COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 22 November 2007

MONEYVAL (2006) 24

EUROPEAN COMMITTEE ON CRIME PROBLEMS
(CDPC)

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

THIRD ROUND DETAILED ASSESSMENT REPORT on P O L A N D[1]

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

Memorandum
prepared by the Secretariat
Directorate General of Human Rights and Legal Affairs

[1] adopted by MONEYVAL at its 23rd Plenary Session (Strasbourg, 5 – 7 June 2007).

TABLE OF CONTENTS

LIST OF ACRONYMS USED

AML Law	Anti-Money Laundering Law
BSC	Commission for Banking Supervision
CCP	Code of Criminal Procedure
CETS	Council of Europe Treaty Series
CTED	Counter-Terrorism Committee Executive Directorate
DNFBP	Designated Non-Financial Businesses and Professions
EAW	European Arrest Warrant
ETS	European Treaty Series [since 1.1.2004: CETS = Council of Europe Treaty Series]
FIU	Financial Intelligence Unit
FMA	Financial Market Authority
GIFI	General Inspector of Financial Information
GINB	General Inspectorate of Banking Supervision ("Generalny Inspektorat Nadzoru Bankowego")
IT	Information Technology
MFA	Ministry of Foreign Affairs
MLA	Mutual legal assistance
MLAT	Mutual Legal Assistance Treaty
MOU	Memorandum of Understanding
MVT	Money or value transfer service
NBP	National Bank of Poland
NGO	Non Governmental Organisation
PBO	Public benefit organisation
PC	Penal Code
PEP	Politically Exposed Person
PHARE	Poland and Hungary: Assistance for Restructuring their Economies (EU Programme)
PSEC	Polish Securities and Exchange Commission
PLN	Poland Złoty
SAR	Suspicious Activity Report
SITs	Special Investigative Techniques
SRO	Self Regulatory Authorities

I. PREFACE

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of Poland was based on the forty Recommendations of the FATF (2003) and the 9 Special Recommendations on financing of terrorism of the FATF, together with the two Directives of the European Commission (91/308/EEC and 2001/97/EC), in accordance with MONEYVAL's terms of reference and Procedural Rules. The evaluation was based on the laws, regulations and other materials supplied by Poland during the on-site visit from 14 to 21 May 2006 and subsequently. During the on-site visit, the evaluation team met with officials and representatives of relevant Polish Government agencies and the private sector. A list of the persons and bodies met is set out in Annex I to the mutual evaluation report.

2. The evaluation team comprised Mr Radovan MARAS, Prosecutor, Higher Military Prosecutor's Office, Slovakia (Legal Evaluator); Ms Iva STROUHALOVA, Banking Supervision, Czech National Bank, Czech Republic (Financial Evaluator); Ms Slagjana TASEVA, Director, Police Academy, "the former Yugoslav Republic of Macedonia" (Law Enforcement Evaluator); Ms Elisabeth FLORKOWSKI (FATF Evaluator) Financial Market Authority, Austria (Financial Evaluator) and Mr. Gary J. PETERS (FATF Evaluator) Senior Advisor, Bureau for International Narcotics and Law Enforcement, U.S. Department of State, the United States (Law Enforcement Evaluator). The examiners reviewed the institutional framework, the relevant AML/CFT Laws, regulations and guidelines and other requirements, and the regulatory and other systems in place to deter money laundering and financing of terrorism through financial institutions and designated non-financial businesses and professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all the systems.

3. This report provides a summary of the AML/CFT measures in place in Poland as at the date of the on-site visit or immediately thereafter. It describes and analyses these measures, and provides recommendations on how certain aspects of the systems could be strengthened (see Table 2). It also sets out Poland's levels of compliance with the FATF 40 + 9 Recommendations (see Table 1). Compliance or non-compliance with the EC Directives has not been considered in the ratings in Table 1.

II. EXECUTIVE SUMMARY

1. Background Information

4. This report provides a summary of the AML/CFT measures in place in Poland as at the date of the third on-site visit from 14 to 21 May 2006, or immediately thereafter. It describes and analyses the measures in place, and provides recommendations on how certain aspects of the system could be strengthened. It also sets out Poland's levels of compliance with the FATF 40 + 9 Recommendations (see the attached table on the Ratings of Compliance with the FATF Recommendations).

5. The second evaluation of Poland took place in April 2002. At that time, Poland had only one money laundering conviction. The confiscation/forfeiture regime was very seldom used and there were significant concerns about the effectiveness of the Polish anti money laundering legal framework. Since then, several money laundering convictions have been achieved and overall the system seems to be working. Institutions are reporting, at least in connection with above threshold transactions. Approximately 80 % of money laundering investigations come from notifications received from the Polish FIU (the General Inspector of Financial Information - GIFI).

6. The majority of predicate offences for money laundering are considered to be economic frauds of various kinds (tax fraud, credit fraud), defrauding legal persons by their management, customs smuggling, production, smuggling and drug trafficking and corruption. With regard to economic offences, the largest illegal income is connected with lost Customs duties and taxes. Approximately 30 different methods for money laundering have been identified.

7. In 2002 the Polish Government initiated a so-called "Anti-Corruption Strategy" and as a consequence established a Central Anticorruption Bureau (CBA). Poland has taken appropriate steps to combat corruption, corruption in public administration and corruption in corporate activities, but considerable issues remain to be addressed.

8. Overall, certain elements in the Polish AML/CFT framework are missing, such as a common understanding by all stakeholders of the obligations under the Act of 16 November 2000 on Counteracting Introduction into Financial Circulation of Property Values derived from Illegal or Undisclosed Sources and on the Counteracting the Financing of Terrorism (hereinafter the AML Act) and a greater emphasis on the recognition, analysis and reporting of suspicious activity by obliged entities. Also more coordination of the main players in the AML system is needed to ensure a consistent approach.

2. Legal Systems and Related Institutional Measures

9. In July 2001, Article 299 of the Penal Code (the money laundering offence) was amended and now provides four offences. Art 299 para 1 is the broad money laundering offence based on an "all-crimes" predicate and - apart from the coverage of all types of activity which amount to terrorist financing - all the minimum categories of offences as referred to in the glossary to the FATF Recommendations are covered. The other three money laundering offences of Article 299 cover breaches of obligations in the preventive law by employees of various reporting institutions. Since the amendments of July 2001, an increasing number of preparatory proceedings has resulted in indictments and convictions. This refers both to cases conducted upon the notification of the FIU (which are the majority – about 80%) and cases commenced as a result of operational actions

of the Police. Cases conducted upon the notification of the FIU in which the money laundering offence has/could not been pursued are said, often to result in an indictment for another offence. From 2003 to 2005, there were 76 convictions under Art 299 para 1 Penal Code.

10. Concerning the physical elements of the money laundering offence, the evaluators are not convinced that possession, acquisition or use of property are covered in all their respects by the Polish legal framework.

11. Though there is only a slight difference between the penalty for the unaggravated form of money laundering (Article 299 para 1) and the penalties for the aggravated offences in Article 299 paragraphs 5 and 6, the sanctions for natural persons appear generally dissuasive. Criminal liability has been extended to legal persons and several types of sanctions can be applied but so far there is no experience with this new provision.

12. The ancillary offences of attempt, aiding and abetting, facilitating and counselling the commission of the money laundering offence appear to be adequately covered, but conspiracy to commit money laundering is not provided in the legislation (though it seems not to be contrary to fundamental principles of domestic law to introduce this offence).

13. Most cases appear to be self laundering and the difficulties of proving the predicate offence is often addressed by prosecuting the money laundering and the predicate in the same indictment. In this context, more emphasis should be placed on autonomous prosecution of money laundering by third parties.

14. Currently, there is no autonomous crime of "terrorist financing" in Poland and such behaviour could only be addressed on the basis of aiding and abetting an "act of terrorism". However, no terrorist financing prosecutions have been undertaken or cases brought before the courts and under current provisions it is difficult to see how funding a terrorist organisation could be prosecuted. Poland has recently initiated a legislative procedure aimed at introducing a separate financing of terrorism offence into the Penal Code.

15. The Polish legal framework covering provisional measures and confiscation has much improved since the second evaluation. Specifically since 2003, the confiscation provisions in Art. 44 and 45 of the Penal Code now provide for reversing the burden of proof in certain cases and in ensuring that title can revert to the Polish authorities in the event of a transaction intended to defeat confiscation (issues specifically identified in the last report). In the absence of statistics, it was unclear how frequently the regime was applied in practice – particularly in respect of indirect proceeds, value orders and orders in relation to third parties. The assessors are also concerned about implementation of the new procedures, especially as they relate to the identification and confiscation of indirect proceeds arising from an offence. Where instrumentalities subject to the regime under Article 44 have been transferred to third parties, it appears that confiscation is not possible.

16. Poland has the ability to freeze funds in accordance with S / RES / 1373 and S / RES / 1267 under European Union legislation though the definition of terrorist funds and other assets in the European Union Regulations do not fully cover the extent of the UN Resolutions, especially regarding the notion of control of funds. However, Poland has no clear legal provisions for implementing action against European Union internals, though the names of European union internals were available to the obliged entities with a view to freezing.

17. GIFI, which is an administrative type FIU, is the central body in the AML/CFT system of Poland. It is located in the Ministry of Finance. The unit employs 49 persons. All employees have higher education and technical employees have legal, economic or information technology education. Continuing training has become common practice.

18. The GIFI is financed from the funds allocated for the activity of the Ministry and the Polish authorities are of the opinion, that the position of the General Inspector as an Under-Secretary of State guarantees full operational independence and autonomy for the Polish FIU.

19. The FIU has a well resourced IT centre. It provides high quality training, which is well received by obliged entities. GIFI has prepared a guidebook for obliged entities. This is widely distributed, is well written and contains many typologies. The private sector confirmed that it is very useful. However, it is not a binding document. The FIU has also put very good efforts into training (including e-learning courses). The overall number of people trained is impressive.

20. The FIU is an active member of the Egmont group, and co-operates with more than 40 countries, though a memorandum of understanding is necessary to be signed in order to share information with Non-EU countries. The number of memoranda of understanding currently totals 33[2].

21. The Polish suspicious transactions reporting regime is rooted in the AML Act. Attempted transactions are not clearly covered in the Law. Also there is no provision explicitly addressing the issue of reporting transactions with a suspicion of the financing of terrorism, but the relevant provisions may be interpreted in the context of the overall purpose of the AML Act so that some aspects of the financing of terrorism are covered. This assumption is supported by the fact that the FIU received numerous terrorist-related reports. Overall GIFI processes a large amount of transactions, which are reported above the threshold of 15,000 Euro and a smaller number of received transactions which might indicate money laundering or terrorist financing. GIFI's analytical work in processing cases can be regarded as quite effective: e.g. in 2005, GIFI received and processed 20,921,317 reports concerning transactions above 15,000 Euro as well as 67,087 suspicious transactions reports concerning money laundering and 2,083 suspicious transaction reports related to terrorist financing; out of these, 175 cases have been passed to the public prosecutor with a suspicion of money laundering. However, banks remain by far the largest reporting obliged entities. Further outreach is strongly advised to some parts of the financial sector (particularly exchange houses) and the designated non-financial businesses and professions - DNFBP (particularly casinos) to explain the concept of suspicion in more detail.

3. Preventive Measures – financial institutions

22. The legal framework for AML/CFT preventive measures is – nearly exclusively – covered in two instruments, namely the AML Act and the "Regulation of 21 September 2001 on establishing the form of a register of transaction, the way of keeping the register and the procedure of conveying the registry data to the General Inspector of Financial Information". The AML Act is very detailed and covers a large number of financial institutions as "obligated institutions". The AML Act requires maintenance of a register and subsequent reporting of transactions above the threshold of € 15,000 (also when a transaction is executed involving more than a single operation, if circumstances suggest that these operations are linked together) and suspicious transaction reporting. Identification of customers who perform above threshold and suspicious transactions is regulated in detail and includes a list of required information, both for physical persons and legal entities.

23. Due to a rather formalistic approach to financial business, it seems that in practice the identification of customers is generally in line with FATF standards. However, the major difficulty is that several key elements of the customer due diligence (CDD) process as set out in the FATF Recommendations are insufficiently embedded in Law or Regulation. Particularly,

[2] as of 10 November 2006: 36.

there are no explicit legal requirements on the financial institutions to implement CDD measures when:

- establishing a business relationship;
- carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII;
- financial institutions have doubts about the veracity or adequacy of previously obtained identification data.

24. Neither the AML Act nor other laws (Banking Act, Insurance Act and Securities Act) require explicitly the verification of identification when starting a business relationship (though this is done in practice). Also other elements (such as risk analysis, identifying suspicion, the steps to take when the customer data is doubtful, the need for enhanced due diligence in higher risk situations such as non face to face relationships, and requirements in respect of legal persons such as companies on bearer shares, non-resident customers, private banking and PEPs) are missing.

25. Although there are regulations in respect of proxies, a definition of "beneficial owner" within the meaning of the FATF Recommendations is not in the AML Act nor in any other Polish normative act. As a consequence, there are no legal requirements to take reasonable measures to determine the natural persons who ultimately own or control the customer or the person on whose behalf transactions or services are provided by financial institutions. Supervisors as well as financial institutions do not see an obligation to go further than asking for possible powers of attorney, or other forms of proxy, and did not interpret the relevant provisions as encompassing the wider obligation that the FATF standards require.

26. There is no provision in the Act or any other law requiring financial institutions to consider making a suspicious transaction report when it is unable to complete CDD. The same applies for situations where a financial institution has already commenced a business relationship. There is also no requirement to terminate an existing business relationship when CDD is not completed.

27. Currently, Poland has not implemented any AML/CFT measures regarding the establishment of cross-border correspondent banking relationships, but it seems that, in practice, banks carefully select the respondent institutions before establishing new correspondent relationships. Inspections also show that if there is no customer data on the money transfer from abroad, the banks request their correspondent financial institutions to supply the information on the customer's identity.

28. There is no specific requirement in the law which requires financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not, or insufficiently apply, the FATF Recommendations. Only a manual issued by GIFI (entitled "Counteracting money laundering") contains a list of countries and geographical areas to which obliged institutions should pay attention in the area of suspicious transaction reporting.

29. Polish legislation does not provide a prohibition on financial institutions from entering or continuing correspondent banking relationship with shell banks. Financial institutions are also not obliged to satisfy themselves that a respondent financial institution in a foreign country does not permit its accounts to be used by shell banks. However, it seems that financial institutions follow these standards voluntarily and the inspections have not discovered any evidence of cooperation of any bank with a shell bank.

30. The sanctioning regime in the AML Act is a criminal one and its penalties are fairly strict, including imprisonment. As a result the examiners consider there is a risk that it will not be applied in other than in particularly egregious cases. The Polish authorities should consider an additional regime of complementary administrative sanctions, such as fines to enhance the AML/CFT compliance, especially in the non financial sector.

31. The financial sector supervisors (Banking Supervision Commission, Securities and Exchange Commission, Commission for Insurance and Pension Funds Supervision) seem to be experienced, well managed and to know the supervised entities well, inspect them regularly and provide a generally good framework of supervision, information, regulation and control. However, their engagement in AML/CFT supervision seems overly formal and very narrow, as they only see their role in inspections on site as based on a formalistic list of criteria. The onsite inspections are conducted as a formal check of the obligations mentioned in the law, without a material engagement with the less formal requirements of the Polish AML/CFT system, such as risk analysis, enhanced due diligence, ongoing monitoring of customers, monitoring of unusual and complex behaviour, and detection of suspicion. GIFI itself does not have the resources in personnel to effectively supervise the whole financial sector. This is an important gap.

32. Neither the AML Act nor any other law covers the registration and/or licensing of natural and legal persons that perform money or value transfer services. The Polish authorities explained this is due to the fact that Western Union and Moneygram, the companies active in Poland, act exclusively through banks as their agents. Money transfer services are also provided by the Polish Post, which is an obliged institution according to the AML Act. However, private sector representatives confirmed that bureaux de change are also contracting with Western Union. There seems also to be an important gap in this area with regard to the awareness of the authorities, which means that this internationally well-known high risk area is not adequately addressed in the Polish system.

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

33. The coverage of DNFBP in the AML Act is very complete and in line with both international standards and the first and second EU Directives. It comprises casinos, notaries public, legal advisers, statutory auditors, tax advisers, auction houses, antique shops, precious metals and stones traders, commission sales business, pawnshops, real estate agents. Additionally, the Polish Post and foundations, which are not required by international norms, have been included. The CDD requirements, so far as they go, (if and when) applicable to DNFBP are more or less the same as those applicable to financial institutions, since the core obligations for both DNFBP and financial institutions are based on the same law (the AML Act). However, the evaluators were concerned that CDD requirements do not apply to accountants; also real estate agents, counsel, legal advisers and foreign lawyers are only partially covered, as they have to register only suspicious transactions (but not above threshold transactions).

34. The engagement and understanding of DNFBP in the AML/CFT regime is very uneven; e.g. casinos are quite unconcerned about ML/FT risks in their field and lawyers, tax advisers and auditors remain unhappy with their obligations. As a consequence, the number of STR received from this part of the DNFBP sector is quite small. The supervision of DNFBP is performed by GIFI, the Minister responsible for public finances (concerning entities organizing and operating games of chance, mutual betting, automatic machine games and automatic machines games with low prizes) and the Presidents of Appeal Courts (concerning notaries public). The GIFI seems to have made a strong effort to inform associations or representatives of DNFBP when they became obliged entities under the AML Act, but the private sector does not perceive continued follow up on this issue by GIFI. A few onsite inspections have been made.

35. As with financial institutions, the sanctioning regime of the AML Act for DNFBP is disproportionate for minor cases (only criminal sanctions are provided for), which carries the risk that it is not applied and reduces its effectiveness. This might also be a reason that only few sanctions have been imposed as yet. In addition, the competences of the sanctioning authorities are at least unclear and should be clarified to avoid double or no sanctioning.

5. Legal Persons and Arrangements & Non-Profit Organisations

36. Polish legislation covers profit-oriented entities, non-profit companies and foundations.

37. According to Polish laws only the following types of profit-oriented entities can be established: registered partnerships, professional partnerships, limited partnerships, limited joint-stock partnerships, limited liability companies and joint-stock companies.

38. Non-profit companies may be established for serving public purposes and interests as non-governmental organisations. The NPO sector comprises corporate and non-corporate entities not forming part of the public finance sector, not operating for profit, and formed under relevant legislative provisions, including foundations and associations, religious organisations and unions and also local authority unions.

39. Polish law requires 16 different types of entities to be registered (meaning both profit-making companies as well as NPOs; e.g. limited liability companies, joint stock companies, European companies cooperatives, state enterprises, branches of foreign enterprises etc.). The Register is kept in electronic form by district courts (Commercial Courts of Law). It is divided into sub-registers which separately cover entrepreneurs, non-profit companies, and foundations. Everyone has the right to access data from the Register through the Central Information and also to receive certified copies, excerpts and certificates on data included in the Register.

40. Polish Law contains no clear legal provisions to register the beneficial ownership of companies as it is defined in the Glossary to the FATF Recommendations (i.e. those who ultimately own or have effective control). Beneficial ownership information is also not available in relation to foreign companies which are registered in Poland. In some cases, information on beneficial ownership may be available in the company's books at the registered office. Though Polish authorities can in practice rely on investigative and other powers of law enforcement to produce from company records the immediate owners of companies, it would be a lengthy and difficult process for the investigative authorities to gather such information (and in some cases not even possible if the competent authorities have to investigate up the chain of legal persons).

41. Though there are procedures in place to ensure some financial transparency, it appears there has been no special analysis of the risks in the NPO sector to be abused for financing of terrorism. The Polish authorities should review the adequacy of the current legal framework relating to this sector.

6. National and International Co-operation

42. The AML Act is the legal basis for cooperation between the entities involved in counteracting money laundering. It defines the obligations on state and local administration authorities and other state organisational units to cooperate within the scope of their competence with the GIFI. Poland established in February 2006 a "horizontal working group for international sanctions". Its main responsibility is focused on legal aspects of implementation of international sanctions. However, it seems that at the national level the existing coordination measures are not completely effective; e.g. the GIFI does not provide information directly to the police, which must obtain such financial data through the public prosecutor. It would be helpful to have more coordination of the main AML/CFT players to ensure a consistent approach.

43. Mutual legal assistance is regulated by Chapter 62 of the Code of Criminal Procedure. Poland has ratified *inter alia* the Vienna Convention and the Palermo Convention. In addition, Poland has ratified the European Convention on Mutual Assistance in Criminal Matters (ETS 030) and its two Additional Protocols (ETS 99 and ETS 182). Also several bilateral agreements/treaties have been concluded under which mutual legal assistance may be afforded. Due to provisions of the Code of Criminal Procedure, courts and prosecutors shall refuse assistance if the requested action conflicts with the legal order of Poland or constitutes an infringement of its sovereignty. Dual criminality as well as a lack of reciprocity are reasons to deny assistance. However, the assessors were assured that this discretionary provision was rarely applied in practice.

44. Poland does have appropriate laws and procedures to seize, freeze and forfeit objects, instrumentalities, direct and indirect proceeds on behalf of foreign countries. Additionally, as a European Union member state, Poland has implemented the European Union framework decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence.

45. Poland is a party to numerous multi- and bi-lateral agreements dealing with Extradition, 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 Convention of 27 September 1996 relating to extradition between the Member States of the European Union (1996 EU Extradition Convention). Poland has implemented the European Arrest Warrant, which introduced a legal basis that – in principle - Polish nationals can be returned within the European Union for money laundering and terrorist financing without a strict application of the dual criminality principle. However, as the Polish Constitutional Tribunal stated that the relevant provision of the Criminal Procedure Code, insofar as it permits the surrendering of a Polish citizen to another Member State of the European Union on the basis of the European Arrest Warrant, does not conform to Article 55(1) of the Constitution, it is questionable if it is possible to extradite Polish nationals[3]. Aside from this uncertain situation concerning the extradition of Polish nationals, money laundering is an extraditable offence. The lack of an autonomous Terrorist Financing offence would make extraditions for all relevant conduct at least difficult. Notwithstanding this, the team was assured, that mutual legal assistance in respect of Terrorist Financing could be rendered more flexibly as the dual criminality requirements are optional rather than mandatory.

[3] Polish authorities informed that the Constitution was amended on 8 September 2006 (entering into force on 7 November 2006) and that this shortcoming no longer applies.

III. Mutual Evaluation Report

1 GENERAL

1.1 General information on Poland and its economy

46. The Republic of Poland (hereafter "Poland") is located in Central Europe and is bordered by Germany, the Czech Republic, Slovakia, Ukraine, Belarus, Lithuania and Russia (in the form of the Kaliningrad Oblast exclave). It shares a maritime border with Denmark and Sweden in the Baltic Sea. The area of Poland is 312,685 sq. km. It has a population of 38,5 million people.

47. The capital, Warsaw, is well connected with the main European cities: it takes about two hours by plane to get to Paris or London and not more than one hour to reach Vienna or Berlin. Mobile phone networks cover 94% of the country.

48. The GDP of Poland (first quarter 2004 to first quarter 2005) is 2,1%. The inflation (February 2005 to February 2006) is 0,7 %. Since the turning point of 1989, Poland has undergone great political, social and economic changes: the introduction of democratic structures, the shift from a command economy to the free market and wide-ranging systemic reforms. During the period of transformation the Polish economy was still in a difficult state and radical reforms were selected as the only solution to change the situation. The Poles were very active in the liberalisation of the international trade. As a result of hyperinflation in the early 1990s, the decimal point on the currency was moved by four places: on 1 January 1995, 10,000 old złotych (PLZ) became one new złoty (PLN). Now the złoty became convertible to other currencies and internal convertibility was also established, providing another platform for dynamic economic growth. The Polish government focused in the past very much on economic growth to catch up with the developed economies of Europe and the rest of the world. New markets in countries previously closed to Poland were opened up to Polish companies. Since May 1, 2004, Poland is a member state of the European Union and now the European Union and the USA are the key directions in which Polish goods are exported. The reforms of the transition period and subsequent hard and consistent monetary policy gave the Polish economy solid foundations. Now it has a strong currency and consistently falling inflation. Liberalisation and stabilisation were accompanied by structural reforms. Banking and lending policies were reformed, which together with newly reshaped ownership relations, independent enterprises and strengthened domestic competition all had great impact. Capital and labour markets also started to operate in Poland.

49. The implementation of systemic reforms and responsible government policies, as well as improved global competitiveness, mean that Poland anticipates fast-track economic growth. Although the Polish economy is currently progressing, it has to be noted that there are still many challenges ahead. Currently Poland is preparing its economy to meet the strict economic criteria to join the Eurozone.

50. Foreign capital represents a significant factor in the banking sector (see below).

51. As a European Union member, any of the structural elements set out in paragraph 7 of the AML/CFT Methodology, which might significantly impair implementation of an effective AML/CFT framework are being addressed.

52. Poland had signed but not ratified and implemented the 2003 United Nations Convention against Corruption at the time of the on-site visit[4]. Furthermore it has signed and ratified the Council of Europe Criminal Law Convention on Corruption (CETS 173; signed on 27 January 1999, ratified on 11 December 2002), the Council of Europe Civil Law Convention on Corruption (CETS 174; signed on 3 April 2001, ratified on 11 September 2002), and the European Union Convention on the Fight against Corruption involving Officials of the European Communities or Officials of the European Union Member States (OJ 97/C 195/01 25.6.97 ; ratified on 25 January 2005). The following instruments to prevent and combat corruption are in force:
    - Act of 21 August 1997 on the restriction to carry out economic activity by persons performing public functions (Dz. U. No 106, item 679 as mended, referred to as the Anti-corruption act);
    - Act of 9 June 2006 on the Central Anticorruption Bureau;
    - Law On Civil Service of 24 August, 2006 and the Law on Staff Resources and exposed Public Officials of 24 August 2006;
    - The Civil Service Code of Ethics.

