on November 25, 2002.

Signed: 2006-11-30

Entered into force: 2006-12-30

Moldova

Agreement between the Government of the Republic of Poland and the Government of the Republic of Moldova on Cooperation in combating Organized Crime and Other Crimes

Signed: 2003-10-22

Entered into force: 2004-07-26

Published: J oL.2004 No 228, item 2302

 **Netherlands**

Memorandum of Understanding between the Minister of Internal Affairs of the Republic of Poland and the Minister or Internal Affairs and Minister of Justice of Netherlands on Cooperation in Development of the Police Operations, signed at The Hague on October 30, 1996

Signed: 1996-10-30

Entered into force: 1996-10-30

 **Russian Federation**

Agreement between the Ministry of Internal Affairs of the Republic of Poland and the Ministry of Internal Affairs of the Russian Federation signed in Moscow on November 20, 1992

Signed: 1992-11-20

Entered into force: 1992-11-20

Agreement between the Government of the Republic of Poland and the Government of the Russian Federation on Transborder Cooperation

Signed: 1992-10-02

Entered into force: 1992-12-07

 **Romania**

Agreement between the Government of the Republic of Poland and the Government of Romania on Cooperation in combating Organized Crime, Terrorism and Other Crimes

Signed: 2001-07-11

Entered into force: 2003-08-27

Published: J oL.2004 No 154, item 1625

Saudi Arabia

Agreement between the Government of the Republic of Poland and the Government of the Kingdom of Saudi Arabia on Cooperation in combating Organized Crime and Other Crimes

Signed: 2007-06-25

Entered into force: 2008-08-09

Published: J oL.2009 No 28, item 172

Serbia

Agreement between the Government of the Republic of Poland and the Government of the Republic of Serbia on Cooperation in combating Organized Crime and Other Crimes

Signed: 2011-11-07

Slovak Republic

Agreement between the Government of the Republic of Poland and the Government of the Slovak Republic on Cooperation in combating Crime and Cooperation in the Border Territories

Signed: 2004-03-24

Entered into force: 2006-12-01

Agreement between the Government of the Republic of Poland and the Government of the Slovak Republic which changed the Agreement between the Government of the Republic of Poland and the Government of the Slovak Republic on Cooperation in combating Crime and Cooperation in the Border Territories, signed in Warsaw on March 24, 2004

Signed: 1996-10-30

Entered into force: 2011-07-31

Published: J oL.2011 No 249, item 1497

Slovenia

Agreement between the Government of the Republic of Poland and the Government of the Republic of Slovenia on Cooperation in combating Terrorism, Organized Crime and Illegal Drug, Psychotropic Substances and their Precursors Trafficking

Signed: 1996-08-28

Entered into force: 1998-04-06

 **Spain**

Agreement between the Republic of Poland and the Kingdom of Spain on Cooperation in combating Organized Crime and Other Serious Crime

Signed: 2000-11-27

Entered into force: 2003-11-26

Published: J oL.2004 No 154, item 1621

 **Sweden**

Agreement between the Government of the Republic of Poland and the Government of the Kingdom of Sweden on Cooperation in combating Serious Crime

Signed: 2005-04-13

Entered into force: 2005-11-04

Published: J oL.2006 No 14, item 100

 **Tajikistan**

Agreement between the Government of the Republic of Poland and the Government of the Republic of Tadzhikistan on Cooperation in combating Crime

Signed: 2003-05-27

Entered into force: 2004-04-02

Published: J oL.2004 No 211, item 2141

 **Thailand**

Memorandum of Understanding Between the Government of the Republic of Poland and the Government of Kingdom of Thailand on Cooperation in Combating Drugs

Signed: 1996-09-23

Entered into force: 2002-09-04

Published: MoP 2003 No16,item 242

Tunisia

Agreement between the Minister of Internal Affairs of the Republic of Poland and the Minister of Internal Affairs of the Republic of Tunisia

Signed: 1994 -09-26

Entered into force: 1994-09-26

Turkey

Agreement between the Government of the Republic of Poland and the Government of the Republic of Turkey on Cooperation in combating Terrorism, Organized Crime and Other Crimes

Signed: 2003-04-07

Entered into force: 2004-07-25

Published: J oL.2005 No 12, item 94

Ukraine

Agreement between the Government of the Republic of Poland and the Government of Ukraine on Cooperation in combating Organized Crime

Signed: 1999-03-03

Entered into force: 2003-08-24

Published: J oL.2004 No 38, item 343

Uzbekistan

Agreement between the Government of the Republic of Poland and the Government of the Republic of Uzbekistan on Cooperation in combating Organized Crime

Signed: 2002-10-21

Entered into force: 2003-11-22

Published: J oL.2004 No 38, item 345

Hungary

Agreement between the Government of the Republic of Poland and the Government of the Republic of Hungary on Cooperation in combating Terrorism, Illegal Drug Trafficking and Organized Crime