53. On 17 September 2002, the Polish Government adopted the "Anti-Corruption Strategy", which is a collection of target solutions and set of actions to be undertaken by government administrations in combating corruption. Poland has established a so-called Central Anticorruption Bureau (CBA) which is planned to become a new secret service of the state with a mission to supervise the observance of anticorruption regulations; this involves for example checking the assets of public officials and whether they comply with the ban on combining public functions with economic activity. The CBA is also supposed to examine privatisation and commercialisation procedures as well as procedures connected with providing financial support to businesses and awarding public contracts, licenses, permits and tax exemptions. Since 20 May 1999, Poland has been a member of the Group of States against Corruption (GRECO), and has been evaluated by GRECO. Pursuant to GRECO's Second Round Evaluation Report on Poland (2004), the country has taken appropriate steps to establish an adequate legislative framework to enable the competent authorities to cope with issues related to proceeds of corruption, corruption in public administration and corruption in corporate activities. On the other side it was noted that a higher degree of specialisation and specific training is needed for prosecutors and police officers in order to enable them to fully implement provisions on seizure and confiscation of proceeds of corruption. Furthermore, it was considered that the success of corruption prevention policies in public administration could be strengthened, notably, by regular monitoring and updating of implementation and the regulation of conflicts of interest. The provisions of the "Act of 28 October 2002 on the Liability of Collective Entities for Acts Prohibited under Penalty" (Annex 2) were considered to meet to a large extent the standards laid down in Article 18 of the Criminal Law Convention on Corruption.

1.2 General situation of money laundering and financing of terrorism

.

54. The Polish authorities advised in their replies to the questionnaire that the predicate offences for money laundering mainly involve economic frauds of various kinds (tax fraud, credit fraud), defrauding legal persons by their management, customs smuggling, production, smuggling and drug trafficking and corruption. With regard to economic offences, the largest illegal income is connected with lost Customs duties and taxes. This encompasses in particular any kind of fraud

[4] Poland ratified the Convention on 15 September 2006.

connected with dealing in fuel and scrap-metal. The most often reported suspicious transactions consist in flows of funds associated with tax fraud connected to actual or fictitious trade in fuel, mainly liquid fuel, and components used in its production. From 2001 to 2005, the Polish FIU investigated 317 so-called "fuel fraud cases". Based on the outcomes of these investigations, GIFI submitted 179 reports to the prosecutor's office. The estimated value of the transactions was 1.763,2 million PLN (approx. 450 million Euro). Another category detected by the Polish authorities as suspicious operations involves trade in scrap metal and recyclable materials (basically VAT tax fraud). Apparently, the perpetrators act in the same manner as in the "fuel fraud cases". The FIU has identified approximately 30 different methods for money laundering at placement, layering and integration stages. The most popular among them are reported to be the following:

1) ***Legalisation of funds derived from crime through loans and donations -*** This method is based on an agreement concluded between two or more natural or legal persons who or which draw up a fictitious loan or donation contract. Afterwards they register it in the Inland Revenue Office and pay the due tax levied on the civil law actions.
2) ***Blending of revenues –*** This method is characterised by blending proceeds from legal business activity with funds derived from illegal or undisclosed sources. In the first place the method is used in such economic activities where it is difficult to predict the value, e.g. seasonal revenues.
3) ***A fictitious account*** – The perpetrators open an account to conduct one or several transactions within short time intervals for very high amounts, using the maximum number of fictitious data of both persons conducting the transaction and documents that these persons use.
4) ***Distribution box*** - A distribution box typically consists of depositing small amounts of money on a given account so as not to exceed the Polish threshold for registration of transactions (see beneath). These deposits usually derive from various sources (rarely from one source only). The funds are transferred usually electronically when they are about to reach the level of threshold reporting.
5) ***Target account -*** This method is characterised by a transfer of large amounts of funds to one banking account, from which they are immediately withdrawn in cash. In this case withdrawal of cash concludes a certain preconceived money laundering "path". The transfers to a final account are of course preceded by a number of operations (which are an integral part of this method) to impede or to prevent identification of a illicit origin of financial means.
6) ***Purchase and sale of fixed assets -*** This method involves integration of illicit proceeds into fixed assets, such as premises, machines, equipment and means of transport. Funds from illegal sources may also be introduced into financial circulation by under pricing or overpricing of such assets.

55. Since the amendment of Article 299 of the Penal Code (the money laundering offence) in July 2001, an increasing number of preparatory proceedings has resulted in indictments and convictions. This refers both to cases conducted upon the notification of the FIU (which are the majority – about 80%) and cases commenced as a result of operational actions of the Police. Cases conducted upon the notification of the FIU in which the money laundering offence has/could not been pursued are said, often to result in an indictment for another offence. The Polish authorities mentioned in their replies to the questionnaire that their key problems connected with money laundering cases include the (long) time needed for mutual legal assistance and the necessity to carry out fiscal inspections in order to identify untaxed sources of income, where the underlying offence involves tax losses. In this event, it is said that the money laundering cases are suspended until the time of the final, lawful and binding decision in the tax case.

56. The General crime statistics for 2001 - 2006 have been provided by the Polish authorities and are set out beneath:

	Affirmed	Suspected	Detecting
2005	1.379.962	594.088	58,6
2004	1.461.217	578.059	56.2
2003	1.466.643	557.224	55.2
2002	1.404.229	552.301	54.9
2001	1.390.089	533.943	53.8

	Roads	Criminal	Economic
2005	196.486	1.000.096	136.801
2004	177.296	1.085.295	152.148
2003	168.827	1.101.387	151.596
2002	163.012	1.083.854	109.698
2001	138.817	1.107.073	103.521

Suspected persons

	Murder	Rape	Damage of body	Participation in scrimmage or beating	Theft	Robbery crimes	Theft with burglary
2005	861	1.183	9.665	22.163	59.026	21.151	31.778
2004	970	1.253	10.008	22.081	62.256	22.793	35.920
2003	1.015	1.449	9.857	21.402	55.179	23.212	38.603
2002	1.206	1.476	10.431	22.175	55.142	22.909	43.951
2001	1.274	1.524	10.129	22.369	55.118	24.680	48.888

57. Turning to the situation of financing of terrorism, first of all it has to be noted that the Polish legal framework provides no autonomous offence of terrorist financing, although the Ministry of Justice has already prepared amendments to the Polish Penal Code introducing an autonomous offence of financing terrorism. Such action can only be addressed by the provisions on aiding and abetting the commission of a terrorist act. So far no proceedings on financing of terrorism have been brought in Poland and criminal justice administration bodies do not have any experience in this area. Nonetheless the examiners noted that the Polish FIU is very active in the CFT field. It responds to all signals from obliged institutions and cooperating units about transactions for which there are suggestions of a possible connection between the transferred funds and the financing of terrorism, including transactions carried by Islamic non-profit organisations. In particular this includes cases of cash being brought to Poland by people arriving from countries suspected of supporting terrorism and electronic transfers from such countries. In these matters the FIU co-operates with the Internal Security Agency and the Prosecutors. The FIU also participates in the work of many international

bodies such as Financial Services Working Group, Working Group on Terrorism (international aspects), Working Group on Terrorism, Multidisciplinary Group on Organised Crime, the sessions of EGMONT Group, Task Force on Organised Crime in the Baltic Sea Region (BALTCOM) and the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL).

58. 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). As will be seen below, Poland generally follows the European Union implementation of the United Nations Security Council Regulations. Nevertheless it has to be noted, that there has been no real risk assessment of the potential for abuse of the non-profit sector from the point of view of financing of terrorism.

1.3 Overview of the financial sector and Designated Non-Financial Businesses and Professions (DNFBP)

Financial Sector

59. Article 2 of the Act of 16 November 2000 on Counteracting Introduction into Financial Circulation of Property Values derived from Illegal or Undisclosed Sources and on the Counteracting the Financing of Terrorism (hereinafter the AML Act, Annex 1), covers the following financial institutions (numbers in brackets):
    1) banks, foreign bank branches (69)
    2) the National Bank of Poland – where it operates bank accounts of legal persons, numismatics sales, purchases gold and exchanges damaged legal tender in accordance with the provisions of the law of 29 August 1997 on the National Bank of Poland (Journal of Laws No. 140, item 938 with subsequent amendments) (1)
    3) electronic money institutions, branches of foreign electronic money institutions and settlement agents on the basis of the Law of 12 September 2002 on electronic instruments of payment (Journal of Laws No. 169, item 1385) (0)
    4) investment companies and custodian banks (56)
    5) Joint Stock Company National Depository for Securities S.A. as far as it keeps securities' accounts (1)
    6) insurance companies, the main branches of foreign insurance companies – 67
    7) investment funds (approx. 170)
    8) investment funds societies (23)
    9) co-operative savings and credit unions (73)
    10) the state public utility enterprise Polish Post (1)
    11) entities engaged in currency exchange (3,852)
    12) entities conducting leasing and factoring activity (450).

Banking sector

60. On the territory of Poland 69 commercial banks and 588 cooperative banks conduct activities. Eleven banks are controlled by Polish investors, 43 by foreign investors and 7 are branches of credit institutions. The sum of the banks' own funds as of 31 December 2005 was PLN 45 700 million (EUR 11 840 million) and their net assets were PLN 587 000 million (EUR 152 100 million[5]).

[5] 1EUR=3,8598 PLN (as of 30 December 2005)

Polish capital market

61. The following types of financial institutions operate on the Polish capital market: the Warsaw Stock Exchange – operating the regulated market; MTS-CeTO – operating the regulated over-the-counter market; the National Depository for Securities (all of these institutions operate in the legal form of a joint stock company); brokerage houses; banks conducting brokerage activity; foreign investment firms; custodian banks; investment fund companies; investment funds; investment firms agents (tied agents); depository banks. The Polish Securities and Exchange Commission (PSEC)[6] exercises the supervision over these entities. The activities performed by these entities are defined in the Act on capital market supervision, the Act on trading in financial instruments and the Act on investment funds.

Insurance undertakings

62. The insurance undertakings carry out insurance activities. The performance of insurance activities requires the consent of the supervisory authority. From among domestic insurance undertakings 32 life insurance undertakings and 35 non-life undertakings carry out operating activities. During the first nine months of 2005 the gross premiums written, which constitute the main source of income for insurance undertakings, amounted to PLN 22.69 billion and were 10.70% (PLN 2.19 billion), higher than the same period in 2004. The share of the five largest insurance undertakings in the first three quarters of 2005 amounted to 73.62% of gross premiums of segment I (life insurance) and 77.44% of premiums of segment II (non-life: other personal insurance and property insurance).

Foreign Exchange business providers

63. As of 31 December 2005, there were 3 852 bureaux de change operating in Poland. According to Chapter 9 of the Foreign Exchange Law the control is exercised by the National Bank of Poland.

DNFBP

64. The major DNFBP are as follows:

1) entities conducting activity involving games of chance, mutual betting and automatic machine games, and automatic machine games with low prizes – 140 entities and 27 casinos,
2) notaries public insofar as dealing in property values is concerned – 1,550
3) counsellors performing their profession ("performing their profession" means that the lawyers are active; the regulation does not concern lawyers who have only a title "counsellor") – 5,500,
4) legal advisers performing their profession outside their labour relationship – 25,000
5) foreign lawyers rendering legal aid outside their labour relationship – 66
6) competent auditors performing their profession – 3,000,
7) tax advisers performing their profession – 11,000,
8) entrepreneurs running auction houses – 30,
9) antique shops – 155
10) activity in the scope of precious and semi-precious metals or stones trade – 2,014
11) commission sale – 900

[6] Since 19 September 2006 "Polish Financial Supervisory Authority" (merger of PSEC and Commission for Insurance and Pension Funds Supervision - based on the Act of 21 July 2006 on supervision of the financial market, O.J. No 157, item 1119).

12) giving loans on pawn (pawnshops) – 1,453
13) real estate agents – 4,150
14) foundations – 5,700;
15) trust services companies – not applicable.

65. The regulation concerning supervision of casinos is covered by Articles 49 and 50 of the Act of 29 July 1992 on Games and Mutual Bets (Journal of Laws of 2004 No. 4, item 27; Annex 3), as well as Articles 2 and 8 (subsection 1a) of the AML Act. According to Articles 21 and 41 of the AML Act, the compliance with the rules in this Act is under the supervision of GIFI.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements

66. The general rules concerning the setting up and the operation of companies are mainly set out in three laws, namely the Act of 15 September 2000 ("The Code of Commercial Partnerships and Companies"), the Act of 2 July 2004 on Freedom of Economic Activity and the Act of 20 August 1997 on the National Court Register (see Annexes 4, 5 and 6).

67. The Code of Commercial Partnerships and Companies regulates the main duties in the area of formation, operation and transformation of profit oriented entities. The Polish law deals with the following types of entities (Article 2): registered partnerships, professional partnerships, limited partnerships, limited joint-stock partnerships, limited liability companies and joint-stock companies. In June 2006, there were 199,791 limited liability companies, 55,845 Joint stock companies and 2,761,558 natural persons leading a business activity operating in Poland.

68. Non-profit companies may be established for serving public purposes and interests as non-governmental organisations. These are defined in Art. 3, para. 2 of the Act of 24 April 2003 on Public Benefit and Volunteer Work as corporate and non-corporate entities not forming part of the public finance sector, as described in the Public Finances Act, not operating for profit and formed under relevant legislative provisions. They include foundations and associations. Furthermore, also corporate entities and organisations operating under provisions on relations between the State and the Catholic Church in the Republic of Poland (and other churches also) may engage in public benefit work, but their statutory objectives must encompass public benefit work. Also local authority organisation unions may act as NPO. Foundations may be formed for public interest, or religious purposes by statute of foundation and executed by the founders.

69. When required by Polish law, any legal entity (meaning both profit-making companies as well as NPOs), may be registered under conditions prescribed by the Act of 20 August 1997 on the National Court Register. The Register is divided into sub-registers which separately cover entrepreneurs, non-profit companies, and foundations. The National Court Register is held and maintained by the Supreme Court.

70. Registration regarding certain forms of entities is not only declarative, but also of constitutive nature. This means the company comes into being not by the simple deed of foundation, but by decision of the Court ordering its incorporation.

71. According to Article 12 of the Code of Commercial Partnerships and Companies upon entry into the register, a limited liability company in organisation or a joint-stock company in organisation shall become a limited liability company or a joint-stock company and gain legal personality.

72. Under Article 14 of the Act on Freedom of Economic Activity, entrepreneurs may undertake economic activities after they have been registered in the Register of Entrepreneurs in the National Court Register or in the Economic Activity Records (hereinafter "Records") which are

kept by the commune competent for the entrepreneur's place of residence. Entry in these Records is required in the case of natural persons who conduct economic activity. In accordance with Article 13 par 1 of this Act, foreign persons from the European Union Member States or the European Free Trade Association (EFTA) member countries – parties to the European Economic Area Agreement may undertake and conduct economic activity on the same terms and conditions as Polish entrepreneurs. In this context, foreign persons means "*a) a natural person with the place of permanent residence outside of the Republic of Poland and without Polish nationality; b) a legal person with its registered office abroad; c) a non-corporate organisational unit with legal capacity and with its registered office abroad*" (Article 5 para. 2 and Article 13 para. 3 state that other foreign persons have the right to undertake and conduct economic activity only in the form of a limited partnership, limited joint-stock partnership, limited liability company and joint-stock company, as well as to join such partnerships and companies and to take over or acquire shares in these entities, unless otherwise provided for in international agreements.

73. Poland has not signed the Convention on the Law applicable to Trusts and on their Recognition (1 July 1995, the Hague).

1.5 Overview of strategy to prevent money laundering and terrorist financing

a. AML/CFT Strategies and Priorities

74. It can be noted, that the Polish Government has given careful consideration to the combating of money laundering and financing of terrorism and seeks to implement all the new international standards to the extent possible subject to available legal, financial and human resources. Since the 2nd Round Evaluation the number of investigations, indictments and convictions for money laundering cases has increased. The STR/CTR reporting system is impressive in terms of received reports, e.g. in 2005 the FIU (the General Inspector of Financial Information – GIFI) received 20,988,959 reports (67,642 STR and 20,921,317 CTR). After analysing these reports, GIFI initiated 973 analytical proceedings, demanded suspension of five transactions (for the total amount of PLN 1.6 million; ca. 417,000 Euros), demanded blockade of 34 accounts (connected with suspicious transactions for the total amount of PLN 36 million; ca. 9,4 million Euros) and submitted 175 notifications to the public prosecutor's office on suspicion of the crime as defined in Article 299 of the Penal Code. The effectiveness of a system dealing with such an enormous amount of reports is discussed below. It is also noted with approval that GIFI has undertaken considerable outreach to the designated non-financial businesses and professions (DNFBP).

75. Since its accession to the European Union, Poland has participated in decision-making on new regulations and measures to be adopted by the Member States. The representatives of the GIFI actively participated in the preparation of the 3rd EU Directive on money laundering. Poland also participates in other fora, such as the working groups of the Egmont Group, PC-R-M Committee of the Council of Europe (which negotiated the 2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS no. 198), typological meetings of MONEYVAL and FATF.

76. The GIFI is required to present the President of the Council of Ministers annual reports on his activities within 3 months from the end of the reporting year. The report shall contain information on activities undertaken, statistical data and commentary referring to phenomena and trends observed. Moreover, the GIFI:
    - prepared and published for internal use a guide for obliged institutions and co-operating units, entitled "Counteracting money laundering" (in 2005 the second, revised edition was published),
    - presents information on its activity in inter-ministerial, inter-sectoral and international conferences and meetings.

77. Also the General Inspectorate of Banking Supervision (GINB) monitors compliance with the law and shares with the GIFI information related to counteracting money laundering which was obtained during the inspections in the banks or during the analytical supervision.

78. Numerous authorities are involved in the AML/CFT issue, though co-ordination of the main players in the system would benefit from further consideration to ensure a more consistent approach. It may be helpful to constitute a permanent working group of senior representatives of the key institutions to examine strategically the performance of the system as a whole. This issue is taken up below in sections 3.10, 4.3 and 6.1.

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

79. The following are the main bodies and authorities involved in combating money laundering or financing of terrorism:

The National Bank of Poland

80. The role of the National Bank of Poland (NBP) is twofold: On the one hand, pursuant to Article 2 (para. 1) of the AML Act, the NBP belongs to the category of obliged 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.

General Inspectorate of Banking Supervision

81. The General Inspectorate of Banking Supervision is the executive body of the Banking Supervision Commission which is responsible for supervision and licencing of banks.

Commission for Insurance and Pension Funds Supervision

82. This commission is responsible for supervision and licencing of insurance undertakings.

Securities and Exchange Commission

83. This Commission is responsible for supervision and licencing of investment companies, investment funds and investment funds companies.

National Association of Credit and Savings Unions

84. The National Association of Credit and Savings Unions is a co-operative society of legal persons which's objective is to supervise credit unions.

Ministry of Interior

85. 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 carries out

tasks ordered by the public prosecutor. In accordance with the AML Act, the Police is obliged to inform the FIU of every initiation of preparatory proceedings in the AML/CFT field.

Ministry of Finance

86. A wide range of responsibilities of the Polish Ministry of Finance relate to AML/CFT issues. Firstly, 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. The GIFI is a Deputy Minister who is also Head of Fiscal Control. There is also a Director of the FIU who is the day to day Head of the Office. The Customs Services are also in the structure of the Ministry of Finance. They deal 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). Furthermore, 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.

Ministry of Foreign Affairs

87. The Ministry of Foreign Affairs (MFA) provides general co-ordination of internal policy in relation to international sanctions (including combating terrorism). The representatives of MFA participate in the meetings of international bodies responsible for imposition of international sanctions (e.g. UN, EU Council, OSCE), and are involved in the decision-making process. 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. In order to facilitate co-ordination in the Ministry, in February 2006, a horizontal working group for international sanctions was established.

Ministry of Justice

88. 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

89. The tasks of the public prosecuting authorities have been formulated in the Law of June 20, 1985 on Public Prosecution Authorities. The Prosecutor General is the chief prosecuting authority, to which prosecutors of common and military structural units of prosecuting authorities are subordinated. The function of the Prosecutor General is performed by the Minister of Justice**.** The Prosecutor General manages the activities of the public prosecution office personally or through his deputy, issuing regulations, guidelines and orders. He may also undertake all and any activities belonging to the scope of activities of public prosecution or recommend their performance by subordinated prosecutors, unless the Law provides that such activity may be performed by the Prosecutor General personally.

90. In performing their activities and as provided for in the applicable laws, the work of public prosecutors should be guided by principles of neutrality and equal treatment of all citizens. *External* independence of the public prosecutor is guaranteed by Art. 8 para. 1 of the Law on the System of Public Prosecution. External independence means in this context that the public prosecutor will act independently of any other authorities or persons. By contrast, *internal* independence is greatly restricted and the prosecutors are bound by instructions of the superior public prosecutors.

91. The structure of the Public Prosecuting Authorities is as follows:
    - *Prosecutor General*
    - *National Public Prosecution Office*, which is organisationally incorporated into the Ministry of Justice, managed by the National Public Prosecutor, being at the same time a deputy to the Prosecutor General. The National Public Prosecution Office consists of four departments, managed by Directors, i.e. :
        a. The *Preparatory Proceedings Bureau:* Its basic task is the coordination of official supervision over preparatory proceedings performed within appellate public prosecution offices,
        b. The *Organised Crime Bureau* was established for the purpose of coordinating prosecution in this form of crime and for international cooperation in combating organised crime,
        c. The *Judicial Proceedings Bureau* performs the prosecuting tasks associated with participation in proceedings before the Supreme Court and Supreme Court of Administration, and in cases of reprieve,
    - The *Presidential Bureau* performs organisational functions of the National Public Prosecution.
    - 11 *appellate public prosecution offices* managed by appellate public prosecutors;
    - 44 *regional public prosecution offices* managed by regional public prosecutors (5 of these cover an area of more than one voivodship[7]);
    - 325 *district public prosecution offices* managed by district public prosecutors.

c. The approach concerning risk

92. As described in the FATF Recommendations, a country may decide not to apply certain AML/CFT requirements, or to reduce or simplify the measures being taken, on the basis that there is low or little risk of money laundering or financing of terrorism. Turning to higher risk situations such as non face to face relationships, legal persons such as companies on bearer shares, non-resident customers, private banking and PEPs, it has to be noted, that enhanced due diligence is currently missing. On the other side, there are also only a few examples of the application of simplified measures in lower risk situations. Generally Polish provisions do not allow for simplified customer identification or departure from the obligation to register transactions carried out by the entities classified by a bank as belonging to the category of low risk of money laundering or terrorist financing. However, there are some exceptions from the obligation to register transactions in certain cases, some of which are problematic (as discussed beneath under section 3.2).

93. The Polish authorities are making efforts to implement "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" ("Third anti-Money Laundering Directive") and *inter alia* its obligation to implement provisions for exercising simplified due diligence, and thus are addressing this issue.

d. Progress since the last mutual evaluation

94. The last on site visit took place in April 2002. At that time the Polish authorities could report only one money laundering conviction. Moreover, the regime of confiscation/forfeiture was very seldom used to deprive the perpetrators of the proceeds of their crime. Consequently, in the

[7] Voivodship is a Polish geographical unit of administration.

second round evaluation report the effectiveness of the Polish anti money laundering legal framework was questioned.

95. Since then money laundering cases being prosecuted and also convictions (seven in 2003, 24 in 2004) have been increasing. One concern of the (then) evaluators was the level of proof required to demonstrate that the proceeds in question derived from a relevant predicate offence (which was already mentioned by the evaluators of the first round). It seems that it is still not yet solved what level of proof is required in respect of the underlying predicate offence(s). This might, together with the absence of jurisprudence from the Supreme Court, be a reason why the majority of money laundering cases appear to be self laundering.

96. The confiscation regime appears now to be much more soundly based and some provisions are much improved since the second evaluation. Specifically since 2003, they now provide for reversing the burden of proof in certain cases and in ensuring that title can revert to the Polish authorities in the event of a transaction intended to defeat confiscation (issues specifically identified in the last report). In the last report was mentioned that the confiscation, post conviction, of indirect proceeds was very much an exception due to various reasons (*inter alia* absence of sufficient focus on proceeds in the course of investigations, lack of sufficient law enforcement expertise, insufficient funds to properly resource often expensive and complex financial investigations, and inadequacy of existing budgetary provision to cover the costs associated with the management of assets subject to provisional measures). Though in the absence of relevant statistics it could not be clarified if this situation has changed and how frequently these new provisions are applied now in practice.

97. The examiners both from the first and also from the second round recommended the Polish authorities to consider the introduction of the concept of corporate criminal liability into the Polish legal system. Since then this recommendation has been met and corporate criminal liability is covered by the Act of 28 October 2002 on the Liability of Collective Entities for Acts Prohibited under Penalty (Annex 2). However, till now there is no experience with these new provisions.

98. Further progress can be seen in the position of Poland concerning international co-operation in confiscation issues. While at the time of the second on site visit dual criminality was a mandatory ground for refusal, it is now only a discretionary reason. Furthermore, the assessors learned that this discretionary provision was rarely applied in practice.

99. Although there was an increasing trend, the suspicious transaction reports were regarded in the last report as relatively few in number; most reports came from a small number of institutions in the banking sector, and only very few reports from brokerage houses, and none from bureaux de change. This situation has changed only slightly. Most of the reports still come from banks. It could not be clarified whether the spread of reporting across the banking sector was now more even. However, whereas at the time of the last on site visit the FIU received only 21 suspicious transaction reports from brokerage houses and insurance firms, it increased in 2005 up to 72 (see section 2.5). On the other side, bureaux de change, casinos, dealers in precious stones / metals and some other DNFBP have not forwarded any suspicious transaction report to the FIU. Hence, there is still a need for greater outreach to some parts of the financial and non banking financial sector to ensure that they are reporting adequately.

100. The last evaluators were not convinced that the FIU always was provided with the relevant information by the law enforcement authorities. Particularly, they recommended that clear procedures be established in order to ensure that the FIU receives all relevant information also on money laundering cases not emanating from a suspicious transaction report. Also the present evaluators got the impression that the law enforcement authorities' approach to money laundering issues is quite minimalist and that they are reactive mainly to notifications from the

FIU; also the number of police generated money laundering cases is quite unclear. To improve the performance of the Police in generating money laundering cases outside of the reporting regime a specialised money laundering Unit should be considered.

101. A major concern of the last evaluators was that neither the AML Act nor the Banking Act provided clear provisions requiring customer identification at the time of opening an account. It is disappointing that still neither the AML Act nor other laws (Banking Act, Insurance Act and Securities Act) require explicitly the identification of clients when starting a business relationship. However, supervisors, especially the banking supervisors, confirmed that the practice is followed, and that no account is opened without proper documentation.

102. In the second round report it was mentioned on the positive side that the initially limited scope of the AML Act was much broadened; however, legal and accountancy professions, as well as dealers in high value items, were not included. This has been changed, and now the aforementioned professions are obligated institutions under the AML Act. Now the coverage of DNFBP is very complete and in line with both international standards and the second EU Directive; It comprises casinos, notaries public, legal advisers, statutory auditors, tax advisers, auction houses, antique shops, precious metals and stones traders, commission sales business, pawnshops, real estate agents. Also foundations, which are not required by international norms, have been included. Furthermore, it was clarified that also the National Bank of Poland is encompassed by the AML Act when it operates bank accounts of legal persons, sales numismatics, purchases gold and exchanges damaged legal tender.

103. Another weakness of the Polish AML system identified by the last evaluators was the customer identification process for legal persons: the only requirement in place for legal persons was to identify account signatories but there was no requirement to identify directors or major shareholders. This situation remains unchanged as there is still more focus on proxies but no legal requirement to take reasonable measures to determine the natural person with ownership or control over a legal person.

104. In the view of the last evaluators the concept of reporting only on the basis of "transactions" rather than "activities" encompassed the risk that intermediaries could refrain in certain situations from sending a report, because a real transaction had not yet been asked for by the client. The evaluators recommended to review this situation either by changing the law so as to include suspicious activity or to communicate to the obligated parties that the term "transaction" should be understood to cover also suspicious activities and not only transactions. The Polish authorities followed the recommendation of the evaluators and GIFI presented during its training courses to obligated institutions the concept of "suspicious transaction" and "suspicious activity". However, the definition of "transaction" in the AML Act remained unchanged.

105. The efforts of GIFI in providing training to the obligated entities were already very much appreciated in the last report. In the meanwhile GIFI published the second edition of its free manual for obliged institutions and cooperating entities entitled "Counteracting money laundering" and also opened an e-learning course; the overall number of people trained is impressive.

2 LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalisation of money laundering (R.1 and 2)

2.1.1 Description and analysis

Recommendation 1

106. Poland has signed and ratified 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 organised crime (the Palermo Convention).

107. Money laundering is criminalised in four offences under Article 299 of the Penal Code, which provides as follows:

§ 1. A person who accepts, 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 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.

§ 2. An employee of a bank, financial institution or other entity legally obliged to record the transactions and persons carrying out the transactions who accepts, against legal regulations, 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. In case a person who, as an employee of a bank, financial institution or credit institution, assumed the obligation to inform the management board or other authority for financial supervision about the execution of a financial transaction, does not fulfil the obligation immediately in the form provided for in legal regulations, despite the fact that the circumstances accompanying the execution of the transaction excite a justified suspicion that they are related to the source of origin referred to in § 1, shall be subject to imprisonment up to 3 years.

§ 4. A person who, as an employee of a bank, financial institution or credit institution, is responsible for appointing the person authorised to receive the information referred to in § 3, does not comply with binding regulations, shall be subject to punishment referred to in § 3.

§ 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.

108. Also Articles 35 to 37a of the AML Act (Annex 1) contain penal provisions which criminalise certain breaches of AML duties. It was understood that they are used by the supervisors though all criminal cases go through the prosecutors.

109. The Article 299, para. 1, offence, reproduces some of the main physical elements set out in treaties, in that the language covers transfer of property and arguably concealment and disguise. The notion of conversion, knowing that such property is derived from (offences) is not clearly covered. Likewise possession, acquisition or use of property (with knowledge at time of receipt) is not specifically covered. While there is a wide formulation ("...undertakes other activities that foil or substantially obstruct the ascertainment of their criminal origin..."), the examiners considered it was difficult to read into this language the missing elements. The Polish authorities pointed to Articles 291 or 292 of the Penal Code which should cover these issues. These provisions are in a separate chapter of the Penal Code from Article 299. It seems to the evaluators that the offences in Articles 291 and 292 cover physical property or goods rather than proceeds, as widely defined in the international Conventions. In this context, the evaluators noted that in Article 299 a wide description of indirect proceeds is set out. In these circumstances the evaluators are not convinced that Articles 291 or 292 are entirely apt to cover possession, acquisition or use of all property, widely defined which are the proceeds of crime.

110. The examiners were advised that the offence extends to any type of property representing proceeds of crime. In the criminal offence there is no clear statement that "benefits" extend to any property that directly or indirectly represents the proceeds of crime (criterion 1.2). To meet this requirement therefore the Polish authorities rely on domestic judicial practice although there is no case law on this point from the Supreme court. The prosecutors indicated that they had not experienced difficulties in practice.

111. The examiners were advised that in practice a prior conviction for the predicate offence is not generally necessary for the imputation of money laundering. The Polish authorities indicated that they had experience of prosecuting money laundering in the same indictment as the predicate offence, though it was unclear if there is a legal provision covering this point. The examiners accepted that it appeared to be the case that a conviction was not necessary in respect of domestic predicate offences. It was less clear for foreign predicate offences, where the Polish authorities indicated that a conviction might / would be necessary.

112. Turning to criterion 1.3, the money laundering offence is based on an "all crimes" model (arg. ex "*...benefits related to the committed crime ...*").

113. The Polish authorities provided a full list of the offences in the Polish Penal Code which correspond to the designated categories of offences referred to in the Glossary to the FATF Recommendations (Annex II). It appears that nearly all the minimum categories of offences are covered; only financing of terrorism in all its forms, as defined in the IN to SR.VII, is missing (see Section 2.2 "Criminalisation of terrorist financing").

114. Criterion 1.5, requiring predicate offences to extend to conduct that occurred in another country (subject to dual criminality), is not explicitly covered in the money laundering offence. The examiners were advised that this is implicitly covered by the Articles 109 to 114 of the Penal Code which regulate the liability for offences committed abroad. In addition, given the ratification of the 1990 Council of Europe Convention by Poland, this should not be a problem (see Article 6 (2)a of the Council of Europe Convention).

115. Criterion 1.6 (self laundering) is sufficiently covered in the criminal legislation.

116. As regards Criterion 1.7 (ancillary offences), Articles 13 and 18 of the Penal Code set out definitions for attempt, aiding and abetting. Facilitating and counselling the commission of an offence are covered within these articles.

117. Turning to *conspiracy*, the wording in Paragraph 5 of Art 299 (read in conjunction with Article 18 para. 1) Penal Code does not refer to "conspiracy" in the sense of an agreement between two or more natural persons to commit a criminal offence (which is not completed) but to a special kind of complicity in committing the offence. Conspiracy to commit money laundering in the sense it is used in the Methodology is not a criminal offence.

118. Article 299, paragraphs 2 to 4, cover criminal offences specifically relating to employees of obliged entities. The statistics beneath show Article 299, para. 2 particularly is used. There is arguably some overlap between this offence and the criminal sanctioning regime under Article 35 AML Act (see Section 3.10 beneath). It is assumed that Article 299 (2) is only used in the most egregious of cases.

Additional elements

119. The examiners were advised that if a predicate offence has been committed abroad by a Polish citizen, there are no obstacles to impute the perpetration of money laundering offence, even if the predicate offence was not considered as an offence in the country of its commission.

Recommendation 2

120. While it is considered implicit, there is no express reference in Article 299 of the Polish Penal Code to the concept of knowledge, as it is used in the international instruments, i.e. knowledge that property is proceeds or the benefits of an offence or offences. The Polish authorities advised that the general provisions of Articles 8 and 9 contain a reference to the element of intention which would be used in relation to the money laundering offence.

121. The judges and prosecutors with whom the team met firstly indicated that all Article 299 Penal Code offences require a deliberate act and cannot be committed negligently.

122. The judges assured the assessors that they could draw inferences from the evidence (principle of free evaluation of evidence) in order to prove the intention, though confirmed that the law does not expressly permit the mental element to be inferred from objective factual circumstances. The evaluators were not able to confirm that this principle is established in practice and firmly supported by case law / jurisprudence.

123. Corporate criminal liability is covered by the Act of 28 October 2002 on the Liability of Collective Entities for Acts Prohibited under Penalty (Annex 2) which sets out the basic principles governing procedures to be followed in matters of such liability. 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 that 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 an entity does not incur liability provided by the Act. There is no experience with this new provision yet.

124. Due to Article 6 of the aforementioned 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 (criteria 2.4 and 2.5).

125. The penalties in relation to natural persons in respect of money laundering are set out above. With regard to money laundering in its unaggravated forms, the penalty (imprisonment from 6 months to 8 years) has been brought to European Union standards (maximum of not less than four years).

126. There is only a slight difference between the penalty for the unaggravated form of money laundering and the penalties for the aggravated offences in Article 299(5) and (6). Nevertheless, the sanctions for natural and legal persons appear generally dissuasive.

Statistics

127. The Polish authorities were invited to provide a breakdown of the cases that resulted in convictions from 2002 to the on-site visit in 2006 indicating, if possible, the predicate offence, the precise offence for which they were convicted, i.e. Article 299 (1,2,3,4,5 or 6); the sentence imposed; together with whether it was prosecuted autonomously or with the predicate offence, and whether confiscation was imposed. The Polish authorities have in response provided the following data:

	Initiated proceedings			**Stated offences**			**Requests for act of indictment**			**Binding convictions**		
	2003	**2004**	**2005**	**2003**	**2004**	**2005**	**2003**	**2004**	**2005**	**2003**	**2004**	**2005**
Art. 299 § 1 PC	110	121	135	11	54	44	11	53	44	6	10	10
Art. 299 § 2 PC	3	1	2	1	-	17	1	-	17	-	1	3
Art. 299 § 3-4 PC	-	1	1	-	1	-	-	1	-	-	6	1
Art. 299 § 5-6 C	10	16	13	13	44	100	13	44	100	1	7	31
Total	123	139	151	25	99	163	25	98	163	7	24	45

Money laundering convictions in the year 2005						
Art. 299	**Convicted persons**					
	Total	**Including imprisonment**				
		suspension of sentence on probation	**Up to 6 months**	**6 months to 1 year**	**1 year to 2 years**	**Total**
§ 1	10	9	2	1	7	10
§ 2	3	3	1	-	2	3
§ 3	1	1	-	-	1	1
§ 5 in con. with § 1	26*)	20	-	7	16**)	25
§ 5 in con. with § 2	2	2	-	-	2	2
§ 6 in con. with § 1	3	1	-	3	-	3

Explanatory Note:
*) one sentence 2,000 PLN (500 EUR).
**) 2 persons were convicted for a period of 3 years.

128. The examiners were advised that money laundering cases being prosecuted have been increasing. Statistical information on the types of predicate offences these money laundering cases involved was not available for the years 2003 to 2005 and for the time up to the onsite visit in May 2006. The vast majority of the above-mentioned statistics refer to cases conducted upon notification of the GIFI. The rest relate to notifications of other entities (revenue offices, banks, Police etc.). Fuel fraud was generally cited in this context as the major predicate offence. At the examiners' further request, the Polish authorities provided a breakdown of the predicate offences in 2006. The information provided went up to and beyond the onsite visit. Predicate offences in 2006 showed a broad balance between fiscal offences and non-fiscal offences. Non-fiscal predicate offences included corruption, trafficking in influence, participation in organised crime groups and offences against property. All money laundering cases were self laundering.

129. The examiners were told onsite only of one autonomous conviction under Article 299 (2) in 2004[8].

2.1.2 Recommendations and comments

130. The Polish authorities consider that although the language of the money laundering offence does not explicitly cover all the physical aspects (conversion, acquisition, possession, use) of Article 6 of the Palermo Convention and Article 3 of the Vienna Convention, they fall within the scope of Article 299 para 1 under "other activities that foil or substantially obstruct the ascertainment of their criminal origin" or would be prosecutable under Articles 291 or 292 of the Penal Code (Annex 7). The examiners non-the-less consider that the language of Article 299 should be reconsidered to ensure that conversion, acquisition, possession and use are fully covered in the legislation.

131. While the Polish authorities consider this is covered in practice, property capable of being proceeds could still be clarified. It would be helpful if the criminal law expressly covers both direct and indirect property which represent the proceeds (or benefits) of the crime.

132. 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 predicate offences to money laundering.

133. 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.

134. Though the Polish authorities consider this is possible, it may still be helpful to clarify by law or 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).

[8] During the pre-meeting, the Polish authorities provided the following information in relation to proceedings for money laundering cases for the year 2006 based on new information data collection by the Ministry of Justice:

1.) Self-laundering (predicate offence and introduction into financial circulation of property values derived from it is covered by the same proceedings) – 159 cases
2.) Prosecutions where the introduced charges concern exclusively money laundering, and the predicate offence is the subject of separate proceedings – 55 cases
3.) Proceedings in which there were other charges introduced than money laundering, although the proceedings concerned Art. 299 PC – 57 cases

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

136. The evaluators welcomed the extension of criminal liability to legal persons. They encourage the Polish authorities to take further steps to implement this provision in practice in money laundering cases.

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

138. It seems that the inability to define the original crime 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 the particular predicate offence. Most cases appear to be self laundering and the problem of the proof of the predicate offence is often addressed by prosecuting the money laundering and the predicate 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 crime is needed generally (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.).

139. More detailed statistics on money laundering investigations, prosecutions, convictions should be maintained (*inter alia* show the underlying predicate offence, and whether the money laundering offence was prosecuted autonomously or together with the predicate offence, the sentence, and whether confiscation was ordered)[9]. At the time of the onsite visit, it would appear that self laundering was the principal basis for money laundering convictions. In the absence of statistical information on the predicate offences for the 3 years 5 months up to the onsite visit, the examiners cannot comment on the range of money laundering predicates that were involved.

[9] Since the onsite visit, the Ministry of Justice has collected statistical information for the period of 1 January to 31 December 2006 covering the range of predicate offences which were subject to money laundering prosecutions.

2.1.3 Compliance with Recommendations 1 and 2, and 32

	Rating	Summary of factors underlying rating
R.1	**Largely compliant**	• Some of the legislative provisions need further clarification on the physical aspects of money laundering (conversion, acquisition, possession or use). • Not all essential criteria are 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.
R.2	**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.

2.2 Criminalisation of terrorist financing

2.2.1 Description and analysis

140. Poland has adopted and ratified the 1999 International Convention for Suppression of the Financing of Terrorism. It is binding on Poland since 13 December 2004. The Polish authorities pointed to the binding nature of this Convention together with other provisions of the Penal Code (Articles 65, 110, 115 and 258; Annex 7) as the criminalisation of all relevant acts associated with terrorist financing.

141. Article 115 of the Penal Code (under Chapter XIV - "Explanations of terms of the Law") has been supplemented with para. 20 which provides the definition of an "offence of a terrorist character": any offence being subject to a penalty of imprisonment for a minimum term of at least 5 years shall be regarded as an "offence of a terrorist character" provided that it is committed with the purpose of:

1. serious intimidation of a large number of persons,
2. compelling the public authorities of the Republic of Poland or of another State, or the agency of the international organisation, either to perform or abstain from performing any act,
3. causing serious disorder in the system of government and the economy of the Republic of Poland, or of another State, as well as threatening to do so.

Article 115 para. 20 relates to the prohibited acts, whose elements of crime are provided for in the existing provisions of the penal law. The terrorist character of the prohibited act is considered as aggravating; it increases the penal liability, which is reflected in Articles 65 and 258 of the Penal Code. Article 65 para. 1 of the Penal Code, which relates to the rules of sentencing with regard to perpetrators who make commission of offences their permanent source of income, or who commit offences acting in an organised group or association whose purpose is to commit offences, and to the perpetrators of offences of a terrorist character, and obligatorily imposes stricter sentencing on the perpetrators for the above-mentioned offences (under the same rules that apply to habitual offenders).

142. In turn, the content of Article 258 of the Penal Code, which penalizes participation in an organised group or association aimed at committing offences, was amended as follows: Paragraph 2 of this provision was supplemented with an element of the activities of organised groups or associations with the purpose of committing a terrorist offence ("*If the group or association (...) has the characteristics of an armed organisation or are aimed at committing an offence of a terrorist character*"). This offence is subject to a stricter penalty of imprisonment, namely from 6 months to 8 years. In para. 4 a new type of offence was introduced, namely a crime that involves an organised group or an association launched and controlled with the purpose of committing a terrorist offence ("*Whoever sets up the group or association aimed at committing an offence of a terrorist character, or leads such a group or of Poland organisation*"). In such case the court imposes a penalty of deprivation of liberty for a term of not less than 3 years.

143. The content of Article 110, para. 1 of the Penal Code was also changed. According to the new text of this provision, the national jurisdiction has been extended to include the application of the Polish penal law to foreign clients who commit terrorist offences outside the territory of Poland. Polish authorities consider this amendment to strengthen the fight against terrorism within international context.

144. The Polish authorities stated that despite the fact that there is no "stand–alone offence" related to the financing of terrorism ("autonomous offence of terrorist financing"), it does not mean, that financing of terrorism remains unpunished because such action would be treated as aiding and abetting (Article 18 para. 3 of the Penal Code) an "act of terrorism". Article 18, para.3, defines aiding and abetting as facilitating the commission of the prohibited act, and examples are given including "providing the instrument, or giving counsel or information".

145. SR.II requires countries to criminalise the financing of terrorism, terrorist acts and terrorist organisations; in addition, countries should ensure that such offences are designated as money laundering predicate offences. Criterion II.1 (a) notes that financing of terrorism should extend to any person who wilfully provides or collects funds by any means, directly or indirectly with the unlawful intention that they be used in or in the knowledge that they are to be used, in full or in part:

1. to carry out a terrorist act(s);
2. by a terrorist organisation; or
3. by an individual terrorist.

146. Footnote 40 to the Methodology and the FATF Interpretative Note to SR.II make it clear that criminalisation of financing of terrorism solely on the basis of aiding and abetting, attempt or conspiracy does not comply with SR.II. Thus it appears aiding and abetting a terrorist offence under Article 115, para. 20 and / or the establishment of the group or association aimed at committing an offence of a terrorist character, leading such a group or organisation (under Article 258, para. 2, 4) does not fully cover all the essential criteria in SR. II and the requirements of the FATF Interpretative Note to SR.II.

147. No financing of terrorism investigations have been undertaken or cases brought before the Court. Thus there is no case-law or practice on the exact scope of the current provisions. In the examiners' view, there is no certainty that Article 258 Penal Code would or could be interpreted to cover all relevant acts embraced by the concept of "financing of terrorism " as defined by the Convention for the Suppression of the Financing of Terrorism and the FATF's Interpretative Note:

- the collection of funds with the intention that they should be used in full or in part to carry out the acts referred to in Article 2 (a) or (b) of the Convention
- the collection of funds irrespective of whether the funds are actually used to carry out or attempt a terrorist act
- the provision or collection of funds for a terrorist organisation for any purpose, including legitimate activities run by a terrorist organisation.

148. The examiners also consider that it is not possible to read into Article 258 the provision or collection of funds with the unlawful intention that they should be used in full or in part by an individual terrorist. Thus Criterion II.1a (iii) appears to be not covered (see also paragraphs 2d and 8c of the FATF Interpretative Note to SR.II).

149. In the absence of jurisprudence, it is unclear whether Article 258 offence would cover the full definition of funds as defined by criterion II.1b. Equally, to the limited extent that Article 258 may apply, it is unclear whether the offence would cover the situations as described by criterion II.1c where there are no links to a particular terrorist act or whether the funds were actually used to carry out or attempt a terrorist act(s).

150. Criterion II.2, as noted above, is not fully satisfied, as the Article 258 Penal Code offence, together with the aiding and abetting principles in relation to any offence of belonging to a terrorist group (or committing an act of terrorism) would not provide for the complete range of predicate offences to money laundering embraced in the definition of a terrorist financing offence.

151. Given that it is not entirely clear that inferences can be drawn from objective factual circumstances, criterion II.4 appears also not to be fully satisfied (particularly in respect of criterion 2.2 in Recommendation 2). As mentioned under Section 2.1, there is not yet experience with the recently introduced provisions governing corporate criminal liability.

2.2.2 Recommendations and comments

152. Currently, there is no autonomous crime of "terrorist financing" in Poland. At present, such behaviour could only be addressed through the provisions of aiding and abetting (Article 18 para. 3 of the Penal Code) an "act of terrorism." The obliged entities under the AML Act clearly are convinced that there is no potential for terrorist financing in Poland. The examiners learned that Poland has recently initiated a legislative procedure aimed at introducing financing of terrorism as a separate, *sui generis* offence into the Penal Code. Bearing in mind the above mentioned analysis, Poland should provide as a matter of urgency an independent, autonomous offence of terrorist financing which explicitly addresses all the essential criteria in SR.II and requirements of the Interpretative Note to SR.II.

2.2.3 Compliance with Special Recommendation SR.II

	Rating	Summary of factors underlying rating
SR.II	**Non compliant**	The Polish authorities rely on the possibility of proceeding for aiding and abetting an offence of terrorist character as indicated in Article 115 para. 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 para. 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.

2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)

2.3.1 Description and analysis

153. The main provisions of the Polish confiscation regime (known as "forfeiture" domestically) and the provisional measures regime can be found in the Penal Code, the Code of Criminal Procedure, Article 412 of the Civil Code and Article 33 of the Penal Fiscal Code. The Penal Code provides for both general forfeiture measures and for special forfeiture in money laundering cases.

154. *Special* forfeiture in a money laundering context is addressed by Article 299 para. 7 of the Penal Code: In the event of a conviction for the offences specified in para.1 or 2 of this Article (i.e., the major substantive laundering offences) "*the court decrees*[10] *a forfeiture of implements*[11] *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"* Thus, it can be noted on the positive side that, according to this provision, both direct and indirect proceeds in money laundering cases can be confiscated. Similarly value confiscation applies in these cases. It also extends confiscation to proceeds transferred to third parties. Complete or partial forfeiture shall not be decreed under Article 299, para. 7, Penal Code if an object, benefit or equivalent thereof is subject to restitution to the offence victim or some other entity.

155. The *general* confiscation system is mainly based on Articles 44 and 45 of the Penal Code; Article 44 - in the most recent version provided by the Polish authorities - covers objects and instrumentalities derived directly from an offence and is broadly mandatory in nature where the law so states (as in the case of money laundering), though it incorporates discretionary elements:

> *§ 1. The court shall decree the forfeiture of implements derived directly from the crime.*
>
> *§ 2. The court can decree, and - in the cases indicated in the law – it shall decree the forfeiture of implements that served the crime or were used to commit the crime. [...]*
>
> *§ 5. A decision on the forfeiture of implements referred to in § 1 or 2 shall not be made if they can return to a wronged person or other authorised entity.*
>
> *§ 6. The court may decide on, and – in cases provided for in the law – it decrees the forfeiture of the specified implements if a convict has been sentenced for the crime consisting in violating the interdiction to manufacture, possess, sell, send, carry or transport the implements. [...]*
>
> *§ 8. The implements covered by the forfeiture shall become property of the Treasury the moment the judgement becomes valid.*

156. *Value* confiscation in respect of direct proceeds can be applied on a discretionary basis in the circumstances of Article 44 para. 4 Penal Code:

> *§ 4. In case the decision on forfeiture referred to in § 1 or 2 above is not possible, the court can decree the forfeiture of value equivalent to the value of the implements derived directly from the crime or the implements that served the crime or were used to commit the crime.*

157. A difficulty is found in Article 44, para. 7, which stipulates that the forfeiture under this Article can only be applied in respect of property or parts of the property that belong to the offender ("*In case the implements referred to in § 2 or 6 do not constitute the property of the perpetrator,*

[10] It is understood that this means "shall decree" and is therefore a mandatory obligation.

[11] It is understood that this includes objects.

their forfeiture can be decreed only in the cases stipulated in the law; in case of joint ownership, the forfeiture can be decreed in the part possessed by the perpetrator or in the value equivalent to his share"). Consequently, confiscation under Article 44 in relation to property transferred to third parties seems to be not possible unless specifically provided for in legislation. This may constitute an unintentional gap in the Polish legislation, given that forfeiture from third parties appears to be provided for in respect of indirect proceeds under Article 45 (see below).

158. Article 45 covers property related benefits. *Indirect* proceeds are capable of forfeiture in the circumstances covered by Article 45 Penal Code. This provision now encompasses (since 2003) reverse burdens where the property-related benefit is of considerable value, and this is a significant improvement since the second evaluation. Article 45 is couched in mandatory terms though it is possible for it to be discretionary where the benefit is needed in whole or in part to compensate victims. Importantly, it also addresses the issue of benefits transferred to third parties. It provides:

§ 1. In case the perpetrator, even indirectly, acquired a property-related benefit from the crime, and the benefit is not subject to forfeiture of implements set out in Art. 44 § 1 or 6, the court decrees the forfeiture of such benefit or its equivalent. The forfeiture shall not be decreed in part or in whole if the benefit or its equivalent should be returned to the wronged person or other 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.

§ 4. Provisions of § 2 and 3 shall apply, respectively, to the seizure conducted in accordance with the provisions of art. 292 § 2 of the Code of Penal Proceedings while securing the imminent forfeiture of benefits and during its execution. A person or entity the presumption established in § 3 refers to, can bring an action against the Treasury to reverse the presumption; the executive proceedings shall be suspended till the time a legally binding decision is made.

§ 5. In case of co-ownership, the forfeiture of the share belonging to the perpetrator or its equivalent shall be adjudicated.

§ 6. A property-related benefit covered by the forfeiture or its equivalent shall become the property of the Treasury the moment the judgement becomes valid, and in case referred to in § 4 second sentence, the moment the judgement dismissing the action against the Treasury becomes valid.

159. Under the general forfeiture statutes, Articles 44 and 45 Penal Code, it is provided that the forfeiture shall not be applied if its imposition would not be commensurate with the severity of the offence committed. The court may, instead of forfeiture, impose a supplementary payment to the State Treasury (Art 44 para. 3 Penal Code: "*In case the decision on forfeiture referred to in § 2 was incommensurably low in relation to the consequences of the crime committed, the court can decree interests to be paid in favour of the Treasury"*). If the imposition of forfeiture is impossible, the court may impose the forfeiture of the amount equivalent to the value of the objects directly derived from an offence or which served or were designed for committing the offence.