Signed: 1996-05-15

Entered into force: 1998-05-14

United Kingdom of Great Britain and Northern Ireland

Common Declaration of the Government of the United Kingdom of Great Britain and Northern Ireland on combating International Crime

Signed: 1997 02 27

Entered into force: 1997-02-27

Vietnam

Agreement between the Government of the Republic of Poland and the Government of the Socialist Republic of Vietnam in combating Organized Crime

Signed: 2003-07-28

Entered into force: 2004-04-26

Published: J oL.2004 No 216, item 2197

Annex 7. Inter-agency agreements signed by Law Enforcement

Agreement between the General Inspector of Financial Information and the Head of the State Protection Office (ABW's predecessor) of 22 August 2001 on cooperation

Agreement between the Police Commander in Chief and the Prosecutor General of 18 October 2002 on transmission of criminal information into the National Criminal Information Centre

Agreement between the Police Commander in Chief and the Head of the Internal Security Agency of 21 October 2003 on establishing detailed field and operating mode between the Police and Internal Security Agency (classified)

Agreement between the Minister of Finance and the Police Commander in Chief of 6 November 2003 on Cooperation between the Customs Service and the Police

Agreement between the Police Commander in Chief and the Head of the Intelligence Agency of 2 March 2004 on establishing detailed field and operating mode between the Police and Internal Security Agency (classified)

Agreement between the Police Commander in Chief and the Border Guard Commander in Chief of 17 June 2004 on Cooperation between the Police and Border Guard

Agreement between the Police Commander in Chief and the General Inspector of Treasury Control of 11 January 2005 on Cooperation between the Police and The Treasury Control Services

Agreement between the Police Commander in Chief and the Head of The Central Anti - Corruption Bureau of 2 May 2007 on Cooperation between the Police and The Central Anti-Corruption Bureau

Declaration of Cooperation of 18 December 2008 signed between the Minister of Interior, the Minister of Finance and the General Prosecutor

Agreement of 15 September 2009 concluded between Minister of Internal Affairs and Administration, Minister of Finance and Minister of Justice on Cooperation against the use of proceeds from crime and in identification of those proceeds or other assets connected with crime in terms of reference of the National Assets Recovery Office

Annex 8. MoUs signed by the GIFI

	List of MoUs signed by the GIFI	Date
1.	Czech	2001-11-13
2.	Estonia	2001-12-10
3.	Slovakia	2001-12-10
4.	Lithuania	2002-02-07
5.	Belgium	2002-03-21
6.	Bulgaria	2002-04-01
7.	United Kingdom	2002-04-29
8.	Romania	2002-07-05
9.	Spain	2002-08-08
10.	Korea, Republic of	2002-10-14
11.	Finland	2002-11-06
12.	Israel	2003-01-21
13.	Slovenia	2003-06-03
14.	Russia	2003-06-24
15.	Latvia	2003-06-30
16.	Lichtenstein	2003-07-01
17.	Australia	2003-07-22
18.	Italy	2003-10-29
19.	USA	2003-11-07
20.	Ireland	2003-11-21
21.	Portugal	2004-01-19
22.	Andorra	2004-01-20

23.	Cyprus	2004-04-02
24.	Ukraine	2004-04-14
25.	Monaco	2004-04-16
26.	Germany	2004-04-20
27.	Thailand	2004-10-26
28.	Guernsey	2005-04-12
29.	Chile	2005-06-29
30.	Croatia	2005-06-29
31.	Indonesia	2005-06-29
32.	Macedonia	2005-07-21
33.	Switzerland	2005-09-13
34.	Canada	2006-11-08
35.	Taiwan	2006-11-08
36.	Serbia	2006-11-10
37.	Albania	2007-11-15
38.	Montenegro	2007-11-15
39.	Peru	2008-03-03
40.	Brazil	2008-03-11
41.	Philippines	2008-03-11
42.	Georgia	2008-09-29
43.	Argentine	2008-10-22
44.	Mexico	2008-12-01
45.	Moldova	2009-08-28
46.	Norway	2009.09.15
47.	San Marino	2009-09-21

48.	Armenia	2009-09-22
49.	Isle of Man	2009-09-29
50.	Commonwealth of Bahamas	2009-09-30
51.	South Africa	2010-02-22
52.	Kyrgyzstan	2010-02-25
53.	Egypt	2010-06-30
54.	Qatar	2010-06-30
55.	Jersey (Channel Island)	2011-04-28
56.	Aruba	2011-07-12
57.	British Virgin Islands	2011-07-12
58.	India	2011-07-12
59.	Saudi Arabia, Kingdom of	2011-07-12
60.	Saint Vincent & Grenadines	2011-07-22
61.	Hashemite Kingdom of Jordan	2011-11-01
62.	United Arab Emirates	2011-11-23
63.	Algeria	2011-09-26