160. The reverse burden of proof provisions in Article 45 para. 2) and 3) are however welcomed though in the absence of statistics, it was unclear how frequently the regime was applied in practice – particularly in respect of indirect proceeds, value orders and orders in relation to third parties.

161. Under Article 412 of the Civil Code, courts can also forfeit objects or their value where it can be shown that a person committed an illegal act or an act of a "vicious nature." For cases of fiscal crimes, including some that are money laundering predicates (e.g. tax fraud, customs fraud), forfeiture can also be imposed under Article 33 of the Penal Fiscal Code (which follows Article 45 of the Penal Code in form and wording.

162. Regarding Criterion 3.1, within the confines of the present criminalisation of financing of terrorism (which is not in line with the Methodology) benefits and objects and instrumentalities appear capable of forfeiture under the general regime in Articles 44 and 45 where the property itself derives from other criminal offences, but not where the property is of legitimate origin (e.g. funds collected from persons who are unaware that their contributions are used to finance terrorism).

163. Turning to the requirements of Criterion 3.2 (provisional measures), a range of provisions in the Criminal Procedure Code were drawn to the examiners' attention: Article 217 para. 1 of the Criminal Procedure Code provides that objects "*which may serve as evidence in a case, 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."* Articles 291 to 295 of the Criminal Procedure Code (Annex 8) allow the authorities to obtain security against the property of the accused, in order to ensure that the proceeds of crime and related property are not dissipated prior to conviction and forfeiture. Such security 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.

164. Criterion 3.3 requires countries to provide laws or measures which allow the initial application to freeze or seize property subject to confiscation to be made *ex-parte* or without prior notice, unless this is inconsistent with fundamental principles of domestic law. The Polish authorities pointed to Article 291 of the Criminal Procedure Code which provides for *ex officio* applications (Para. 1: "*In the event of the commission of an offence subject to a fine or forfeiture of material objects, or supplementary payment to the injured or pecuniary consideration for a public purpose, or to imposition of the obligation to redress damage or compensate for the injury sustained, the execution of this decision may be secured ex officio on the property of the accused.*". Para. 2: "*If an offence is committed against property, or if it causes damage to property, the claims for the reparation of damages may be secured ex officio on the property of the accused.*"). A requirement of prior notice for the initial application to freeze or seize property subject to

confiscation is not included, so this criterion is satisfied, always assuming that these quick procedures apply to all property benefits including those not subject to compensation claims.

165. Criterion 3.4 requires Law enforcement agencies, the FIU, or other competent authorities to have adequate powers to identify and trace property that is or may become subject to confiscation or is suspected of being the proceeds of crime.

166. It can be noted that Poland has signed the Palermo Convention and that both Articles 44 and 45 Penal Code contain such protections. Generally the third parties have to prove the lawful acquisition of the property they claim to possess. Also the Code of Execution of Penalties of 1997 (Annex 9) contains supplementary provisions providing protection to the rights of spouses of the accused (Articles 28 and 29) and third parties (Article 29a).

167. The Polish authorities provided the following statistics (maintained from the Police) concerning the value of secured property in conducted cases concerning money laundering:
- 2002 – PLN 505,000
- 2003 – PLN 2,486,534
- 2004 – PLN 50,638,760
- 2005 – PLN 76,795,803.

168. During the on-site visit the Polish authorities were asked to provide a table concerning cases with the seizure of property. In response, the data beneath was provided.

Fiscal case Proceedings						
Seizure of	**Number of cases**		**Value (total)**		**Sanctions (range)**	
	2004	**2005**	**2004**	**2005**	**2004**	**2005**
Polish currency	16,731	18,739	2,237,460,200	2,663,939,000	5,334 penal cases initiated, 826 sentenced, 3,200 voluntary bearing of the responsibility	4,941 penal cases initiated, 685 sentenced, 3,065 voluntary bearing of the responsibility
Other means of payment (gold, etc.)	-	-	-	-	-	-
Goods seized	-	-	-	-	-	-

Foreign currency seized		
Stage of proceedings	**2004**	**2005**
Judicial proceedings is pending	1 case (USD, EUR)	12 cases (USD, EUR, SKK)
Customs Chamber has approved a decision on discontinuance of investigation	1 case (USD)	1 case (NOK)
A case in the court – a valid decision on granting permission for voluntary submission to responsibility is missing	1 case (USD)	
A case in the court – the judgement delivered orally, the written version of the judgement is missing		1 case (USD)
Self-contained fine – voluntary submission to responsibility, forfeiture		4 cases – voluntary submission to responsibility: 19500 PLN, forfeiture: 26050USD, 35820EUR, 1000HUF
A case brought to the court with an indictment, not put on the cause-list		7 cases (USD, EUR)
Discontinuance of the proceedings and return of currency		1 case (EUR)
A case in the court – an appeal against the judgement has been lodged		1 case (USD)
Self-contained fine – voluntary submission to responsibility, return of material evidence		1 case – voluntary submission to responsibility: 700 PLN
Fine and forfeiture		2 cases – fine 7000 PLN, forfeiture: 37150USD, 2585GBP
The Regional Public Prosecutor's Office discontinued the investigation due to insignificant social danger of deed		1 case (GBP)
The case has been passed to the Regional Public Prosecutor's Office with a draft of indictment and material evidence		1 case (GBP)

169. The examiners requested further figures on the numbers of forfeiture orders made. There are no figures available in respect of predicate offences in the absence of a money laundering charge. Some statistics were provided covering the whole of 2006, covering both before and after the onsite visit. These show that forfeiture orders were made in cases where money laundering was included on the indictment, amounting to 7,826,567 Euro. The offences include charges involving drugs, fraud, falsification of documents and organised crime cases. It was unclear how many of these cases related to the period up to and immediately beyond the onsite visit in May 2006. In these circumstances the examiners cannot establish the real effectiveness of the forfeiture system at the time of the onsite visit.

170. According to the AML Act, the Polish FIU, named "General Inspector of Financial Information" ("GIFI") in Poland, has the authority to trace and identify property as required by Criterion 3.4. Under certain circumstances, so do the court, the prosecutor, the police, and other law enforcement and related agencies such as the Internal Security Agency and the Central Anti-Corruption Bureau. The police and these other agencies act pursuant to Articles 213 and 214 of the Code of Criminal Procedure. The police and certain other agencies can also conduct covert

investigations on the finances of a suspect and his family for purposes of establishing assets and sources of income.

171. Criterion 3.6 requires countries that there should be authority to take steps to prevent or void actions, whether contractual or otherwise, 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. Article 44 para. 8 PC provides that "*the implements covered by the forfeiture shall become property of the Treasury the moment the judgement becomes valid*". In conjunction with the provisions of Article 45 para. 3 and 6 (see above), it can be said that the requirements of criterion 3.6 are satisfied.

Additional elements

172. Article 258 Penal Code covers the offence of participation in an organised crime group. Articles 44 and 45 in the "general part" of the Penal Code also would refer to Article 258, but there is nothing special beyond that.

173. For criminal forfeiture, final confiscation applies only after a criminal conviction. In addition, Article 412 of the Civil Code provides for the civil confiscation (i.e. the confiscation of property without a conviction of any person) of property (or its value) obtained from the intentional commission of an act that is illegal or otherwise of a particularly "foul" nature (an example was given of a person renting a room for a prostitute to work without any criminal prosecution). It was reported to the assessors that there was an interagency working group that was addressing the issue of civil and administrative freezing and amending Article 412.

174. Turning to additional criterion 3.7 c), it has been noted with approval that under the circumstances of Article 45, para. 2 and 3 Penal Code (see above) the defendant has to demonstrate the lawful origin of his property which is subject to confiscation. Also, Article 33 para. 2 and 3 of the Penal Fiscal Code, contain provisions in this regard (Annex 10). However, the Polish authorities could not provide examples of the new reverse onuses under Article 45 para. 2 and 3, being used since 2003 when the provisions were introduced, under introduced provision for reversing the burden of proof in certain cases. Consequently, the effectiveness of these provisions remains uncertain.

2.3.2 Recommendations and comments

175. The Polish confiscation regime appears now to be much more soundly based. In particular, the provisions in Art. 44 and 45 of the Penal Code are much improved since the second evaluation. Specifically since 2003, they now provide for reversing the burden of proof in certain cases and in ensuring that title can revert to the Polish authorities in the event of a transaction intended to defeat confiscation (issues specifically identified in the last report). The assessors remain concerned about implementation of the new procedures, especially as they relate to the identification and confiscation of indirect proceeds arising from an offence. The Polish authorities are encouraged to use the new powers proactively in major proceeds-generating cases.

176. Where instrumentalities subject to the regime under Article 44 have been transferred to third parties, it appears that confiscation is not possible. This should be addressed.

177. Furthermore, the evaluators doubt, that the Polish authorities are making sufficient use of the procedures relating to the identification and confiscation of indirect proceeds arising from an offence. It was unclear how frequently value orders were made and how often the issue of confiscation from third parties is attempted where proceeds have been transferred.

178. Criminal confiscation orders would be limited in respect of financing of terrorism offences (given that there is currently no complete incrimination of financing of terrorism). This should be rectified when there is an autonomous offence that fully reflects all the aspects of the offence set out in the international standards

179. More comprehensive statistical information should be kept on provisional measures and confiscation.

2.3.3 Compliance with Recommendation R.3

	Rating	Summary of factors underlying rating
R.3	**Partially compliant**	• 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.

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and analysis

180. In Poland basically directly applicable EC Regulations deal with some of the requirements set out in SR.III. The GIFI has a central role in disseminating information. It is part of their statutory remit to transmit information to obliged institutions where there exists a well-founded ground that that relates to the commission of terrorist acts (Article 4/3) AML Act). The Act of 16 November 2000 also supplements the directly applicable EC Regulations with some procedures relating to the financing of terrorism, notably Articles 16a and 18a AML Act which requires the reporting institutions to suspend transactions on block accounts in these circumstances. The Polish authorities also referred to Act of 29 August 1997.

Polish Procedures

181. It is convenient at this point to explain what actually happens in Poland with the various terrorist lists. So far as the examiners could ascertain, all lists are treated in the same way, i.e. GIFI is the central point for receipt and dissemination. The GIFI produces one consolidated list of suspected terrorists and terrorist organisations on the basis of all the data from the lists of entities suspected of terrorism published on the websites of the United Nations, the European Union and from national lists (in the case of Poland from the United States of America), as well as the data delivered to the Department of Financial Information by the foreign financial intelligence units and the Ministry of Foreign Affairs. This consolidated list is regularly updated. In 2004 and 2005, the distribution of this list was carried out among all the obliged institutions, which have to determine if any of the persons or entities on the list are or were in the past their clients or parties of financial transactions executed by them. Since January 2006, this consolidated list can be downloaded by the obligated entities from the restricted access area of the GIFI's website[12]. Where a positive identification is made, the obliged institution must immediately notify GIFI. To date, no such accounts have been identified.

182. Article 18a permits the GIFI to demand in writing an obliged institution to suspend a transaction or block an account, which may be linked to acts of terrorism, without a report from the obliged institution. So the initiative can be taken by GIFI if they, from their data bases, identify that a named person has an account in Poland. Similarly once information is communicated about names (even if not identified by GIFI as having accounts in Poland) then they can order the temporary blocking of accounts for 48 hours if the reporting institutions find a match. After this, GIFI would inform the relevant prosecutor, who, in turn, under Article 19 AML Act, may demand the suspension of the transaction or proceed with the blocking of the account for a period not exceeding 3 months ("prosecutorial freeze"). Thereafter general criminal procedure applies.

183. The general forfeiture provisions of the substantive penal law (Article 44 and 45 of the Penal Code) and Article 291 of the Criminal Procedure Code concerning security on property also provide legal instruments that may be used for freezing the proceeds of terrorism financing in certain circumstances. Prior to the expiration of the three month period of "prosecutorial freezing", the prosecutor must apply for the security on property under Article 291 or the freeze is lifted.

184. In addition to the obliged institutions, the Tax and Customs Authorities, the Police and the Public Prosecutor and other co-operating institutions are obliged to notify GIFI of information about

[12] The following statistics concerning the taking of the list from the website by obliged institutions was provided by the Polish authorities during the premeeting: 2006 – 519 downloads (168 up the date of on-site visit).

suspicions of terrorist financing obtained by them in the course of their operations. As noted above, GIFI is obliged to examine whether that obligated institutions comply with the requirements of the law to register and report transactions. In carrying out this responsibility, GIFI is entitled to, and indeed expected to conduct on-site examinations of the obliged institutions to verify their compliance with the law.

185. Banks are also directed to take measures to prevent the use of their institutions for purposes of money laundering or terrorist financing by Article 106 of the Act of 29 August 1997 ("Banking Law"), though the examiners could not see that this provision adds substantially to the scheme for implementation of SR.III.

S / RES / 1267

186. Poland is since 1 May 2004 a member country of the European Union and relies substantially on European Union mechanisms to comply with Criterion III.1. European Union Council Regulation (EC) Nr. 881 / 2002 regarding the implementation of United Nations Security Council Resolution 1267 (1999) and its successor resolutions, which provides for measures against Al-Qaeda and the Taliban, is effective on its national legal system without the need for domestic implementing legislation. This means that the European Union Regulation has direct force of law in Poland and requires the freezing of funds and economic resources belonging to persons designated by the United Nations Sanctions Committee and listed in the Regulation, and prohibits making funds or economic resources available to such listed persons. These lists are updated regularly by the European Union, and at this point assets are required to be frozen. Enforcement in Poland (by means of penalties for non-compliance) is provided for by general provisions in various sectoral laws sanctioning breaches of the law generally (e.g. Article 138 of the Banking Act; Article 167 of the Act on Trading in Financial Instruments; Article 228 of the Act on Investment Funds).

187. The European Union list of designated persons is the same as the United Nations list of persons and is drawn 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. Thus theoretically, sanctions could be applied from the point of European Union listing and dissemination of the information by GIFI.

S / RES / 1373 (2001)

188. S/RES/1373 is implemented in a similar way in Poland as S/RES/1267 (1999). With regard to S/RES/1373 (2001), the obligation to freeze the assets of terrorists and terrorist entities in the European Union through Council Common Positions 2001/930/CFSP (Common Foreign and Security Policy) and 2001/931/CFSP. The resulting European Union Regulation is Council Regulation 2580/2001. It requires the freezing of all funds and economic resources belonging to persons listed in the Regulations and the prohibiting or making available of funds and economic resources for the benefit of those persons or entities.

189. The authority for designating persons or entities lies with the Council of the European Union. Any member State as well as any third party State can propose names for the list. The Council, on a proposal from the Clearing House, establishes, amends and reviews the list. This list, as it applies to the freezing of funds or other assets, does not include persons, groups and entities having their roots, main activities and objectives within the European Union (European Union internals). European Union internals are still listed in an Annex to the Common Position 2001/931/CFSP, where they are marked with an asterisk, showing that they are not covered by the freezing measures but only by an increased police and judicial co-operation by the member States. There is no separate national legislation dealing with European Union internals. The authority for

making decisions on designations in Poland under S / RES / 1373 (2001) is said to be the GIFI (Article 4 para. 3 of the AML Act is considered to be the basis for this view). The GIFI advised that they have the possibility to designate under Res. 1373 and that they circulate the names which appear on all lists which they receive from whatever source (including European internals); there is no discretion exercised by GIFI not to circulate such a name. All obliged entities would be expected to report to the GIFI under Art 16a para 2 of the AML Act if they identify assets. The GIFI circulates this information only to banks and makes this information available on its secure website. It was unclear to the evaluators whether all obliged entities have access to this secure website. No matches have been reported to GIFI either in relation to non-European citizens or European internals.

Generally

190. The GIFI advised also that they can make discretionary decisions on actions initiated under the freezing mechanisms of other jurisdictions. The procedure under Article 18a of the AML Act, taken at the initiative of the GIFI, to begin freezing actions promptly in these circumstances goes some way to meeting criterion III.3. The problem with the Polish approach is that SR.III is a preventive measure and the procedures to maintain freezes depend ultimately on the ability to take criminal proceedings, which may not be possible in all relevant circumstances. Ensuring that freezes are not inappropriately lifted at a later date remains a problem. This issue is addressed further in the Recommendations and Comments beneath.

191. The assessors were not satisfied that there was a clear legal mechanism which covers designations in Poland with respect to EU citizens or other named persons proposed by other countries that were not included on the EU clearinghouse list. It was indicated by the Polish authorities during the pre-meeting that the names of European union internals were available to the obliged entities with a view to freezing (see above). The Polish authorities considered that such authority is implied in Articles 16a and 18 of the Act of 16 November 2000 and that these Articles, along with the Code of Criminal Procedure and Council of Europe conventions, enabled Poland to give effect to any foreign request for freezing, either directly in the case of EU partners or by converting foreign forfeiture orders under their national judicial authorities. However, a clear designating mechanism in such circumstances should be articulated for all such requests.

192. Regarding Criterion III.4, measures to freeze assets under the United Nations Resolutions must apply to (a) funds or other assets owned or controlled wholly or jointly, directly or indirectly by the persons concerned etc., and (b) to funds or other assets derived or generated from funds or other assets owned or controlled by such persons. So long as a person or entity appears on one of the lists of suspected terrorists or terrorist organisations distributed by the United Nations, the US or the European Union, then it appears that the freezing mechanisms available to GIFI and the Public Prosecutor would extend to assets under either (a) or (b). Assuming the conduct could be successfully prosecuted as aiding and abetting an act of terrorism, so could the seizing mechanism in the Penal Code. In neither case, however, do specific provisions exist. In addition, the two European Regulations make no mention of the elements underlined. Therefore the definitions of terrorist funds and other assets subject to freezing and confiscation contained in the regulations do not cover the full extent of the definitions given by the Security Council (or FATF) – in particular the notion of control of the funds does not feature in Regulation 881 / 2002, in particular, the European Union Regulations implementing S / RES / 1267 (1999) simply direct the freezing of all funds and economic resources belonging to, or owned or held by, a natural or legal person, group or entity designated on the list (Article 2 para 1). However, it is prohibited to make funds available directly or indirectly to or for the benefit of a natural or legal person, or group, or entity designated on the list (Article 2 para 2).

193. Criteria III.5 and III.6 require countries to have effective systems for communicating actions taken under the freezing mechanisms to the financial sector and/or the general public

immediately. Actually, Poland does not have at present the ability to immediately communicate freezing actions to its financial sector through the database maintained by GIFI's Department of Financial Information or any other mechanism. Nevertheless, under the EU Council framework decision on the execution in the European Union of orders freezing property or evidence (2003/577/JHA of 22 July 2003), Polish judicial authorities are obliged to transmit information on the action taken in the execution of foreign freezing orders without delay to the issuing authorities of EU States.

194. During training organised by GIFI, obligated institutions often reported the need for practical assistance in implementing the tasks imposed on them by AML laws and regulations. In order to meet these demands, a publication entitled "*Counteracting money laundering"* was prepared by the GIFI in 2004, addressed to entities obliged to implement tasks foreseen by the law. The GIFI distributed 10,000 copies of this guide among the obliged institutions and cooperating units. The guide presents typologies of suspicious transactions, describes the methods of transactions identification, discusses the duties of the obliged institutions and cooperating units, contains practical guidelines, and explains rules of submitting data to the GIFI. A second edition of the handbook was prepared and published in 2005. In addition, an Internet site of the General Inspector was launched containing replies to queries sent in by the obligated institutions, and GIFI publishes a number of its replies to questions on the website. The assessors found widespread familiarity with these guides.

195. Criterion III.7 requires countries to have in place effective and publicly known procedures for unfreezing (in the case of mistakes and namesakes). Poland claims that the procedures and premises for considering de-listing are effective and publicly known. However, the assessors found no evidence to support that claim. Reportedly, there is an interagency group that is currently addressing this need. For the moment, the assessors were told that such a request would have to come from the Court of Administrative Procedures to the Ministry of Foreign Affairs, which would decide whether to petition the United Nations. In fact, it seemed that the Polish authorities were unaware of the formal de-listing procedures which exist under the European Union mechanisms, both in relation to funds frozen under S / RES / 1267 (1999) and S / RES / 1373 (2001). For 1267 the European Union Council Regulation (EC) No. 881 / 2002 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). For 1373 the European Union Council Regulation 2580 / 2001 provides that the competent authorities of each member State may grant specific authorisations 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 competent authorities who, if satisfied, would take the case up with the Commission and / or the United Nations. As the evaluators were not informed about any freezing orders it can be presumed that no such cases occurred. The same procedure would apply to persons or entities inadvertently affected by freezing upon verification that the person is not a designated person (criterion III.8).

196. Turning to criterion III.9, it has to be said that no such procedures were identified. In addition, there are no specific provisions in EC No. 881 / 2002 for authorising access to funds frozen in accordance with S / RES 1267 (1999). As no funds under 1267 have been frozen as being related to Usama Bin Laden or members of Al-Qaeda or the Taliban or associated individuals or entities, there has been no need to consider how release could be effected in line with S / RES / 1452 (2002). It is none-the-less important that the Polish authorities advise the financial sector and DNFBP and other members of the public of the necessary procedures in this type of case.

197. Criterion III.10 requires countries to have appropriate procedures in place through which a person or entity whose funds or other assets have been frozen can challenge that measure with a view to having it reviewed by a court. This is covered by Article 293 of the Criminal Procedure Code (*"§ 1. The order securing claims shall be issued by the court or, in the course of*

preparatory proceedings, by the state prosecutor. Such an order shall determine the scope of the security and the manner of securing. § 2. The order on security shall be subject to interlocutory appeal. The interlocutory appeal against an order from the state prosecutor is examined by the district court in whose area the proceedings are pending."), but it is only applicable in criminal cases.

198. There is a specific procedure in EC No. 2580 / 2001 (implementing S /RES 1373) for release of basic expenses and related costs and application must be made to the competent authority of the member State in whose territory the funds have been frozen (Article 5).

Freezing, seizing and confiscating in other circumstances

199. SR III and the Methodology require countries to be able to freeze and/or seize, and confiscate terrorist-related funds and other assets in contexts other than those described in criteria III.1 to III.10 (i.e. other than in relation to designations pursuant to UNSCR 1267 and UNSCR 1373). No separate regulations covering these requirements were identified and only the general provisions for confiscation and provisional measures are applicable as described above, which means that the same comments as to the relevant provisions and their effectiveness made in relation to criteria 3.1 - 3.4 and criterion 3.6 also apply in this context. In the context of a prosecution for financing of terrorism (in its present form), funds of a legitimate origin given for terrorist purposes could be confiscatable on the basis of Art 44 para 2 Penal Code in that "implements" are understood to include objects. The Polish authorities also indicated that Art 412 of the Civil Code might be used for licit assets and made also reference to the taxation route under Article 30 para 1 point 7 of the Personal Income Tax Act of 26 July 1991.

200. Poland provides protections for the rights of *bona fide third parties* in the context of criminal proceedings, but as terrorist financing in all its forms is not covered, such protection as exist may not be sufficiently wide. It was unclear how the rights of *bona fide* third parties would be preserved in respect of the Article 18 (a) procedure before the criminal procedure is invoked. Any administrative procedure would need to take into account there interests.

Monitoring

201. According to criterion III.13, countries should have appropriate measures to monitor effectively the compliance with relevant legislation, rules or regulations governing the obligations under SR III and to impose civil, administrative or criminal sanctions for failure to comply with such legislation, rules or regulations. Some sanctions for breaches of CFT requirements are in the AML Act (see Article 35 [3] which covers failure to notify GIFI about transactions connected with acts of terrorism and presumably failure to block the account where requested by GIFI in respect of terrorism is also sanctionable. The duty to monitor the obligations on reporting entities in respect of financing of terrorism is clearly set out in the Law for GIFI and the other supervisors. However, the Insurance and Pension Funds Supervision Commission does not include this issue in their on-site visits; the PSEC relies during their onsite visits only on the answers provided by the private sector in a questionnaire (Annex 27; see Section 3.13). Monitoring on this issue should be comprehensively put in place.

Additional elements

202. Poland has implemented some of the issues covered in the Best Practices Paper for SR III. There are no procedures in place to authorise access to funds or other assets that were frozen pursuant to S/RES/1373(2001) and that have been determined to be necessary for basic expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses.

2.4.2 Recommendations and comments

203. As mentioned above, the obliged entities under the AML Act are convinced that there is no potential for terrorist financing in Poland. Knowledge of the existence of a list of terrorist names and organisations is widespread, and the availability on the GIFI website seems to be known to most. However, except for the most sophisticated entities, which would mainly be obliged to use these lists based on instruction from their group or shareholders abroad, use of the list is made rather sporadically and only *ex post facto*, and not during the conduct of a transaction[13].

204. Implementation of SR.III is formally in place, but Poland has no clear legal provisions for implementing action against European Union internals, though, as indicated, the names of European union internals were available to the obliged entities with a view to freezing (see above). There was also no real understanding of how the relevant bodies and persons were implementing the Special Recommendation. The two European Union Regulations (881 / 2002 and 2580 / 2001) have definitions of terrorist funds and other assets subject to freezing and confiscation which do not fully cover the extent of those given by the United Nations Security Council and the FATF, especially regarding the notion of control of funds in 881 / 2002.

205. Specifically the authorities need to give the financial and non-financial institutions, DNFBP and the general public guidance as to the obligations under these provisions. The mechanisms for unfreezing and for dealing with basic living expenses, which exist within the European Union framework, need explanation.

206. At present, there have been no matches found in Poland by GIFI with persons named on lists. If this were to occur, Poland essentially would rely on the AML Act blocking mechanism at the initiative of the GIFI (without any report having been received from the obliged entities) under Article 18a AML Act. Article 18a should provide an efficient mechanism at the beginning of the process for freezing terrorist funds. This would then be followed up by prosecutorial freezing. The problem with this is that SR.III is preventive in nature and the prosecutorial freeze is dependent ultimately on investigations leading to criminal proceedings. A freeze may be achieved by this route for a while, but if no criminal case ultimately can be made out (which may frequently be the case), then the freeze would have to be lifted. In such circumstances, it is difficult to see how any degree of permanence could attach to freezing under the criminal route. In the circumstances, as the Intergovernmental Group are reviewing their procedures (especially in respect of European Union internals), they may wish to review this aspect as well, and consider the merits of a more general administrative procedure based on Article 18a for handling SR.III freezing in its entirety, subject to proper safeguards (especially with regard to *bona fide* third parties). This would ensure that where matches are identified, freezing orders issued under the criminal procedure are not inappropriately lifted at a later date simply because there is insufficient evidence for criminal proceedings, or because for other reasons the criminal procedure cannot be pursued.

[13] See Footnote above.

2.4.3 Compliance with Special Recommendation III and Recommendation 32

	Rating	Summary of factors underlying rating
SR.III	**Partially compliant**	• The definition of funds (deriving from the European Commission Regulations) does 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 is 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 is 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 Act dealing with terrorist financing issues is unclear.

2.5 The Financial Intelligence Unit and its functions (R.26, 30 and 32)

2.5.1 Description and analysis

Recommendation 26

207. Criterion 26.1 requires countries to establish a financial intelligence unit (FIU) that serves as a national centre for receiving (and if permitted, requesting), analysing, and disseminating disclosures of STR and other relevant information concerning suspected money laundering or terrorist financing activities. In Poland, that authority is the General Inspector of Financial Information (GIFI). It was established by the Act of 16 November 2000 on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources and on Counteracting the Financing of Terrorism (the AML Act). The legal basis for the FIU is to be found in Article 3 of the AML Act. From that, it is noted that the General Inspection of Financial Information (referred to as the General Inspector) is the central government authority for counteracting the introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources and for counteracting the financing of terrorism. The General Inspector is appointed by the Prime Minister and can be dismissed by the Prime Minister on petition by the Minister responsible for financial institutions. The General Inspector is an Under-Secretary of State in the Ministry of Finance. He performs his duties with the assistance of an organisational unit created for that purpose in the Ministry of Finance (Department of Financial Information – together with GIFI - the FIU), of which the Director is the day to day operational Head subordinate to the General inspector himself. The FIU is thus an administrative FIU.

208. With regard to Criterion 26.1, the tasks of the GIFI are set out in Article 4 of the AML Act:

a) Obtaining, gathering, processing and analysing of information pursuant to the AML Act as well as transactions suspected to derive from illegal or undisclosed sources and of counteracting the financing of terrorism, in particular analyses of transactions in relation to which GIFI has come to reasonable suspicion;
b) performance of transaction suspension or of account blocking procedures;
c) transmitting to obligated institutions the information on entities towards which there exist a well-founded ground, that they are connected with commitment of terrorist acts;
d) preparation of documents justifying the execution of criminal act suspicion and forwarding them to competent authorities;
e) initiating and taking other actions serving to prevent the use of the Polish financial system to legalize revenues derived from illegal or undisclosed sources, including the training of personnel of obligated institutions within the scope of the responsibilities of these institutions;
f) inspection of the observance of the AML Act;
g) co-operation with foreign institutions, working with AML/CFT.

209. AML/CFT system is rooted in Article 8 para.s 1) and 3) which provide for the duty to "register" transactions and persons executing transactions, which includes duties of identification etc. Transactions to be registered are transactions above the amount of 15,000 EUR, connected transactions of the same amount and "*as well as of such transactions, when the circumstances suggest that the property values involved used may derive from illegal or undisclosed sources*" are specified in the AML Act (Article 8) and in the "Regulation of 21 September 2001 on establishing the form of a register of transaction, the way of keeping the register and the procedure of conveying the registry data to the General Inspector of Financial Information" (Annex 11). Information on transactions registered under Article 8 para.s 1) and 3) have to be reported to GIFI. Criterion 26.1 is clearly satisfied in respect of AML issues. In respect of CFT

issues, the Act of 16 November 2000 now includes counteracting the financing of terrorism in its title and Article 1 of the AML Act includes counteracting the financing of terrorism in its overall remit. In one English translation of the AML Act which the examiners saw, there is a footnote to the title which explained that whenever separate provisions refer to counteracting AML it shall also mean counteracting financing of terrorism. Article 16a (2) of the AML Act appears to provide a mandatory reporting obligation in respect of transactions suspected to be linked to terrorism. Article 16a(1) appears to be the legal basis on which GIFI transmits information about the lists of suspected terrorists. Therefore Criterion 26.1 is completely fulfilled.

Provision of guidance on reporting

210. The tasks of GIFI include training of obligated institutions as regards the tasks imposed by the AML Act (Article 4 para. 5). According to the GIFI, apart from trainings carried out in the form of e-learning, the GIFI has also published a free manual for obliged institutions and cooperating entities entitled "Counteracting money laundering". The manual is well known among most of the obliged institutions (the representatives of the casinos were not aware of this guidance) but not well understood as to be a guidance regarding the manner of reporting. The means of reporting the information are specified in the Act and in the Ordinance of 21 September 2001, which determines the template and the manner in which the Register should be maintained in precise detail. The issue of guidance and the significant training which has been undertaken by GIFI is comprehensively explained under section 3.12 (AML/CFT Guidelines). Criterion 26.2 is satisfied.

211. Regarding Criterion 26.3, GIFI has *direct* access to the following data bases:

- the KCIK - National Crime Register (administered by the Police),
- PESEL – National Register of Personal Identification Numbers (administered by Ministry of Interior) and the
- KEP - National Tax Payers Register (administered by the Ministry of Finance).

Furthermore, GIFI has *indirect* access to data both of Customs, Tax Offices Databases[14] (administered by the Ministry of Finance), the Prosecutor's Office and as well to the Polices operational data on request. According to Article 14, paragraph 2, of the Act the Public Prosecutor's office, the Home Security Agency and Units subordinated to or supervised by the Minister responsible for Internal Affairs shall also inform the General Inspector forthwith of any proceedings initiated in connection with the offence referred to in Article 299 penal Code. This information shall indicate in particular the circumstances of the offence and the participants.

212. In addition, GIFI keeps the following databases:

- data base containing transactions/persons/accounts/ from suspicious activities reports (SAR),
- data base containing transactions exceeding appropriate threshold as defined by Article 8 of the AML Act,
- data base of subjects involved in terrorist activity,

213. The FIU has also the wide possibility to request all the information of the obliged institutions and co–operating units under Article 13a and 15 of the AML Act.

214. Upon a written request of GIFI, a reporting party has to give access to the data of transactions which fall under the provisions of the AML Act. A right to access encompasses, in particular, the data on parties that executed the transactions, content of suitable documents, including the ones showing balances of an account and its turnover, their certified copies or relevant documents

[14] After the onsite visit, GIFI got online access to this database.

under Article 11(1) AML Act. This is also the case with the Customs and the Border Police. For instance, the Polish Securities and Exchange Commission (PSEC) cooperates with the GIFI by:

- immediately informing the General Inspector that it suspects the introduction of property values originating from illegal or undisclosed sources to financial transactions;
- delivering certified copies of documents concerning the transactions, in relation to which there is a suspicion that they are linked to a crime and submitting the data to persons carrying out these transactions.

At the same time, the PSEC is obliged to submit to the General Inspector a written information on the results of the inspections conducted in the entities supervised by the Commission, in the scope they refer to compliance with provisions of the AML Act.

Disseminating financial information

215. Chapter 5 of the AML Act (Art 16 to 20c) contains provisions determining the procedure for suspension of transactions and blocking of accounts: In the case that a transaction may be linked to money laundering, The same blocking of accounts procedure applies to financing of terrorism (see Article 18a of AML Act). The GIFI is authorised to demand (in writing) the obligated institutions to suspend the transaction or to block the account. This demand has to be done in written form within 24 hours following the confirmation of the notification receipt. The suspension of the transaction or blocking the account may not exceed 48 hours following the confirmation of the notification receipt. The obligated institution shall suspend the transaction or block the account after receiving the written demand with no delay. At the same time the General Inspector has to notify the public prosecutor about the suspected offence and shall forward to him the information and the documents relating to the suspended transaction or the blocked account. Suspending a transaction or blocking an account may be demanded only by the General Inspector or by two employees of the FIU, duly authorised by him in writing and acting together.

216. Pursuant to Article 4 para. 4 of the AML Act, the General Inspector is responsible for elaboration of documents and blocking of accounts justifying the suspicion of money laundering or terrorist financing and delivering them to the public prosecutors (under Article 31). According to Article 32 para. 1 of the AML Act, information on transactions covered by the provisions of the AML Act shall be also submitted by the GIFI to the courts and prosecutors upon their written request for the needs of criminal proceedings.

217. Article 33 of the AML Act allows for the dissemination of information by GIFI to other bodies upon grounded requests, and upon his own initiative. In justified cases, the General Inspector may apply to the tax authority or to the fiscal control authority for examination of the legality of specific property values origin under Article 15 b of the AML Act.

218. Information on results of the actions carried out under these Article 15b initiatives by GIFI shall be delivered to the General Inspector forthwith. There is a risk that the GIFI's initiatives in this regard may be used for tax control, even if the purpose of these requests is to investigate persons for GIFI's own analyses. The GIFI may work to consider this issue further. The GIFI obtained in 69,57% of their requests answers from the tax authorities and tax control authorities. The information provided were in 11 cases the basis to classify a case to "passive analyse": this means that there was a lack of suspicion for money laundering, which resulted in suspending the case and to keep it in the database.

219. During the period from 2003 to 2005, the GIFI sought information under Article 15b of the AML Act and provided (on his own initiative) information about suspicious activities under Article 33 of the AML Act to the below mentioned public institutions:

public institutions	amount of cases given on the basis of Article 33 para. 3 of the AML Act	amount of applications on the basis of Article 15b of the AML Act
Internal Security Agency	2	-
tax control authorities	3	17
tax authorities	1	6
Total	**6**	**23**

Operational independence

220. The Polish authorities are of the opinion, that the position of the General Inspector as an Under-Secretary of State guarantees full operational independence and autonomy for the Polish FIU. On one view Article 32 (2) of the AML Act may appear to have the effect of limiting the independence of the unit as to when it submits reports to the prosecutor.

Criterion 26.7

221. Regarding Criterion 26.7, the GIFI LAN ("local area network") is separate from the Ministry of Finance network. Only a limited number of the GIFI staff has direct access to the data. The protection of and the access to the data gathered by GIFI is regulated by Chapter 7 of the AML Act. Pursuant to Article 32(1), information on transactions covered by the provisions may be disclosed only to courts and Public Prosecutor's Offices for the purpose of criminal proceedings and to those entities, which are exhaustively listed in Article 33 of the AML Act. Disclosure of information to persons and entities, which are not duly authorised, is prohibited – violations of this provision are sanctioned by Article 35 of the AML Act (scil. penalty of deprivation of liberty for a period of up to three years; in the case of an unintentionally offence, the perpetrator shall be liable to a fine). Furthermore, the GIFI issued internal decisions and instructions providing special protection also in terms of technical and organisational measures concerning the information which is gathered in the unit. These regulations contain rules and standards for staying within the premises of the unit, security measures for facilities and equipment after work, procedures for dealing with documentation and information processed on duty. The question of security is always presented in the annual employee trainings.

222. It has been explained to the evaluators that the GIFI submits to the KCIK (National Crime Register) data about the identity of the persons notified by GIFI to the prosecutor under Article 13 of the Criminal Information Act which includes:
    - name,
    - address,
    - day and place of birth,
    - aliases, nickname,
    - tax-identification number;
    - personal identification number (in the case of natural persons);
    - statistical number (for legal persons).

223. To this database, the Prosecutors, Police, Border Guards, Central Anti-Corruption Bureau, Customs, Tax Control, Tax intelligence, Secret Service, Military Police, GIFI, Public Administration in charge of Citizenships, foreigner and repatriation, Military Counter Intelligence, Military Intelligence, Polish Financial Supervisory authority, Direction of State forests and directors of national parks have online access (Article 19 of the Criminal Information Act).

Criterion 26.8

224. The General Inspector is obliged under Article 4a AML Act to present the Prime Minister with an annual report on his activities within 3 months of the end of the reporting year. The report shall contain information on activities taken, statistical data and commentary referring to phenomena and trends observed. This report is publicly available and includes statistics, typologies, trends or information regarding its activities.

Criterion 26.9 and 10

225. The Polish FIU is a member of the Egmont Group since June 2002. The number of memoranda of understanding currently totals 33 and it cooperates with more than 40 countries. To share information with non-EU countries, a Memorandum of Understanding is necessary. The GIFI cooperates with FIUs from others countries of any type by using the rules and terms prepared by the Egmont Group (also using the Egmont Secure Web System, which is used for sending and answering of requests). The accession of Poland to the European Union on 1 May 2004 gave GIFI the possibility of effective co-operation with its partners in the Member States, on the base of the Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA) related to counteracting of financing of terrorism, and also by the IT system of data transmitting between FIU of the member States – FIU.Net. Additionally, GIFI is connected to the Egmont Group's secure information exchange system.

Reports received by the FIU

226. The authorities have provided a breakdown of their work in 2005. In that years, the GIFI received and processed 20,921,317 reports concerning transactions above 15,000 Euro as well as 65,559 suspicious transactions reports concerning money laundering and 2050 suspicious transaction reports related to terrorist financing.

Statistical Information by Monitoring Entities reporting to the FIU[15]				
Monitoring entities/ obliged institutions	**transaction reports sent to GIFI (electronically and on paper) in 2005**			**STRs/SARs involved in notifications to prosecutors (by GIFI)**
	transactions above threshold (Art 8 / 1)	**Suspicious (STR + SAR) Art 8/3[16]**		
		ML	**FT**	
banks, foreign bank branches	18,104,720	61,473	2,050	3,046
investment fund, investment funds society	1,713,964	2,116	0	0
entrepreneurs conducting leasing and factoring activity	383,728	1,451	0	0
Notaries	321,079	1,237	32	0
Co-operative savings and credit banks	271,881	206	1	1

[15] FIU analyzes all reports. One notification to the prosecutor can involve more than one STR.

[16] 79,6% of them were mistakenly sent by the obliged institutions in that the wrong classification was used in the special field of electronic form; 13.656 reports (20,4%) were real STRs / SARs.

insurance companies, the main branches of foreign insurance companies	47,829	43	0	1
brokerage houses or other entities not being a bank engaged in brokerage activities	43,102	36	0	0
entrepreneurs conducting activity in the scope of commission sale	25,290	1	0	0
Joint Stock Company National Depositary for Securities	5,021	0	0	0
entities conducting activity involving games of chance, mutual betting and automatic machine games	3,738	0	0	0
state public utility enterprise Poczta Polska (Polish Post)	666	0	0	0
Residents engaged in currency exchange	142	1	0	2
auction houses	70	0	0	0
antique shops	31	0	0	2
entrepreneurs conducting activity in the scope of precious and semi-precious metals and stones trade,	23	0	0	0
entrepreneurs giving loans on pawn (pawnshops)	21	0	0	0
real estate agents	10	0	0	0
foundations	2	0	0	0
legal advisers	0	0	0	0
Cooperative units	NA	523	0	75
TOTAL	**20,921,317**	**67,087**	**2,083**	**3127**

227. The table beneath shows the number of cases initiated by GIFI in 2001-2005, the number of cases passed to the prosecutors, number of indictments and convictions for money laundering.

	2001[17]	***2002***	***2003***	***2004***	***2005***
Cases initiated by GIFI.	291	611	703	643	973
Cases passed to the public prosecutors	20	104	152	148	175
Number of indictments	10	6	25	54	161
The numbers of persons convicted for money laundering	5	10	3	17	40

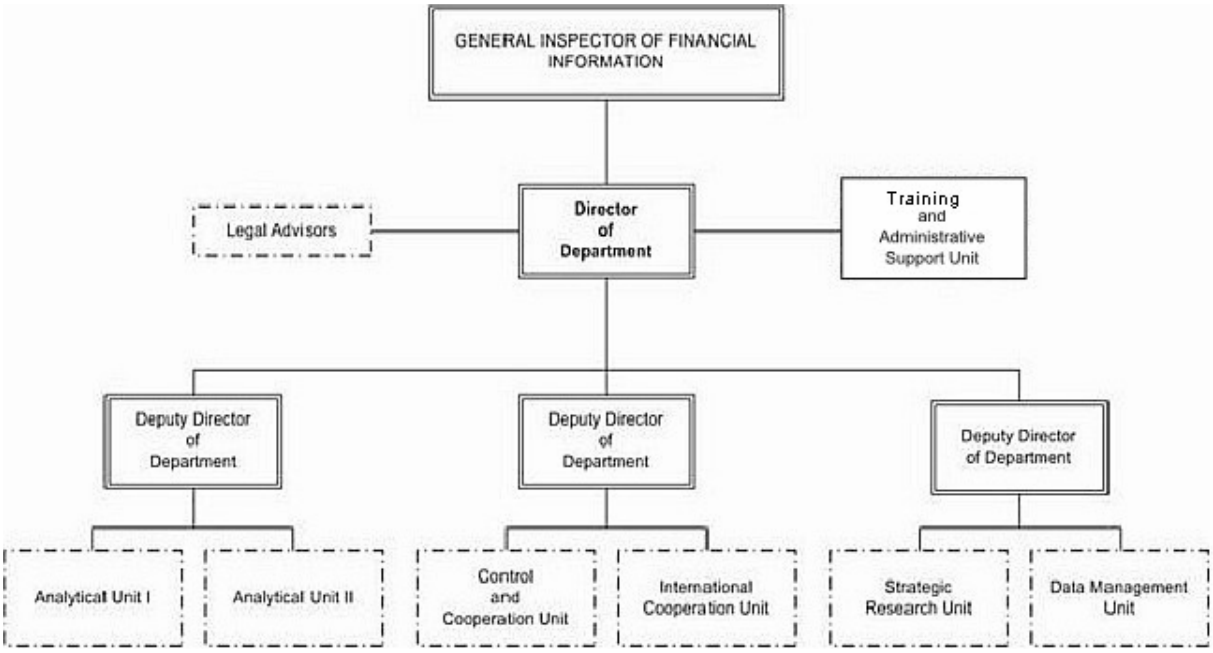
228. The average time of analysing a case in 2005 was 286,5 days (from the initiation of a case to the moment of sending a notification to the public prosecutor). An analysis of a case could last from 24 hours to even two years.

[17] Since 1 July 2001.

Recommendation 30

Structure finding, staff, technical and other resources for the FIU

229. The structure of GIFI is as follows:



230. The unit employs currently 49 persons. All employees have higher education and technical employees have legal, economic or information technology education. Continuing vocational training has become common practice. It is financed from the funds allocated for the activity of the Ministry. The unit is equipped with proper technical and information technology facilities. In justified cases, the employees have access to the GIFI data collection system and other available databases and information exchange networks. Separate teams implementing analyses, as well as employees carrying out the strategic analysis of the data, have access to modern, highly specialised tools allowing the creation and application of module solution for the purposes of respective analysis stages.

231. The staff are expected to maintain high professional standards and are of high integrity. Employees undergo regular trainings on the correct processing of classified information. The GIFI staff receive regular internal training on AML/CFT issues and participate in many international seminars, external workshops, twinning projects and bilateral meetings which extend their knowledge on AML / CFT issues.

2.5.2 Recommendations and comments

232. GIFI is at the centre of the system. The FIU has a well resourced IT centre, and provides high quality training, which is well received by obliged entities. It has prepared a guidebook for obliged entities. This is widely distributed, is well written and contains many typologies. The private sector confirmed that it is very useful. It is not however a binding document. The FIU has also put very good efforts into training (including e-learning courses). The overall number of people trained is impressive.

233. Despite this, some elements are missing including a common understanding by all stakeholders of the obligations under the Act. Equally, there remain a large number of above threshold reports, and a greater emphasis on the recognition, analysis and reporting of suspicious activity by obliged entities would assist. Greater coordination of the main players in the AML system would also help to ensure a more consistent approach. This is taken up further under Recommendation 30.

234. The banks remain by far the largest reporting obliged entities. Still further outreach is strongly advised to some parts of the financial sector (particularly exchange houses) and the designated non-financial businesses and professions - DNFBP (particularly casinos) to explain the concept of suspicion in more detail. There is thus overall a reserve on the effectiveness of the training and outreach across the whole of obliged institutions. Additionally, they should consider publishing more periodic reports with statistics, typologies and trends, as well as information about its activities.

235. The number of cases passed to the Prosecutors by GIFI has risen significantly since the second evaluation and the examiners welcome this trend. It was unclear how the FIU monitors its own performance. For example, no comprehensive statistics were provided showing average processing times in the FIU (apart from the data given for the year 2005).

2.5.3 Compliance with Recommendation 26, 30 and 32

	Rating	Summary of factors underlying rating
R.26	**Compliant**	

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, 28, 30, and 32)

2.6.1 Description and analysis

Recommendation 27

236. Criterion 27.1 requires that "There should be designated law enforcement[18] authorities that have responsibility for ensuring that money laundering and financing of terrorism offences are properly investigated".

237. The Polish authorities explained that, in total, 409 Police officers are involved in the fight against money laundering and provided the following breakdown:
- national police headquarters (2)
- Criminal bureau (2)
- Central Bureau of investigation (30)
- voivodship[19] headquartes of police (32)
- Warsaw metropolitan police headquarters (2)
- regional police headquarters (7)
- district police headquarters (270)
- municipal police headquarters (66).

238. The money laundering and financing of terrorism cases are investigated by the Central Investigation Bureau of the General Headquarters of Police. Within the Police there is no specialised Division for combating money laundering as such.

239. In Poland, the Prosecution exercises the general powers of an investigating authority.

240. The Bureau for Organised Crime of the National Public Prosecutor's Office monitors and supervises proceedings relating to money laundering. Each proceeding is covered by monitoring. In this event, upon request of the Bureau, the units of the Public Prosecutor's Office provide detailed information on the course of conducted cases. With reference to cases conducted by Departments II for Organised Crime of the Appellate Public Prosecutor's Offices units, the Bureau carries out official supervision. With reference to these supervisory cases, the Bureau for Organised Crime of the National Public Prosecutor's Office performs duties under Art. 8 of the Law on Public Prosecution Authorities and, pursuant to the provisions of the Penal Procedure Code, can in appropriate cases extend the period for investigations initiated by Appellate Public Prosecutor's Offices and instructs the prosecutors about directions of investigation if necessary.

241. Every 6 months the public prosecutor's office units send detailed reports on money laundering to the Bureau for Organised Crime of the National Prosecutor's Office for supervisory and monitoring purposes.

242. By an Order of the National Public Prosecutor of 24 February 2006 (8/2006/PK-PZ) a group of prosecutors has been established for the coordination of all pre-trial proceedings concerning abuse in trade in fuel, scrap metal and money laundering ("fuel Mafia").

[18] In certain countries, this responsibility also rests with prosecution authorities.
[19] *Voivodship* is a Polish geographical unit of administration.

243. Criterion 27.2 requires "countries should consider taking measures, whether legislative or otherwise, that allow competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering ". While the Polish authorities drew the evaluators' attention to Article 253 of the Criminal Procedure Code, it is unclear whether there are complete measures in place to postpone or waive the arrest of suspected persons. As noted earlier, the second part of 27.2 is fulfilled as according to Article 27, para. 1, of the Criminal Procedure Code, objects which may serve as evidence in a case, 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. While there are no legal measures allowing competent authorities formally to postpone or waive the arrest of suspected persons for the purpose of identifying other perpetrators or for gathering the evidence, the examiners were advised that in practice this can happen without legal impediment (e.g. controlled delivery).

Additional elements

244. Criterion 27.3 covers the need for an adequate legal base for special investigative techniques. The legal basis for special investigative techniques within money laundering and terrorist financing investigations can be found primarily in the Code of Criminal Procedure (Art. 237 to 241, covering tapping and recording of telephone conversations and intercepting similar transmissions; Article 218); the Police Act of 6 April 1990, including observation and video recording, covert operational and electronic tapping of phones and intercepting similar transmissions; operational covert control of correspondence and other postal material on consignment, controlled covert purchase, sale or interception of objects derived from criminal activity (controlled delivery and pseudo purchase); controlled covert supervision of manufacturing, movement, storage of goods derived from crime; agent provocateur; telecommunication data retention; and undercover operations. Poland is a full party to the European Union Mutual Legal Assistance Convention 2000, which contains special investigative techniques, and the Schengen Convention 1990 which covers cross border observation and hot pursuit. According to the Criminal Procedure Code, the offices, institutions and entities operating in the fields of post and telecommunication activities, Customs offices, and transportation institutions and companies, shall be obliged to surrender to the Court or State Prosecutor, upon demand included in their order, any correspondence or mail as well as listings of connection through telecommunication system or any other transfer of information, including electronic mails with dates and time and other information relevant to the connection which is not the contents of the telephone conversation or any other transfer of information, when the above are significant to the pending proceedings. Only the court and a state prosecutor are entitled to inspect them or to order their inspection.

245. In proceedings concerning money laundering the most common operational technique is telephone tapping.

246. In cases concerning money laundering suspicion relating to property of significant value, the Police may apply operational inspection, secretly supervised consignment or special operations.

247. In money laundering proceedings, the institution of "crown witness" may be applied, if the money laundering is connected with organised crime activities, under which a criminal who has been prosecuted gives evidence in subsequent proceedings against other crime group members.

248. Most of the preparatory proceedings are conducted by Departments for Organised Crime of Appellate and District Public Prosecutor's Offices.

249. No proceedings have been undertaken by using domestic mechanisms such as temporary groups or co-operative investigations involving specially trained financial investigators. No directions have been given to the prosecutors, so far as the examiners are aware, to conduct financial investigations in parallel with general enquiries into organised and economic crime cases. However in some cases the Police work in conjunction with the Revenue Services. With respect to joint international teams, Poland as an EU member and a full party to the Palermo Convention, is aware of the emphasis now placed on Joint Investigation Teams, though as yet there is no practice.

250. The Polish authorities did not provide any information on the use of specialised financial investigators using modern financial investigation techniques proactively.

251. As noted, the GIFI has prepared a handbook for obliged and cooperating units, comprising disclosed methods of money laundering. The manual has also been delivered to Public Prosecutor's Office units. Twice a year (during joint seminars in special Police Training Centres – Pila and Szczytno) the prosecution, Police and FIU review money laundering trends and techniques (and strategy) collectively.

Recommendation 28

252. Criterion 28.1 requires that the competent authorities responsible for conducting investigations of money laundering, terrorist financing and other underlying predicate offences should have the powers to be able to (a) compel production of, (b) search persons or premises for, and (c) seize and obtain transaction records, identification data obtained through the CDD process, account files and business correspondence, and other records, documents or information, held or maintained by financial institutions and other businesses or persons. Such powers should be exercised through lawful process (for example, subpoenas, summonses, search and seizure warrants, or court orders) and be available for use in investigations and prosecutions of money laundering, terrorist financing, and other underlying predicate offences, or in related actions e.g. actions to freeze and confiscate the proceeds of crime. In Poland, the bodies which carry out preparatory proceedings have – according to Chapter 25 (notably Articles 217, 218a) of the Code of Criminal Procedure - the right to search and arrest objects, which refers to any kind of accounting, company and mail documentation.

253. The competent authorities have the power to take witness statements.

Recommendation 30

254. The structure of law enforcement within the police Force is outlined above. As noted, there are 409 officers involved in the fight against money laundering. Like all police officers, they have to be free of criminal convictions and be of high integrity. In accordance with regulations of the Decision 121 of 14 July 1999 of the Commander in Chief of the Police and regulations of the attachment to the Ordinance 805 of 31 December 2003 of the Commander in Chief of the Police, all police officers are obliged to follow a Code of Conduct (or Code of Ethics).

255. With regard to Criterion 30.3, in the Police training is mainly organised internally. Money laundering training is included in general training on economic and organised crime issues. There are annual trainings on money laundering and organised crime with the Ministry of Justice, prosecutors, and GIFI and other departments. Police training is organised every second month. Apart from that, whenever it is necessary, training is given. Course materials prepared by prosecutors were said to be widely disseminated. It was unclear how focused these course materials are on difficult evidential issues such as the level of evidence required to establish the

underlying predicate offence in an autonomous money laundering prosecution. More officers need training in modern techniques of financial investigation.

256. The tasks of the public prosecuting authorities are set out in the Law of June 20, 1985 on Public Prosecution Authorities. The Prosecutor General is the chief prosecuting authority, to which prosecutors of common and military structural units of prosecuting authorities are subordinated. The Prosecutor General manages the activities of the public prosecution office personally or through his deputy, issuing regulations, guidelines and orders. He may also undertake all and any activities belonging to the scope of activities of public prosecution or recommend their performance by the subordinated prosecutors; unless the Law provides that such activity may be performed by the Prosecutor General personally.

257. In performing their activities provided for in the applicable laws, the work of public prosecutors should be guided by principles of neutrality and equal treatment of all citizens. Extend independence of the public prosecutor is guaranteed by Art. 8 para. 1 of the Law on the Public Prosecution's Authority. External independence means in this context that the public prosecutor will act independently of any other authorities or persons. By contrast, internal independence is greatly restricted and the prosecutors are bound to the instructions of the superior public prosecutors. All Public Prosecutor's Office employees are obliged to keep public service secrets; violations are under criminal liability. They have to be of high integrity for appointment. Pursuant to Article 14 of the Law on Public Prosecution Authority, a candidate for a post of public prosecutor has to be of Polish citizenship and not deprived of any civil or public rights. It is required that a candidate should be of unimpeachable character and at least 26 years old. He/She has to be a law faculty graduate and pass the prosecutor-exam after three years of training at local District Prosecution Office. Then, a candidate becomes an assistant prosecutor and after at least a year of further practice is appointed for a post of public prosecutor at District Prosecution Office.

258. Public Prosecutors participate in training organised by GIFI. In June, September and October 2004, 30 Public Prosecutors conducting and supervising cases concerning money laundering participated in three rounds of trainings organised by GIFI. At the end of November 2004, 12 public prosecutors from various units of Public Prosecutor's Office participated in the 3rd symposium organised by the Main Headquarters of Police, co-financed by OLAF, concerning the problems of money laundering, presenting criminal mechanisms identified during own proceedings to the participants. In 2005, 20 public prosecutors participated in a training organised by GIFI and the United States Department of the Treasury, and a similar number participated in the 4th symposium concerning the methods of conducting criminal proceedings on money laundering. It was unclear whether these courses formed on basic evidential issues in money laundering cases, including proof of the underlying predicate offence in autonomous money laundering cases. Given that prosecutors indicated that one of the major problems in money laundering cases was the inability often to define (and identify) the original crime, training needs to be (more) focused on evidential issues in such cases.

Additional elements

259. The evaluators were not advised about any special training or educational programmes provided for judges and courts concerning money laundering and terrorist financing offences, and the seizure, freezing and confiscation of property that is the proceeds of crime or is to be used to finance terrorism.

Recommendation 32 - *Statistics – investigations, prosecutions and convictions*

260. The prosecutors are bound under the AML Act to provide feedback to the FIU on the cases it refers to the prosecutors. Pursuant to Article 14 of the AML Act, prosecutors are bound to notify

GIFI of instituting an investigation concerning money laundering offences. Such notification should embrace the circumstances of the offence, as well as persons engaged in it. The evaluators were provided onsite with very basic statistics on the number of cases referred to the prosecutors by GIFI and the number of indictments, and convictions for money laundering. Beyond these superficial figures the evaluators were not provided with hard statistical information about the types of money laundering cases that were being prosecuted in order to form a judgment on the real effectiveness of criminalisation. As noted under Section 2.1, the Polish authorities provided at the pre-meeting some further statistical information in respect of the year 2006 (see footnote 5). The examiners sought statistics on the predicate offences, whether they were self laundering, or whether they were autonomous prosecutions (see footnote 5). Turning to Police generated money laundering cases, the evaluators had no information on numbers on site. At the pre-meeting, the evaluators were advised that in 2006 there were 26 police-generated cases. Approximately 80 % of Police investigations are reactive to GIFI reports. The types of offences from which money laundering cases are generated by the Police was unclear. Statistics should be available in this regard. Equally detailed law enforcement information on the number of cases in which confiscation, seizure and freezing were ordered were not readily available in any detailed form which would assist conclusions being drawn on the effectiveness of the system.

261. There have been no financing of terrorism enquiries, and no prosecutions or convictions.

2.6.2 Recommendations and comments

262. There has been considerable emphasis on fuel fraud and scrap metal cases, which are important in the local context. That said, overall the law enforcement response to the money laundering issue appears to be mainly reactive to GIFI notifications and the number of police generated money laundering cases (apart from the year 2006) was quite unclear.

263. Different stages of investigations can be handled by different officers, and all are dependent on the supervision of the prosecutors.

264. There are no directions encouraging proactive financial investigation (following the money) in major proceeds-generating cases and this should be considered. Equally more use could be made of joint teams and co-operative investigations with the GIFI. To improve the performance of the Police in generating money laundering cases outside of the reporting regime a specialised money laundering Unit with dedicated officers and financial investigators trained in modern financial investigative techniques should be considered.

265. More detailed statistics are required to demonstrate the effectiveness of the law enforcement regime overall. Statistics need enhancing to ensure that those reviewing the system have a clearer picture of the types of money laundering cases that are being brought, whether they are prosecuted as autonomously or as self laundering, seize and number of confiscation orders and whether freezing occurs at early stages to prevent proceeds being dissipated. These issues need addressing. More focused training is required of the Police and prosecutors in difficult evidential issues in money laundering cases, and more officers trained in modern financial investigation would develop the law enforcement response significantly.

2.6.3 Compliance with Recommendations R.27, R.28, R.30 and R.32

	Rating	Summary of factors underlying rating
R.27	**Partially compliant**	There are designated law enforcement authorities but more emphasis should be placed on Police generated money laundering cases by proactive financial investigation in major proceeds-generating cases.
R.28	**Compliant**	

2.7 Cross border Declaration or Disclosure (SR.IX)

2.7.1 Description and analysis

266. The Customs authorities are responsible for the cash movement control. Customs are a "co-operating unit", as opposed to an obliged institution (see Article 2 AML Act). The Border Guards are responsible for the control of the movement of people. Thus, the initiation of control activities with a view to disclosure of transported items is with the Border Guards.

267. Criterion IX.1 is covered by a declaration system. Residents and non-residents crossing the State border are obliged to declare in writing to Customs authorities or the Border Guard executing customs controls the importation to Poland of gold, or platinum, currency and also domestic or foreign currencies, if their total value exceeds 10,000 Euros (Article 18 para 1 of the Foreign Exchange Law).

268. Residents and non-residents, in order to obtain confirmation of the importation, may also declare in writing to Customs authorities or the Border Guards executing customs controls the importation to Poland of gold or platinum currency and also domestic or foreign currencies, if their total value does not exceed 10,000 Euros (Article 18 para 2 of the Foreign Exchange Law).

269. Residents and non-residents exporting gold or platinum currency and also domestic or foreign currencies, if their total value exceeds 10,000 EUR are obliged to present to the Customs authorities or Border Guards executing Customs controls, without prior requests, documents acknowledging the authorisation for exportation or foreign exchange (Article 19 of the Foreign Exchange Law).

270. According to Article 20 of the Foreign Exchange Law, residents and non-residents are generally obliged to present to Customs authorities or Border Guards executing customs controls importation, on their request, imported or exported domestic or foreign currencies. Customs authorities or Border Guards executing Customs controls are authorised to execute control activities in accordance with the rules foreseen for Customs and border control, in order to verify whether importation or exportation to Poland of domestic or foreign currencies is carried out according to Law or on the conditions laid down in a foreign exchange authorisation. In the case of persons carrying amounts below 10,000 Euros, if there is a suspicion of money laundering or financing of terrorism, the Customs advised that they can ask the Border Guards to use their powers to detain for a reasonable time in order to ascertain whether money laundering or financing of terrorism can be found, in accordance with Criterion IX.3. The legal authority for this is an co-operation agreement between Customs and Border Guards signed on 28 January 2004.]. The examiners have not seen a clear legal basis for this. Additionally Customs have permit to stop and detain for up to 48 hours under the Fiscal Penal Code.

271. The Minister of Finance, in agreement with the Minister of Home Affairs, regulates the procedure of import confirmation to Poland and export confirmation of the domestic or foreign currencies and the list of documents confirming the authorisation for export of the domestic or foreign currencies as well as their formulas (Ordinance of Ministry of Finance from 16 September 2002).

272. Upon discovery of a false declaration, in accordance with criterion IX.2, Customs and Border Guards are authorised to proceed with the preliminary investigation according to the Penal Fiscal Code. Furthermore provisions allow for the possibility to levy a penalty for a fiscal offence in a

case where a natural person does not give oral or written explanations or does not hand over necessary documents relating to the control.

273. The Customs authorities inform GIFI about all the circumstances where suspicion is accused, without unnecessary delay. The number of reports to GIFI is said to be increasing. In 2005 there were 120 suspicious transactions reports. In 2006 up to the time of the onsite visit, there were 78 reports.

274. The retention for use by appropriate authorities of declarations that exceed the perceived threshold (and false declarations) is regulated by the Ministry of Finance Ordinance of 16 September 2002 (Criterion IX.4). The GIFI has direct access to all Customs information (Criterion IX.5) as both are within the Ministry of Finance. GIFI receives from the customs authorities any information on export/import of foreign currency through the Polish border. On the basis of such information, supplied periodically, a special database was created by GIFI (containing identifying data of a person, indication of the border pass, date and sum of imported money etc.) This database is one of the sources of information checked by analysts during the ongoing intelligence. However, if the profile of any cross-border operation gives reason for suspicion at the moment of inserting into the database, the operation is subject to analysis.

275. There have been efforts towards strengthening co-operation between the Customs authorities, Tax revenue, the Police and the Border Guards by signing agreements in the area of consultations concerning persons suspected of financing of terrorism. This should allow swift exchange of information. There are also common forms which are used for declaration of foreign or national currencies and also the same system of powers conferred on Customs Service and Border Guards. At the international level (Criterion IX.7), Poland concluded bilateral agreements with 29 countries (including all neighbouring countries).

276. On sanctioning, the Customs normally seize the money in the case of false declarations and initiate an administrative investigation. Sanctions are said to be covered in the Fiscal Penal Code and to be up to 10 years of imprisonment. These sanctions apply to both persons making false declarations (Criterion IX.8) and persons carrying out physical cross-border transportation of currency or bearer negotiable instruments that are related to money laundering or financing of terrorism, as covered by Criterion IX.9.

277. Criterion IX.10 (relating to Recommendation 3) is covered in the Fiscal Penal Code.

278. With regard to unusual cross border movements of gold, precious metals or precious stones (Criterion IX.12), the Polish authorities advised that they expect the Customs would be informed in advance by other national services about specific threats and that they would anticipate the co-operation envisaged in Criterion IX.12. There is nothing which precludes Polish Customs from making such disclosures reciprocally.

279. The reporting system is subject to strict safeguards under the Law on protection of personal data. Filed reports are maintained in computer databases, and available to GIFI.

280. It was unclear whether all the measures in the Best Practices paper had been implemented.

Statistics

281. The Polish authorities provided the following information:
In 2005, infringements and crimes in the scope of customs or foreign currency resulted in 38,995 proceedings initiated by the Customs (supervised by the Prosecutors), as follows:
- 35,938 cases for the value of PLN 83,003,673 concerning import (over 20,000,000 EUR)
- 435 cases for the value of PLN 4,558,484 concerning export (over 1,000,000 EUR)

- 2,622 cases for the value of PLN 2,484,985 with no specific direction (concerning excise tax) – over 600,000 EUR

(Data provided by the computer system registering cases of fiscal crimes - so-called ESKS - as of 15 March 2006).

Fiscal criminal proceedings initiated; goods and means of payment seized – totals

I-IV quarter 2004
Number of cases 33,557
Value of means of payment seized 90,491 PLN
Value of goods seized 130,905,177 PLN
Value of goods and means of payment seized 130,995,668 PLN (over 33,500,000 EUR)

I-IV quarter 2005
Number of cases 38,995
Value of means of payment seized 1,519,676 PLN
Value of goods seized 88,527,464 PLN
Value of goods and means of payment seized 90,047,140 PLN (over 23,000,000 EUR)

Fiscal criminal proceedings initiated ; goods and means of payment seized– import

I-IV quarter 2004
Number of cases 30,943
Value of means of payment seized 0 PLN
Value of goods seized 118,221,200 PLN
Value of goods and means of payment seized 118,221,200 PLN (over 30,000,000 EUR)

I-IV quarter 2005
Number of cases 35,938
Value of means of payment seized 0 PLN
Value of goods seized 83,003,673 PLN
Value of goods and means of payment seized 83,003,673 PLN (over 21,000,000 EUR)

Fiscal criminal proceedings initiated; goods and means of payment seized– export

I-IV quarter 2004
Number of cases 673
Value of means of payment seized 90,491 PLN
Value of goods seized 6,878,669 PLN
Value of goods and means of payment seized 6,969,160 PLN (over 1,750,000 EUR)

I-IV quarter 2005
Number of cases 435
Value of means of payment seized 1,519,676 PLN
Value of goods seized 3,038,808 PLN
Value of goods and means of payment seized 4,558,484 PLN (over 1,160,000 EUR)

Fiscal criminal proceedings initiated; goods and means of payment seized– no specific direction (excise)

I-IV quarter 2004
Number of cases 1,944
Value of means of payment seized 0 PLN
Value of goods seized 5,805,294 PLN
Value of goods and means of payment seized 5,805,294 PLN (over 1,480,000 EUR)

I-IV quarter 2005
Number of cases 2,622
Value of means of payment seized 0 PLN
Value of goods seized 2,484,985 PLN
Value of goods and means of payment seized 2,484,985 PLN (over 630,000 EUR)

Means of payment seized I-IV quarter 2004-2005

Foreign currency	I-IV Quarter 2004		I-IV quarter 2005	
	cases	**amount**	**cases**	**amount**
USD	3	62 116	19	866 017
EUR	1	28374	11	555 630
GBP	0	0	3	97 973
SKK	0	0	1	36
HUF	0	0	1	16
Totally	**4**	**90 490**	**35**	**1519672**

2.7.2 Recommendations and comments

282. Both the Customs and Border Guards are responsible for cash movement control and the Border Guards are also responsible for control of the movement of people and goods. It was explained during the pre-meeting that co-operation between the Border Guards and the Customs services has a legal basis. It is the "Agreement between the Commander in Chief of the Polish Border Guard and the Minister of Finance on common co-operation between Border Guard and Customs of 28 January 2004". The cooperation with the Customs Service consists of, *inter alia*: mutual assistance in combating tax offences and tax petty offences, joint organisation and carrying out of activities aiming at streamlining (improving) border traffic flow and preventing criminality, including intensified customs control and border control as well as exchanging/transferring information by competent bodies of the both services. It should be clearly stressed, that the competences of the two services are different. The main statutory tasks of the Border Guard are control of the border traffic and protection of the border, whereas the main task of the Customs Service is the control of international traffic of goods. However, there appears to be no clear legal basis for the competent authorities to make targeted inquiries, based on AML/CFT intelligence or suspicion or on a random basis.

283. There are numerous statistics provided on fiscal proceedings, which appear to show that there is a functioning control system at borders, though the statistics provided in the MEQ are difficult to follow in the absence of some further explanations.

284. Moreover, the examiners have not seen any statistics on detentions of persons on the grounds of suspicion of money laundering / financing of terrorism. There have been no reports on terrorist financing which raises concerns as to whether Customs (and Border Guards) are fully sensitized to all the issues involved in financing of terrorism.

2.7.3 Compliance with Special Recommendation SR.IX

	Rating	Summary of factors underlying rating
SR.IX	**Largely compliant**	• More targeted co-operative enquiries are encouraged. • More sensitisation to terrorist financing issues is required.

3 PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

285. In Poland, the preventive side of the AML/CFT system is – nearly exclusively – rooted legislatively in the Act of 16 November 2000 on Counteracting Introduction into Financial Circulation of Property Values derived from Illegal or Undisclosed Sources and on the Counteracting the Financing of Terrorism (hereafter referred to as the AML Act, Annex 1) and the "Regulation of 21 September 2001 on establishing the form of a register of transaction, the way of keeping the register and the procedure of conveying the registry data to the General Inspector of Financial Information" (Annex 11). The Act is very detailed. The Act requires maintenance of register and subsequent reporting of transactions above the threshold of € 15,000 and suspicious transaction reporting. Identification of customers who perform above threshold and suspicious transactions is regulated in detail and includes a list of required information, both for physical persons and legal entities.

286. The following types of financial institutions are covered by Article 2 of the AML Act as "obligated institutions":

- banks, including the National Bank of Poland – where it operates bank accounts of legal persons, numismatics sales, purchases gold and exchanges damaged legal tender in accordance with the provisions of the law of 29 August 1997 on the National Bank of Poland (Journal of Laws No. 140, item 938 with subsequent amendments),
- foreign bank branches;
- electronic money institutions, branches of foreign electronic money institutions and settlement agents on the basis of the Law of 12 September 2002 on electronic instruments of payment (Journal of Laws No. 169, item 1385);
- investment companies and custodian banks;
- Joint Stock Company National Depository for Securities S.A. as far as it keeps securities' accounts;
- insurance companies, the main branches of foreign insurance companies;
- investment funds;
- investment funds societies;
- co-operative savings and credit unions;
- the state public utility enterprise Polish Post;
- entities engaged in currency exchange;
- entities conducting leasing and factoring activity.

Customer Due Diligence and Record Keeping

3.1 Risk of money laundering / financing of terrorism:

287. As described in the FATF Recommendations, a country may decide not to apply certain AML/CFT requirements, or to reduce or simplify the measures being taken, on the basis that there is low or little risk of money laundering or financing of terrorism. Currently Polish provisions do not allow for simplified customer identification or departure from the registration of transactions carried out by the entities classified by a given bank as belonging to the category of low risk of money laundering or terrorist financing. The law excludes certain types of transactions which do not have to be registered - e.g. transfers onto long-term deposit accounts - but not certain types of customers.

288. Nevertheless, taking into account ongoing work on 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 in European Union and the obligation to implement its different provisions, including the possibility for exercising simplified due diligence, Poland is going to analyse the possibility. The implementation of the Third European Union Directive will allow consideration of a more risk based approach.

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

3.2.1 Description and analysis

Recommendation 5

Anonymous accounts and accounts in fictitious names

289. Criterion 5.1 of the Methodology is marked with an asterisk. This means that it belongs to the basic obligations that should be set out in a law or regulation. In this context, "Law or Regulation" refers to primary and secondary legislation, such as laws, decrees, implementing regulations or other similar requirements, issued or authorised by a legislative body, and which impose mandatory requirements with sanctions for non-compliance. Separate to laws or regulation are "other enforceable means" like Recommendations, guidelines, instructions or other documents or mechanisms that set out enforceable requirements, with sanctions for non-compliance, and which are issued by a competent authority (e.g. a financial supervisory authority) or an SRO. In other words: according to the Methodology, obligations set out in law or regulation as well as in other means have to be enforceable. In addition, the law or regulation has to be issued or authorised by a legislative body.

290. The Polish law does not allow for the keeping of anonymous accounts, accounts in fictitious names or collective accounts (i.e. such accounts where assets of different owners are registered). Art 49 para. 2 of the Banking Act (Annex 12) prohibits banks from opening bank accounts for the bearer. The bank may issue a personal savings book or other personal document confirming the conclusion of the agreement to the savings account holder or the savings deposit account holder. Moreover, the bank account agreement is concluded in writing and should specify the parties of the agreement, therefore, it is not possible to open an "anonymous" bank account (Article 52 of the Banking Act).

291. The relevant laws cover other types of business relationships (Securities Act, Insurance Act) and state that a customer has to be identified, and that the account has to be in a name. The level and data of the identification process are discussed in the chapter on Due Diligence.

Customer due diligence

When CDD is required

292. Criterion 5.2 of the Methodology has an asterisk too. It requires all financial institutions to undertake CDD when:

a) establishing business relations;
b) carrying out occasional transactions above the applicable designated threshold (USD/€ 15,000). This also includes situations where the transaction is carried out in a single operation or in several operations that appear to be linked;
c) carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII;

d) there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or thresholds that are referred to elsewhere under the FATF Recommendations; or
e) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

293. The Polish AML Act focuses very strongly on the automatic reporting of transactions to the GIFI (called "registration" as the obliged entities have to keep a register of such transactions and forward this information to the GIFI). Therefore, many of the obligations in the AML Act stem from this primary duty to register certain transactions.

294. Thus, according to Article 8 of the AML Act the obliged institution receiving an instruction or order from a client to execute a transaction in excess of EUR 15,000, shall register such a transaction, also when it is executed involving more than a single operation, if circumstances suggest that these operations are linked together (criterion 5.2 b). If circumstances suggest that the property values involved in this transaction may originate from illegal or undisclosed sources, the obliged institutions shall register such a transaction regardless of its value and nature. In order to fulfil the registration duty, obliged institutions shall identify their clients.

295. The obligation to register above-threshold transactions does not concern electronic money institutions, branches of foreign electronic money institutions and agents performing settlements (Article 8 para. 5 of the AML Act). This constitutes a gap with regard to CDD of electronic money institutions´ customers. However, the evaluators were told that Poland had no electronic money institutions at this point in time.

296. As mentioned above, the AML Act heavily emphasizes maintaining a register of and subsequently reporting all transactions above the threshold of EUR 15,000 and transactions which are suspicious. Identification of customers who do above threshold transactions is regulated in detail, including a list of required information, both for natural persons and legal entities.

297. However, the evaluators have doubts that the AML Act covers Customer Identification when starting a business relationship (criterion 5.2 a), though the Polish authorities explained that so far no problems in this regard occurred, because in their opinion Article 9 para 1 of the AML Act covers this. In addition, the AML Act does not cover customer identification when carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII, except when these are suspicious transactions or transactions above 15,000 Euro (criterion 5.2 c). The AML Act also does not cover customer identification when the financial institution has doubts about the veracity or adequacy of previously obtained identification data (criterion 5.2 e). As these requirements are also not covered by other laws, the evaluators understood that the aforementioned sub-criteria are not met.

Required CDD measures

298. Criteria 5.3 and 5.4 (a) are both marked with an asterisk. Under criterion 5.3 financial institutions are required to identify permanent or occasional customers (whether natural or legal persons or legal arrangements) and verify the customers' identity using reliable independent source documents, data or information. In the case of customers that are legal persons and arrangements, criterion 5.4 (a) provides that financial institutions should be required to verify that any person purporting to act on behalf of the customer is so authorised and verify the identity of that person.

299. In order to fulfil their registration duty, obliged institutions shall identify their clients. The identification shall involve the following (Article 9 para. 2 of the AML Act):

(1) in the case of natural persons or their representatives - determining and noting the distinguishing features of a document confirming the person's identity pursuant to separate regulations, or of a passport, as well as the first name, last name, the citizenship and address of the person executing the transaction, and furthermore the PESEL (national citizens' registry) number in the case of the identification on the base of identity card or country code in the case of the passport. In the case of the person in whose name or on whose behalf the transaction is being executed - determining and noting her first name, last name and address;
(2) in the case of legal entities: noting of up-to-date information from a court registry extract or some other document specifying the name (firm), the organisational form of the legal entity, its seat and address, and information from a valid document confirming the authority of the person executing the transaction to represent the legal entity, as well as noting of data described in Paragraph 1 above pertaining to the representing person;
(3) in the case of organisational units lacking legal entity status: noting of information from a document indicating the organisational form of the entity, its seat and address, and information from a document confirming the authority of the person carrying out the transaction to represent the entity, as well as noting of data described in Paragraph 1 above pertaining to the representing person.

These identification requirements are in line with the international standards, particularly with criteria 5.3 and 5.4 of the FATF Methodology.

300. As far as the legal persons being entrepreneurs are concerned, the authorisation for acting on their behalf can be checked in the National Court Register. The said Register is public, in that everyone has access to the data gathered in it (including the scope of activities). Everyone has the right to receive authenticated copies, excerpts, certificates of data contained in the Register (Law of 20 August 1997 on the National Court Register – O.J. of 2001, No. 17 item 209).

301. Other laws, such as the Banking Act (Annex 12), cover some aspects of CDD, such as identification of the customer when a bank enters a business relationship, or the obligation to create a customer profile under the Securities Act; but there is no mention of the steps to be taken when identifying the client and no mention of verification anywhere. Supervisors refer to the Act when asked, but in the Act, only the above mentioned situation (above threshold and suspicious transactions) is covered. However, for example as regards the insurance sector, it seems that customer identification works in practice there, particularly concerning life insurance contracts which by definition require the gathering and processing of a large amount of personal data of the customers (including data of persons who will be authorised to receive the insurance benefits in the case of insurance accident which results in specific obligations on the part of the insurance undertaking).

Beneficial owners

302. According to the AML Act (Article 9 par. 3 and 3a) if circumstances of the transaction suggest, that the person executing it does not act in her own name, the obligated institution should try to identify the entities, in the name or on behalf of which the person executing the transaction is acting.

303. However, the AML Act contains neither a definition nor a requirement relating to beneficial owner. Supervisors and financial institutions did not read the Act as including an obligation to go further than asking for possible powers of attorney, or other forms of proxy, and did not interpret the relevant paragraph as an obligation going as far as the FATF standards require.

Purpose and intended nature of the business relationship

304. There is no requirement in the law or by other enforceable means (which are sanctionable) to obtain information on the purpose and intended nature of the business relationship.

Ongoing due diligence

305. Criterion 5.7 of the Methodology (again asterisked) requires financial institutions to conduct ongoing due diligence (which should include e.g. scrutiny of transactions to ensure that they are consistent with knowledge of the customer and the customer's business and risk profile.

306. The Polish legislation does not cover the requirement to conduct ongoing due diligence on the business relationship including keeping up-to-date data or information collected under the CDD process. This is only covered by the manual issued by GIFI; however, this manual is not enforceable and this is not covered by any other enforceable guidance either.

307. The heavy emphasis on transactions, not business relationships, and on above threshold registering and reporting becomes even more evident in the fact that there is no mention of "business relationship" in the Act, no mention of "ongoing monitoring", no mention of "risk" and the obligation to report in suspicious circumstances only refers to "transactions", so that a business relationship which over time shows risky or suspicious elements would not be covered by the text of the Act.

308. The Act mentions an obligation to create internal controls and procedures but they refer only to identification of clients, the keeping of records, and training of employees to recognize transactions potentially linked to ML/FT. However, this seems a too slim legal basis to cover all the requirements mentioned above. The supervisors, in their onsite inspections, cover those aspects explicitly mentioned in the law, such as maintaining a register, identification above threshold, appointing an AML/CFT officer, record keeping and training, but the aspects mentioned in the paragraph above are only marginally included.

309. No regulation by the supervisors or GIFI has been issued to address these missing elements, either.

310. All this shows that the AML Act is not interpreted in practice to cover these elements, even by those bodies in charge of developing guidance, supervising, inspecting and sanctioning violations under the Act.

Risk

311. Criterion 5.8 requires financial institutions to perform enhanced due diligence for higher risk customers.

312. Enhanced due diligence in higher risk situations such as non face to face relationships, legal persons such as companies on bearer shares, non-resident customers, private banking and PEPs is completely missing, nevertheless GIFI when providing trainings informs about criteria which should be applied. Different typologies presented give clear view about higher risk activities. This issue is also included in a manual for obliged institutions and cooperating entities entitled "Counteracting money laundering".

313. Due to differing information provided by the Polish authorities, it appeared that a branch with a headquarter abroad may rely on CDD done by headquarters abroad. Given that the legislation

does not permit reliance on third parties, it was, however, unclear if the supervisory bodies sanction branches, when and if they rely on such non-face to face identification.

Simplified or reduced CDD

314. As mentioned under Section 3.1., Polish provisions do not allow for simplified customer identification or abandonment of the registration of transactions carried out by the entities classified by a given bank as belonging to the category of low risk of money laundering or terrorist financing. However, the AML Act excludes certain types of transactions which do not have to be registered; e.g. transfers onto long-term deposit accounts - but not certain types of customers.

315. Article 8 of the AML Act provides several exceptions from the obligation to register (i.e. automatically report) transactions which exceed 15,000 Euros, particularly
    - in case of a valid life insurance policy, if the total amount of periodical premiums that are to be paid during a given year does not exceed the equivalent of 1.000 EUR or a single premium does not exceed the equivalent of 2.500 EUR (para. 1c).
    - in case of insurance policies combined with old-age insurance, unless the insurance terms and conditions contain for the clause on payable renouncement, on the part of the insured person, of the rights resulting from the policy and if the policies cannot be used as a credit or a loan guarantee (para. 1d).
    - for real estate agents, electronic money institutions, branches of foreign electronic money institutions, agents performing settlements, counsels, legal advisers and foreign lawyers as well as competent auditors and tax advisers (para. 5).

    However in any case all obligated institutions are required to register transactions if there is a suspicion of money laundering or terrorist financing (Article 8 par. 3 of the AML/CFT Act).

316. Nevertheless, taking into account ongoing work on "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" ("Third anti-Money Laundering Directive") and the obligation to implement its provisions, which include the possibility of exercising simplified due diligence, Poland will analyse this possibility.

Timing of verification

317. In order to fulfil the registration duty, obligated institutions shall identify their clients whenever they receive from them instruction or order to execute a transaction on the basis of the documents performed each time the instruction or order to execute a transaction is given or a contract with a client is being concluded (Article 9 par. 1 of the AML Act). However, neither the AML Act nor other laws (Banking Act, Insurance Act and Securities Act) require explicitly the identification/verification of clients when starting a business relationship. Supervisors, especially the banking supervisors, confirmed that the practice is followed, and that no account is opened without proper documentation.

Failure to satisfactorily complete CDD

318. There is no provision in the law requiring the financial institution to consider making a suspicious transaction report when it is unable to complete CDD. The same applies for situations where the financial institution has already commenced the business relationship. There is no requirement to terminate the existing business relationship when CDD is not completed. These issues should be required, in line with paragraphs 5.13 and 5.14 of the Methodology, by other enforceable means for all financial institutions.

Existing customers

319. Financial institutions should be required to apply CDD requirements also to existing customers on the basis of materiality and risk. Some examples are given in the box in the Methodology of the times when this might be appropriate – e.g. when a transaction of significance takes place, when the institution becomes aware it lacks sufficient information about an existing customer etc. At present, there are no provisions in the Polish legal system addressing these issues and, as far as the examiners understood, it is also not done in practice (criterion 5.17). This issue should also be addressed preferably in the Law or by enforceable means.

European Union Directive

320. According to Article 7 of the 2nd European Union Anti-Money Laundering Directive, member States shall ensure that financial institutions refrain from carrying out transactions which they know or suspect to be related to money laundering until they have apprised the competent authorities. In addition, these authorities should have the power to stop the execution of a transaction that has been brought to their attention by an obliged person who has reason to suspect that such transaction could be related to money laundering. Chapter 5 of the AML Act (specifically Articles 16, 17 and 18) deal with these issues. Article 16 places a duty on obligated institutions which receive an instruction to execute a transaction in circumstances justifying a suspicion of money laundering to forthwith inform the GIFI and to indicate the grounds to support a suspension of the transaction or an account blocking and to indicate the planned date of the transaction. Article 17 provides an exemption from prior notification if the notification in Article 16 "cannot" be sent prior to the execution or during the execution of the instruction from the client. In these circumstances the GIFI should be informed about the transaction immediately after its execution and provided with reasons for the lack of prior notification. The Polish authorities indicated that Article 18 covers the account blocking procedure: if a transaction to be executed may be linked to the offence referred to in Article 299 of the Penal Code, the General Inspector may, within 24 hours following the confirmation of the notification receipt, demand the obligated institutions concerned, in writing, to suspend the said transaction or to block the account for a period not exceeding 48 hours following confirmation of the notification receipt. At the same time, the General Inspector shall notify the proper public prosecutor about the suspected offence and shall forward to him the information and the documents relating to the suspended transaction.

321. Transaction suspension or account blocking may be demanded only by the General Inspector or by two employees of the unit, duly authorized by him in writing and acting together. The obligated institution shall suspend the transaction or block the account after receiving the written demand referred to in Paragraph 1 above, with no delay.

322. The broad requirements of Article 7 of the 2nd European Union Anti-Money Laundering Directive have been transposed into the Polish Legislation. The Directive uses more precise language for the exemption from prior reporting ("*where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money-laundering operation*"). It would assist if the Polish authorities gave more guidance which specifies what reasons may be acceptable for a departure from prior notification with some examples of the types of transaction where this may be appropriate. The Polish authorities indicated that further explanations can be given orally to the obliged institutions and that the guidance issued by GIFI gives explanation to the obliged institutions on these procedures. The Polish authorities should satisfy themselves that their Guidance fully covers these issues.

Recommendation 6

323. Poland has not yet implemented AML/CFT measures concerning politically exposed persons (PEPs). According to the opinion of some representatives of the financial sector, the Data Protection Act (Annex 13) prohibits them from keeping databases of PEPs as there is no mandate in the law to collect this type of data. Representatives from the banking sector advised the evaluators that there was neither a policy in place nor any guidance on this issue and that they are waiting for the implementation of the 3rd EU Anti-Money Laundering Directive.

Additional elements

324. Poland had signed but not ratified and implemented the 2003 United Nations Convention against Corruption at the time of the on-site visit[20].

Recommendation 7

325. Criteria 7.1 to 7.5 of the Methodology cover cross-border correspondent banking and other similar relationships (gather sufficient information about a respondent institution, assess the respondent institution's AML/CFT controls, obtain approval from senior management, document the responsibilities, etc. Poland has not implemented any AML/CFT measures regarding the establishment of cross-border correspondent banking relationships. However, inspections show that banks carefully select the respondent institutions and approval of senior management before establishing new correspondent relationship is obtained. The inspections also show that if there is no customer data on the money transfer from abroad, the banks request their correspondent financial institutions to supply the information on the customer's identity.

326. It is not possible to operate "payable through" accounts in Poland.

327. Overall, the Polish authorities need at least to prepare enforceable guidance covering Criteria 7.1 to 7.5 in respect of all participants in the financial sector that may be involved in correspondent or similar relationships. GIFI when providing trainings informs about criteria which should be applied. Different typologies presented give a view about higher risk activities. This issue is also included in a manual for obliged institutions and cooperating entities entitled "Counteracting money laundering" issued by GIFI.

Recommendation 8

328. Criteria 8.1 to 8.2.1 of the Methodology cover policies to prevent the misuse of technological developments; policies regarding non-face to face customers including specific and effective CDD procedures to address the specific risks associated with such customers.

329. Although Article 28 of the AML Act imposes a general obligation on the obligated institutions to "*devise internal procedures for preventing the introduction into financial circulation of property values derived from illegal or undisclosed sources or the financing of terrorism, in particular relating to the fulfilling of the requirement of a client's identification and keeping of information gathered as part of the identification process*", there is no requirement in the Polish system for financial institutions to have policies and procedures in place to address the *specific* risks of technological developments in money laundering or terrorist financing schemes[21]. Article 28 of the AML Act imposes an obligation on the obliged institution to prepare internal procedures in

[20] Poland ratified the Convention on 15 September 2006.

[21] The Banking Supervision Commission issued in March 2007 a regulation concerning risk management and internal control system in the banks which deals among others with obligations connected with new technologies area.

respect of counteracting money laundering. In these procedures the banks include all distribution channels of their products and describe the method of conduct in case of transactions carried out without the physical participation of the customers.

330. As it is not allowed to start a business relationship without face to face-contact, this issue does not need to be addressed under Recommendation 8.

331. However, new technologies used (or new solutions such as outsourcing) in areas such as banking and securities, have to be presented to the supervisor and are formally checked and approved by the supervisor. This seems to be a useful element to ensure a high standard in these entities related to AML/CFT as well. The Minister of Finance issued a Regulation on the procedures and conditions to be followed by investment firms and custodian banks in the course of their activities dated 28 December 2005 (Annex 14) which covers verification of already identified customers during non-face to face transactions.

3.2.2 Recommendations and comments

Recommendation 5

332. Due to a rather formalistic approach to financial business, it seems that in practice the identification of customers is generally in line with FATF standards; on the other hand there is no clear obligation embedded in Law or Regulation, and there seem to be, based on interviews with the private sector, important missing elements in the existing practice, particularly related to beneficial owners and the higher risk areas mentioned above. A potential weakness seems to be contained in the strict Data Protection rules which could lead to difficulties. Some private sector entities feel that any assessment of risk, i.e. processing customer transaction data according to filters, collecting additional information not explicitly mentioned in the law, such as sources of funds, might leave them open to action against them by the General Inspector on Data Protection. As noted above, the Data Protection Act (Annex 13), in the interpretation of the financial sector, explicitly forbids them to collect and process data not clearly mandated by a law. As an example, a few years ago, the Data Protection Inspector required banks to destroy their existing collection of copies of ID, and only an explicit mention of the right of a bank to collect and process all customer data in a subsequent Banking Act amendment now allows for the making and storing of such copies of ID documents. Therefore, essential elements of the Customer Due Diligence process do not exist in the Polish legal framework.

333. Financial institutions should be clearly required to identify customers when starting a business relationship, when carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII and when the financial institution has doubts about the veracity or adequacy of previously obtained identification data.

334. Identification requirements concerning above threshold transactions should be applicable also to customers of electronic money institutions.

335. The provision to which the Polish authorities pointed dealing with the concept of beneficial owner (Art 9 para 3a of the AML Act) does not cover the concept of beneficial owner as it is described in the Glossary to the FATF Recommendations. This should be addressed and financial institutions required to take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is.

336. Turning to the sector most at risk (banking) overall, the risks of money laundering seemed to be managed in a reasonable manner, due to the following elements. This, in the evaluators' view is

due to a number of factors including rather formalistic approach to banking services; the readiness to ask for identification rather broadly; and a very controlling Banking Supervisor, who approves most relevant new business ideas (such as outsourcing). However, since the risks are managed perhaps incidentally, because of other factors rather than in a conscious effort to address the risk of money laundering and terrorist financing, changes in factors totally unrelated to crime or money laundering may suddenly weaken the whole system substantially. For example, a liberalisation of rules related to general Banking Supervision would totally undermine the system.

337. For customers that are legal persons or legal arrangements, the financial institutions should be required to take reasonable measures to
- understand the ownership and control structure of the customer; and
- determine who are the natural persons that ultimately own or control the customer.

338. Financial institutions should be required to obtain information on the purpose and intended nature of the business relationship.

339. Financial institutions should be required to conduct on-going due diligence on the business relationship and to ensure that documents, data or information collected under CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

340. Financial institutions should be required to perform enhanced due diligence for higher risk categories of customers, business relationship or transaction, including private banking, companies with bearer shares and non-resident customers.

341. The Polish authorities should satisfy themselves that branches with headquarters abroad undertake the CDD process themselves as it is required by Polish Law and do not rely on their headquarters (as the Polish Law does not allow relying on third parties).

342. Financial institutions should not be permitted to open an account when adequate CDD has not been conducted. Where the financial institution has already started the business relationship and is unable to comply with CDD it should be required to terminate the business relationship. In both cases mentioned above the financial institution should consider making a suspicious transaction report.

343. Financial institutions should be required to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times.

Recommendations 6 and 7

344. Poland should implement Recommendations 6 and 7.

Recommendation 8

345. Financial institutions should be explicitly required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in ML and TF schemes.

3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	**Non compliant**	- The AML Act does not cover: • Customer Identification when starting a business relationship; • when carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII; • when the financial institution has doubts about the veracity or adequacy of previously obtained identification data; - Identification requirements do not cover above threshold transactions of electronic money institutions´ customers; - Although there are regulations in respect of proxies, there is no requirement to ascertain beneficial ownership, including no general requirement to identify and verify the identity of the beneficial owner and no requirements to take reasonable measures to determine the natural person with ownership or control over a legal person; - There is no requirement regarding: • the purpose and nature of the business relationship, • ongoing CDD, • enhanced CDD or conducting CDD on existing customers; - There is no requirement not to open accounts when satisfactory CDD cannot be completed; - No requirement to terminate the relationship with an existing customer when the financial institution is unable to comply with CDD.
R.6	**Non compliant**	Poland has not implemented any AML/CFT measures concerning the establishment of customer relationships with politically exposed persons (PEPs).
R.7	**Non compliant**	Poland has not implemented any AML/CFT measures concerning establishment of cross-border banking relationships.
R.8	**Partially compliant**	Financial institutions are not directly required to have policies in place to prevent the misuse of technological developments in ML and TF schemes.

3.3 Third Parties and introduced business (Recommendation 9)

3.3.1 Description and analysis

346. Neither the AML Act nor any other Law allows for reliance on third parties or other intermediaries to conduct due diligence. However - as far as could be clarified – it appeared that there might be cases where branches rely on CDD performed by headquarters abroad (see above para. 313).

347. It is not possible to share identification data within financial groups in Poland.

3.3.2 Recommendation and comments

348. Notwithstanding the possibilities mentioned in paragraph 346, as the Polish legislation does not allow for reliance on third parties and introduced business, the examiners considered that Recommendation 9 should be marked as not applicable.

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	**N/A**	As the Polish legislation does not allow for reliance on third parties and introduced business, Recommendation 9 is not applicable.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and analysis

349. Criterion 4.1 states that countries should ensure that no financial secrecy law will inhibit the implementation of the FATF Recommendations. Areas where this may be of particular concern are the ability of competent authorities to access information they require to properly perform their functions in combating money laundering or financing of terrorism; the sharing of information between competent authorities, either domestically or internationally; and the sharing of information between financial institutions where this is required by Recommendations 7 and 9 or SR.VII.

350. Disclosures to the GIFI are covered by Article 29 of the AML Act which stipulates that "*regulations limiting access to confidential information shall not apply to disclosing by obligated institutions of any information relating to transactions pursuant to this Act, except for data subject to state secrecy*". Indeed, GIFI also shares information with some other authorities as already noted (see Article 33 AML Act).

351. Article 15 of the AML Act authorizes the GIFI to request supervisory bodies and other co-operating units (see Article 2 para 8) to make available information and copies of documents.

352. Pursuant to Article 13a of the AML Act, obligated institutions shall make available the information concerning transactions subject to the AML Act upon written demand by GIFI.

353. Article 266 para 1 Penal Code provides the basic secrecy regulation which stipulates that anyone "*in violation of the law or obligation he has undertaken, discloses or uses information with which he has become acquainted with in connection with the function or work performed, or public, community, economic or scientific activity pursued shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years*".

354. Data protected by banking secrecy can only be accessed in specific situations and subject to conditions defined by law as mentioned below:

The Banking Act

355. The Banking Act provides that in the case of banking secrets being revealed the bank is liable for any loss caused (Section 105.5). The deliberate disclosure of a banking secret is subject to a fine and up to 3 years in prison (*lex specialis* in comparison to the general provision described at the beginning of this contribution). Under Section 108 a bank is not liable for any loss incurred during the execution of its duties for the prevention of the use of bank services for criminal purposes. If the suspicion of illegal operation turns out to be unfounded the State Treasury is liable.

356. According to Article 105 of the Banking Law, Banks shall be required 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.

357. With a Court order, it is also possible to obtain such information before any charges are brought against legal or natural persons. In practice, this does not appear to cause problems.

Act of 22 May 2003 on Insurance Activity

358. The breaches of the secrecy provisions within the insurance sector are covered by Article 19. Information can be provided e.g. to Police, courts or public prosecutor's office and GIFI.

Act on Trading in Financial Instruments of 29 July 2005

359. According to Article 150, the professional secrecy obligation shall not be deemed breached, if it is disclosed e.g. to GIFI. Article 149 provides the circumstances under which information can be disclosed to prosecutors , courts etc.
360. 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).

National Bank of Poland Act of 29 August 1997

361. Banks are bound under Section 23.2 to transfer to the NBP all data necessary for establishing monetary policy and for the periodical assessment of the State's financial situation including foreign currency balances and operations. Banks are also obliged to transfer to the NBP all data necessary for the assessment of their financial situation and banking sector risk. The confidentiality of the data is guaranteed by Section 23.5 which stipulates: the data can only be used for analytical work and for the appraisal and preparation of balances of foreign assets and liabilities mentioned in this section and cannot be made accessible to third persons.

362. The NBP Act also contains a general clause concerning secrecy. Section 55 provides that the NBP employees and members of the Monetary Policy Board at and other advisory bodies operating within the NBP, must keep secret all information constituting state, banking or professional secrets obtained during their work at the NBP. This obligation continues to be binding even when they are no longer employed by NBP.

363. Regarding the exchange of information among financial supervisors see Chapter 6.1 (domestic exchange of information) and 6.5 (international exchange of information).

3.4.2 Recommendations and comments

364. Financial secrecy laws do not inhibit the implementation of FATF Recommendations. Financial secrecy can be penetrated in appropriate circumstances.

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	**Compliant**	

3.5 Record keeping and wire transfer rules (R.10 and SR. VII)

3.5.1 Description and analysis

Recommendation 10

365. Recommendation 10 has numerous criteria under the Methodology which are asterisked, and thus need to be required in law or regulation. Financial institutions should be required by law or regulation:

- to maintain all necessary records on transactions, both domestic and international, for at least five years following the completion of the transaction (or longer if properly required to do so) regardless of whether the business relationship is ongoing or has been terminated;
- to maintain all records of the identification data, account files and business correspondence for at least five years following the termination of the account or business relationship (or longer if necessary) and the customer and transaction records and information;
- to ensure that all customer and transaction records and information are available on a timely basis to domestic competent authorities upon appropriate authority.

366. Transaction records are also required under Criterion 10.1.1 (which is not asterisked) to be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution. This needs to be required by other enforceable means (and be sanctionable).

367. Relating to Criterion 10.2 (identification data), as the Polish system is transaction based and does not mention the beginning of a business relationship, institutions are only obliged to keep records relating to transactions, which includes identification data, but not when commencing business relations.

368. According to the AML Act, the obligated institutions shall keep on file all accounting documents and other documents related to the registered transactions for five years beginning on the first day of the year following the year in which the last entry related to a given transaction was made (Article 8 para. 4). At the same time the information required as part of the identification procedure shall be kept for a period of five years starting from the first day of the year following the year in which the last entry concerning the given transaction was made (Article 9 para 4). Though not explicitly provided for by law, the Polish authorities consider that the term "transaction" also covers closing of an account. Neither in the AML Act nor the Banking Law is there a reference to keeping the documents longer than five years if requested by a competent authority in specific cases and upon proper authority.

369. In the case of liquidation, merger, division or transformation of an institution, the obligation to keep the documents continues (Article 76 of the Accounting Act; Annex 15).

370. Additionally, due to the specific character of the insurance sector, which includes entities recognised as institutions of public trust, legislation determines the specific method of keeping the accounting records. The scope of data acquired and kept by the insurance companies is regulated (among other issues) by the Regulation of the Minister of Finance of 8 December 2003 on detailed accounting rules for insurance undertakings (O.J. of 2003, No 218, item 2144; Annex 16). Article 6 of the Ordinance imposes a duty on insurance undertakings to run the register of insurance contracts containing, *inter alia*, the data on identification of the policyholder, and in the case of individual contracts also the data identifying the insured and the beneficiaries of the insurance contract; and the data identifying the insurance intermediary if the contract was concluded with his assistance. In addition, Article 11 of the Ordinance concerning the structure of the registers of damages (claims) imposes an obligation on the insurance undertakings to record the date of the damage registration, the date of its occurrence and reporting along with the link to the concluded insurance contract, as well as the data concerning the identification of a third person (if the perpetrator of the damage is identified). The abovementioned data is kept electronically.

371. Article 13a of the AML Act requires that all customer transaction records and information are available on a timely basis to domestic competent authorities upon appropriate request (criterion 10.3). In addition, according to Art. 88 of the Act on trading in financial instruments (Annex 17), an investment firm is required to promptly prepare and deliver - at its own cost - copies of the documents and other information carriers, and to provide written or oral explanations.

SR.VII

372. Under Criterion SR.VII.1, the Methodology requires for all wire transfers that financial institutions obtain and maintain full originator information (including name of the originator; originator's account number or unique reference number if no account number exists) and the originator's address (though countries may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth) and to verify that such information is meaningful and accurate. Under VII.2 full originator information should accompany cross-border wire transfers though under VII.3 it is permissible for only the account number to accompany the message (subject to conditions discussed below).

373. In the Polish legal framework, no obligation to identify customers who transfer money exists (except for transactions exceeding EUR 15,000 or suspicious transactions). It seems that the formal requirements do not allow money to be sent unless there is a name and address provided in the transfer order, but no checks are made unless the transactions is either above the threshold or suspicious. The text of the law, if interpreted generously, might suggest that identification of customers always has to occur when conducting a transaction, but the Banking Supervisors, the National Bank of Poland as supervisor for bureaux de change, and all private sector entities agree that identification only occurs in the two cases mentioned above (transactions exceeding EUR 15,000 or suspicious transactions), or based on internal procedures which reflect a special situation in an entity – e.g. credit unions only perform such services for members and therefore identify all customers for every transaction.

374. Concerning domestic banking wire transfers between account holders, financial institutions 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 are followed by all banks but they are not binding.

3.5.2 Recommendation and comments

Recommendation 10

375. The AML Act is only transaction based and refers to "last transaction made" in the provisions covering record keeping. This carries the risk that this might be interpreted too narrowly. The evaluators recommend that the text of the law should clearly state that all necessary identification data provided to the financial institution has to be kept for at least five years after the end of the business relationship as required by Recommendation 10 and criterion 10.2.

376. Financial institutions should be required to keep documents longer than five years if requested by a competent authority.

Special Recommendation VII

377. Poland should implement all the requirements of SR.VII.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**Partially compliant**	• As the AML Act is only transaction based, there is no guarantee that all necessary documents are kept, e.g. there is no explicit requirement in law or regulation to maintain records of the identification data for at least five years following the termination of an account or business relationship. • There is no requirement in law or regulation to keep documents longer than five years if requested by a competent authority.
SR.VII	**Non compliant**	Although some elements exist in practice, Poland has not implemented SR VII.

Unusual and Suspicious Transactions

3.6 Monitoring of transactions and relationships (R.11 and 21)

3.6.1 Description and analysis

Recommendation 11

378. Recommendation 11, which requires 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, needs to be provided for by law, regulation or other enforceable means.

379. The implementation of this Recommendation results indirectly from the obligation imposed by Article 8 (3) of the AML Act. In addition, the banking supervision repeatedly sent letters to all banks, in which it pointed to the necessity of detailed analysis of transactions connected with the knowledge of the type of customers' activities, types of earlier transactions, the amounts thereof, types of contracting parties, etc.

380. The internal procedures, e.g. of banks, contain exemplary types of transactions which may be connected with money laundering and the criteria to follow during the assessment performed in order to establish whether a given transaction has the characteristics of a suspicious transaction. Also GIFI distributes to all of the obliged institutions the lists of typologies.

381. Thus, there is an *indirectly* enforceable requirement that financial institutions examine all complex, unusual, large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. However, there is not an obligation to examine as far as possible the background and purpose of such transactions nor a requirement to keep any findings made by a financial institution regarding these or other suspicious transactions available for competent authorities and auditors for at least five years. During the pre-meeting, the Polish authorities informed that GIFI saw during the onsite inspections that banks set forth their findings about unusual complex transactions in writing.

Recommendation 21

382. Recommendation 21 requires financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not, or insufficiently apply, the FATF Recommendations. This should be required by law, regulation or by other enforceable means. It places an obligation on financial institutions to pay close attention to any country that fails or insufficiently applies FATF Recommendations and not just countries designated by FATF as non-co-operative (NCCT countries).

383. There is no specific requirement in the law which covers Recommendation 21. The countries on the FATF list and the OECD Offshore list, which has been published in a Regulation by the Minister of Finance, are known. There is no enforceable link between these lists and the AML Act, and there is no obligation to create any own list within the obliged entity to address the subject of geographical risk related to banking partners, customers, or incoming funds. This is only addressed by the non-binding manual issued by GIFI, which contains a list of countries and geographical areas to which obliged institutions should pay attention in the area of suspicious transaction reporting.

384. Counter-measures against a country that continues not to apply or insufficiently applies the FATF Recommendations would be applied via an ordinance issued by the Ministry of Finance.

3.6.2 Recommendations and comments

Recommendation 11

385. Recommendation 11 is only indirectly covered by Polish law. The examiners strongly recommend the Polish authorities to address all the subcriteria of Recommendation 11; that particularly financial institutions should be required 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, to examine as far as possible the background and purpose of such transactions and to set forth such findings in writing and to keep them available for competent authorities and auditors for at least five years.

Recommendation 21

386. A requirement to pay special attention to business relationships and transactions with persons from countries that do not or insufficiently apply the FATF Recommendations should be introduced. To supplement this, country specific guidance could be considered for all financial institutions about those countries (other than NCCT jurisdictions) which might have weaknesses requiring such special attention.

387. Financial institutions should be also required to examine the background and purpose of transactions connected with such countries if those transactions have no apparent economic or visible lawful purpose. Written findings should be available to assist competent authorities and auditors.

3.6.3 Compliance with Recommendations 11 and 21

	Rating	Summary of factors underlying rating
R.11	**Partially compliant**	Recommendation 11 is only indirectly covered by Polish law.
R.21	**Non compliant**	No obligation in law or regulation or other enforceable means to • pay close attention to any country that fails or insufficiently applies FATF recommendations. • examine the background and purpose of transactions connected with such countries if those transactions have no apparent economic or visible lawful purpose. • have written findings available to assist competent authorities and auditors.

3.7 Suspicious transaction reports and other reporting (Recommendations 13, 14, 19, 25 and SR.IV)

3.7.1 Description and analysis

Recommendation 13 and SR.IV

388. Essential Criteria 13.1, 13.2 and 13.3 are to be required by law or regulation.

389. As noted in Section 2.5, the AML/CFT Preventive System is rooted in Article 8 (1) and (3) AML Act, which provide for the overarching duty to "register" transactions, and persons executing transactions, and which includes duties of identification, etc. Article 12 covers the forwarding of registered transactions to GIFI. The above threshold (not suspicious) transactions under Article 8 (1) are forwarded 14 days following the end of every calendar month. By contrast, the Law requires Article 8 (3) registered transactions [which suggest that the property values involved in the transaction may originate from illegal or undisclosed sources regardless of value and nature – i.e. suspicious transactions] to be transmitted forthwith under Article 12, para. 2 (2), containing the data specified in Article 12, para. 1. The obliged institutions should also specify the factors which indicate the necessity to suspend the transaction. The STR reporting under the Act creates a direct mandatory obligation in the Law which satisfies both Criteria 13.1 and the no threshold aspect of 13.3. However, attempted transactions are not clearly covered in the Law, as required.

390. The obligation to make an STR immediately was explained by the Polish authorities to include suspicions that funds may be related to the financing of terrorist activities. This construction arguably derives from a close reading of the wording of the Act itself, which specifically covers Counteracting the Financing of Terrorism (see the title and Article 1) and other provisions including Article 16a (2) of the AML Act and Article 2 (7). Article 16a (2) covers the duty of immediate reporting of accounts which may be linked to acts of terrorism. The evaluators consider that Article 16a (2) can more readily be interpreted as relating to the duty to announce to GIFI accounts matched with lists received pursuant to SR.III under Article 16a AML Act rather than proactively identifying suspicious transactions related to financing of terrorism.

391. However, in the first English language version of the AML Act, there was a footnote 1, which indicated that "whenever separate provisions refer to the act or provisions on counteracting introduction into financial circulation of property values derived from illegal or undisclosed sources, it shall mean respectively the Act on provisions on counteracting introduction into financial circulation of property values derived from illegal or undisclosed sources (i.e. money laundering) and on counteracting the financing of terrorism". This footnote does not appear in the second (and better) English version of the AML Act which the examiners received. Assuming it remains in the Polish language version of the AML Act, the Article 8 (3) registerable suspicious transactions which have to be transmitted immediately appear legally to include suspicious reports relating to some aspects of the financing of terrorism. The FIU have in practice received numerous terrorist-related reports according to the statistics set out earlier in this report. However, Criterion 13.2 requires the making of reports where there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism (see also the language of SR.IV). The only real linkage in the AML Act (apart from the footnote) to financing of terrorism derives from Article 2 (7). Article 2 (7), on which the Article 8 (3) registration requirement is also based, refers only to acts of terrorism (i.e. offences) and not all the other aspects of Criterion 13.2 (linkage to terrorism generally, terrorist organisations or those who finance terrorism). Moreover, it is unclear whether the financing of terrorism reporting obligation is based on (subjective) suspicion alone or

reasonable suspicion alone or both in the alternative as this Criterion (and SR.IV) requires. Thus, at best, the Polish obligation in the AML Act to report suspicions of financing of terrorism does not clearly cover all aspects of Criterion 13.2 (and SR.IV). The third EC Directive 2005/60/EC will extend the preventative system to financing of terrorism, including the issue of transmitting potentially suspicious operations. The Polish authorities will doubtless upgrade their STR regime relating to financing of terrorism in the process of transposition.

392. Criterion 13.4 is covered in the Law. The AML Act is interpreted to cover tax offences by including of the language "assets derived from undisclosed sources".

Additional elements

393. The Polish authorities explained that Criterion 13.5 is covered by on a proper construction of Article 8 (3) and Articles 11 and 12.

European Union Directive

394. Paragraph 1 of Article 6 of the Directive 2001/308/EEC provides that the reporting obligation should cover facts which might be an indication of money laundering, whereas FATF Recommendation 13 places the reporting obligation on suspicion or reasonable suspicion that funds are the proceeds of criminal activity. It appears that as the polish reporting obligation is transaction based, it is insufficiently wide to cover all facts which might be an indication of money laundering.

395. Comments on Article 7 of the Second EU Anti-Money Laundering Directive (in respect of the requirement to refrain from carrying out transactions which financial institutions know or suspect relate to money laundering until they have apprised the competent authorities) have been discussed under Recommendation 5. It is considered that Articles 16-18 of the AML Act broadly cover this.

Safe Harbour Provisions (Recommendation 14)

396. The Polish authorities indicated that Articles 20 and 29 cover Criterion 14.1. Article 20 simply states that the State Treasury shall be liable for "damages" resulting from blocking the account or transaction suspension and not from the reporting itself. Article 9 equally does not fully cover this issue, as it simply states that regulations limiting access to confidential information shall not apply to disclosures under this Act. While the spirit of the Criterion is very broadly covered, it would be helpful if it is explicitly stated in the law that all financial institutions, directors, officers and employees should be protected from both criminal and civil liability for breach of any restriction or disclosures of information in good faith (in the comprehensive way it is addressed in Criterion 14.1).

Tipping off (Recommendation 14)

397. Article 34 of the AML Act states that it is prohibited to disclose to unauthorised persons, including the parties of the transaction or holders of the account, the fact of informing the General Inspector about transaction suspected of involving property values derived from illegal or undisclosed sources or about accounts of the entities towards which there exist a well-founded ground, that they are connected with the commission of terrorist acts and about transactions executes by these entities. This carries a significant deterrent criminal penalty of up to 3 years imprisonment, or a fine (if committed unintentionally). This provision is understood to be of general application and applies to both staff of obliged institutions and the FIU. However, the provision does not clearly cover the transmission of related information even though disclosure of the fact of reporting is clearly prohibited.

398. Additionally, the FIU staff are bound by confidentiality in respect of any "secrets" they receive while carrying out their activities. They remain bound by this confidentiality after their employment has ceased. Arguably this covers the requirement on the FIU in additional element 14.3 – keeping the names and addresses of staff of financial institutions confidential.

Recommendation 19

399. Recommendation 19 is fully met. The reporting of transactions above a fixed threshold is covered in the law and the additional elements (fully protected computerised database) are also fulfilled.

Recommendation 25 (feedback and guidance related to STRs)

400. According to the Act of November 16, there is no obligation for GIFI to provide the direct feedback to the reporting institutions at the stage of preparatory proceedings conducted by a prosecutor's office or during proceedings in court. GIFI provides the obligated institutions with the general feedback. Feedback information about actions taken by the GIFI as a result of a report, provided at such an early stage of proceedings would, under Polish laws, constitute an infringement of the basic rights of parties to proceedings (in particular – the principle of the presumption of the accused's innocence). Feedback about the results of reporting is possible only after the court renders judgement and the judgement becomes final in the particular case. However, in order to advise co-operating and obliged institutions about the usefulness of their reporting, the GIFI – during training courses – presents general feedback, which means exemplary cases selected with regard to the institution receiving training. The GIFI has also developed a special manual (guidebook) that is highly appreciated by the employees of obliged and co-operating institutions, who use the manual in their everyday activities.

401. The prudential supervisors also indicated that they can provide some guidance during on-site inspections.

3.7.2 Recommendations and comments

402. The suspicious transaction reporting regime is satisfactorily provided for in the legislation but more guidance is still needed to ensure that reporting entities place sufficient emphasis on the STR regime, as opposed to the above-threshold reporting regime. The most reports still come from the banks. It was not clear from the statistics provided to the team whether the spread of reporting across the banking sector was even. More attention should be given to outreach to other parts of the financial and non banking financial sector to ensure that they are reporting adequately.

403. Attempted transactions are not covered in the Law and the examiners are unaware of coverage of this issue in guidance. However, the evaluators were informed that attempted transactions were reported though no figures were provided. The examiners recommend that the AML Act should clearly provide for attempted suspicious transactions to be reported, in line with Essential Criteria 13.3 (marked with an asterisk).

404. The present reporting duty in respect of financing of terrorism can only be deduced by reference to several articles in the AML Act, and then the real width of the reporting obligation is unclear. Although in practice reports are being received, more guidance is required on the width of the financing of terrorism reporting obligation. It appears solely linked to acts of terrorism (however that is interpreted) and it is unclear whether reporting institutions are expected to make subjective or objective assessments (or both) of whether a transaction is linked to financing of terrorism in all its aspects as described in Criterion 13.2 and SR.IV.

405. The reporting duty needs to be explicitly clarified in the law to include all funds where there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism. There have been no reports relating to the financing of terrorism, and no guidance issued.

406. The examiners consider that it would be helpful if it is explicitly stated in the law that all financial institutions, directors, officers and employees should be protected from both criminal and civil liability for breach of any restriction on *bona fide* disclosures of information (in the comprehensive way the issue is addressed in Criterion 14.1).

407. Though not part of the 2004 Methodology, the examiners are of the view that Poland should make the requirements of Article 6 of the Second European Union Anti-Money Laundering Directive explicit in legislation or guidance.

408. The tipping off provision should clearly cover the transmission of related information, as well as the fact of reporting.

409. On feedback and guidance it is quite clear that GIFI has put in a large amount of work into training and guidance. Feedback is given in training and in the manual in the form of typologies. The Polish authorities may wish to consider whether some system of case specific feedback could be devised (perhaps computer generated simply advising on the basic stages of the process – e.g. passed to prosecution, awaiting trial, etc.) which would not infringe Polish legal principles.

3.7.3 Compliance with Recommendations 13, 14, 19, 25 and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13	**Partially compliant**	There is a direct mandatory reporting requirement in the AML Act, though • attempted transactions not covered; • financing of terrorism only partially covered, though reports had been received; • low number of reports outside the banking sector raises issues of effectiveness of implementation.
R.14	**Largely compliant**	• It should be clarified that all civil and criminal liability is comprehensively covered; • The tipping off provision should cover related information.
R.19	**Compliant**	
R.25	**Largely compliant**	Consideration could be given to some case specific feedback.
SR.IV	**Partially compliant**	Reporting obligation in respect of financing of terrorism insufficiently wide.

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 and 22)

3.8.1 Description and analysis

Recommendation 15

410. Recommendation 15, requiring financial institutions to develop programmes against money laundering and financing of terrorism, can be provided for by law, regulation or other enforceable means.

411. According to Article 28 of the AML Act the obligated institutions shall devise internal procedures for preventing the introduction into financial circulation of property values derived from illegal or undisclosed sources or the financing of terrorism, in particular relating to the fulfilling of the requirement of a client's identification and keeping of information gathered as part of the identification process, shall provide personnel with training in identifying transactions potentially linked to the offence referred to in Article 299 of the Penal Code, and shall name the individuals responsible for fulfilling the obligations resulting from this Act. In case of obligated institutions, being limited companies or joint-stock companies, the responsible person is a Managing Board member appointed by the Managing Board.

412. There is no requirement in the legislation or regulation concerning timely access of the AML/CFT compliance officer and other appropriate staff to customer identification data and other CDD information, transaction records, and other relevant information.

413. There is no general legal requirement for financial institutions to maintain an adequately resourced and independent audit function to test compliance with AML/CFT procedures, policies and controls (criterion 15.2). However, the banking and securities sector are obliged to have an internal audit function, which also covers AML/CFT policies (Article 9 to 9d of the Banking Act, § 12 of the Regulation of the Minister of Finance on technical and organisational conditions required of investment firms and custodian banks); compliance is checked by the supervisors. For the insurance sector there is only the requirement to set up an internal control system but without specifications mentioned before.

Screening of Employees

414. There are no general formal obligations imposed on financial institutions regarding screening procedures to ensure high standards when hiring employees (criterion 15.4). In practice there are procedures for screening the board of directors; however, employers are not given access to any information about potential employees from an official source, such as criminal records. The banks informed that they are actually forbidden under Labour and Data Protection rules to ask for such information from a potential employee. Some banks seem to find ways to circumvent these rules by making clear that they expect voluntary presentation of such documents when hiring new staff, but they see this as a risk, because this might make them liable for an illegal act.

415. The Polish authorities informed the evaluators after the onsite visit about the Regulation of Minister of Labour and Social Policy from 28th of May 1996 on the scope of conducting by employers documentation concerning employment and manner of conducting personal dossier of employee *(O.J. No 62, item 286 with amendments)*. According to this Regulation, employers can demand from potential employees the following information:

- personal questionnaire,

- dossier of former employment,
- certificates concerning appropriate knowledge for current position,
- opinion from doctor concerning lack of adverse factors which may affect working in a position,
- other documents, if there is obligation on the basis of another regulation, e.g. criminal records, civil servant has to provide statement of his property condition.

Additional elements

416. In case of obligated institutions, being limited companies or joint-stock companies, the person responsible for fulfilling the obligations resulting from the AML Act has to be a managing board member (Article 28 of the AML Act). Concerning the operational level, the banking supervisor advised that they found during their inspections, that the so-called coordinator for the AML-programme in the majority of banks enjoys large independence and regularly submits the information on the programme implementation to the bank's board.

Recommendation 22

417. The Polish financial sector is currently largely owned by foreign entities, mostly from other EU countries, with most of its large banks being held by shareholders from the EU. This seems to be an element of strength in the AML/CFT regime, as group-wide standards are also applied in Poland, and many international financial entities provide support for the local ML prevention in their entity, through lists and typologies, and also conduct onsite internal audits.

418. There is only one bank which has a subsidiary abroad (a banking entity in Ukraine). It was mentioned to the evaluators that there was a joint onsite inspection conducted there, covering AML/CFT, by the Polish and the Ukrainian Banking Supervisors.

419. There is no mention in the AML Act, or other Law, Regulation or requirement by other enforceable means providing for the application of the AML/CFT standard obliging the entity in Poland to ensure its branches or subsidiaries abroad observe AML/CFT standards consistent with home country requirements. However, the Polish authorities advised that foreign branches are subject to the AML Act because they are parts of obliged (domestic) entities.

3.8.2 Recommendation and comments

Recommendation 15

420. Poland is in line with most subcriteria of Recommendation 15 including establishing and maintaining internal procedures, designating an AML/CFT compliance officer at the management level (in the case of limited liability companies and joint-stock companies) and employee training. Entities within the banking and securities sectors are also required to maintain an independent audit. However there are some areas which should be addressed, as described below.

421. The AML/CFT compliance officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

422. Only the banking and securities sectors are obliged to have an internal audit function, which also covers AML/CFT policies. The same should be introduced for the rest of the financial sector.

423. An obligation should be introduced to require financial institutions to establish screening procedures to ensure high standards when hiring employees.

Recommendation 22

424. Though, at present, the risks in this area appear low, as the Polish financial market expands, it is likely that the requirement of FATF Recommendation 22 will need more attention in the financial sector generally. Accordingly, Poland should implement an explicit obligation to require financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with the Polish requirements and FATF recommendations. It should add provisions to clarify that particular attention has to be paid to branches and subsidiaries in countries which do not or insufficiently apply the FATF recommendations and that the higher standard have to be applied in the event that the AML/CFT requirements of the home and host country differ.

3.8.3 Compliance with Recommendations 15 and 22

	Rating	Summary of factors underlying rating
R.15	**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 sector) are obliged to have an 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.
R.22	**Non compliant**	• There is no explicit obligation for foreign branches and no obligation for subsidiaries to observe AML/CFT measures consistent with Polish requirements and the FATF recommendations to the extent that host country's laws and regulations permit. • There is no requirement that particular attention has to be paid to branches and subsidiaries in countries which do not or insufficiently apply FATF recommendations and that the higher standard has to be applied in the event that the AML/CFT requirements of the home and host countries differ.

3.9 Shell banks (Recommendation 18)

3.9.1 Description and analysis

Criterion 18.1

425. Criterion 18.1 requires countries not to approve the establishment or accept the continued operation of shell banks. According to the Banking Act, the establishment of a bank is subject to licensing by the Commission for Banking Supervision (BSC). Article 30 of the Banking Act provides for the establishment of a bank the following conditions:

1) it is ensured that the bank will be provided with:
a) a capital base commensurate to the kinds of banking activity anticipated and the scale of operations intended,
b) premises equipped with suitable facilities for the proper safekeeping of funds and valuables, taking into consideration the scope and kinds of banking activity to be conducted,

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 possess the education and professional experience necessary to direct a bank, as well as a proven knowledge of the Polish language,
3) (repealed).
4) the founders submit a plan of the bank's operations for at least the immediate three years which indicates that these operations will not endanger the funds held in the bank's custody.

Thus, it can be said that the establishment of shell banks is not allowed in the Polish legal framework.

Criteria 18.2 and 18.3

426. There is no specific provision with regard to a prohibition on financial institutions to enter or continue correspondent banking relationships with shell banks. A specific obligation on financial institutions to satisfy themselves that a respondent financial institution in a foreign country is not permitting its accounts to be used by shell banks is also missing. However there seems to be correct handling of this at the practical level and the inspections have not discovered any evidence of the cooperation of any banks with a shell bank.

3.9.2 Recommendations and comments

427. Poland should implement provisions with regard to a prohibition on financial institutions to enter or continue correspondent banking relationship with shell banks. In addition, there should be an obligation on financial institutions to satisfy themselves that a respondent financial institution in a foreign country is not permitting its accounts to be used by shell banks.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	**Partially compliant**	There is no legally binding prohibition on financial institutions to enter or continue correspondent banking relationships with shell banks nor is there any obligation on financial institutions to satisfy themselves that a respondent financial institution in a foreign country is not permitting its accounts to be used by shell banks.

Regulation, supervision, monitoring and sanctions

3.10 The supervisory and oversight system - competent authorities and SROs / Role, functions, duties and powers (including sanctions) (R.17, 23, 29 and 30)

3.10.1 Description and analysis

Authorities' roles and duties, structure and resources – Recommendations 23 / 30

Recommendation 23 (Criteria 23.1 and 23.2)

428. Criterion 23.1 requires that countries should ensure that financial institutions are subject to adequate AML/CFT regulation and supervision and are effectively implementing the FATF standards. Criterion 23.2 requires countries to ensure that a designated competent authority (or authorities) has responsibility for ensuring AML/CFT compliance.

429. No sector specific regulation has been issued by financial supervisors. The PSEC is not empowered to do so.

430. The GIFI is responsible for controlling whether obligated institutions, excluding the National Bank of Poland, fulfil the duties referred to the AML/CFT area (Article 21 para. 1 of the AML Act).

431. According to the AML Act (Article 21 para. 3) such AML/CFT controls are also carried out by institutions performing supervision over the obligated institutions pursuant to separate regulations. The aforementioned institutions include the following subjects:
   (1) the Banking Supervision Commission with regard to banks and branches of foreign banks, and the National Bank of Poland with regard to residents engaged in foreign currency exchange operations;
   (2) the Insurance and Pension Funds Supervisory Commission with regard to insurance companies and main branches of foreign insurance companies;
   (3) the Securities and Exchange Commission with regard to investment companies and custodian banks as well as with regard to investment funds and the Joint Stock Company National Depository for Securities S.A.
   (4) the minister competent for matters of public finance with regard to entities arranging and operating games of chance, mutual bets or slot machines,
   (5) Presidents of Appeal Courts with regard to notaries public,
   (6) National Association of Co-operative Savings and Credit Unions with regard to co-operative savings and credit unions.

432. The chart beneath shows the supervisory and licensing authorities for all financial institutions.

Financial institution	Supervisory authority	Licensing authority
Banks	GIFI[1]; BSC[2]	BSC
Credit unions	National Association of Credit and Savings Unions	No licensing authority
Insurance companies (including life)	GIFI; Insurance and Pension Funds Supervisory Commission	Insurance and Pension Funds Supervisory Commission
Pension Funds	GIFI, Insurance and Pension Funds Supervisory Commission	Insurance and Pension Funds Supervisory Commission
Companies issuing credit cards	N/A[3]	N/A[3]
Foreign Exchange Offices	GIFI; NBP	NBP
Money remitters / funds Transfer firms	-	No licensing authority
Investment companies (including stock brokers)	GIFI, Securities and Exchanges Commission	Securities and Exchanges Commission
Investment funds companies	GIFI, Securities and Exchanges Commission	Securities and Exchanges Commission
Custodian banks	GIFI, BSC, Securities and Exchanges Commission	BSC, Securities and Exchanges Commission
Investment funds	GIFI, Securities and Exchanges Commission	Securities and Exchanges Commission
Joint Stock Company National Depository for Securities S.A	Securities and Exchanges Commission	N/A[4]
Electronic money institution (if non banks)	GIFI; BSC	only notification to the NBP required[5]-

Explanatory note:
1) Except the National Bank of Poland
2) Also for branches of foreign banks
3) Credit cards companies are always in co-operation with banks.
4) established by law
5) In case of a joint stock company a permission of the BSC is required

Recommendation 30 (Structure and resources of the supervisory authorities)

433. According to the Act on the National Bank of Poland (Annex 18), bank examiners should be persons of appropriate education and professional experience. In particular, those eligible for the post of bank examiner shall be persons who:
1) hold solely Polish citizenship and enjoy full civic and public rights,
2) give adequate guarantee of the proper performance of their duties,
3) have impeccable references and have not been convicted of a wilful criminal offence,
4) hold a degree in law or economics, or a degree in another subject useful in the performance of banking supervision,
5) have at least 3 years work experience in banking,
6) have taken a qualifying examination for the post of bank examiner, held by an examinations committee appointed by the Commission. (Article 30 para. 1)

434. The BSC is staffed with 240 inspectors, 21 of which are specialised in the AML/CFT area. The National Association of Credit Unions is staffed with 12 inspectors, 7 of which conduct inspections in the AML/CFT area. The Polish authorities informed that the staff of the following supervisory authorities was on 18 September 2006 as follows and rather similar at the time of the

onsite visit: the Insurance and Pension Funds Supervisory Commission is staffed with 215 employees and 30 employees (specialists) responsible also for controlling insurance undertakings within the scope of anti-money laundering during their controls. Simultaneously, there are 4 coordinators specialised in the AML/CFT area, i.e. in accordance with the Insurance Activity Act. The PSEC is staffed with 177 employees including 15 inspectors who conduct onsite visits and are trained for checking compliance with the AML Act.

Authorities´ Powers and Sanctions – R.29 and 17

Recommendation 29 (supervisors' powers)

435. Criterion 29.1 requires that supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and financing of terrorism. According to Article 22 of the AML Act on demand by an inspector, obligated institutions shall make available all documents and materials needed to carry out the control with the exception of documents and materials containing State secrets. Obligated institutions shall provide inspectors with working conditions needed to carry out the control effectively. In particular, they shall present the documents and materials requested for inspection forthwith and shall ensure timely explanations by their personnel. Pursuant to Article 21 (1) and (3) of the AML Act the FIU and the prudential supervisors all have the power to control for money laundering and financing of terrorism.

436. Pursuant to Article 22 para. 3 of the AML Act, inspectors shall have the right to:

(1) enter the premises of the obligated institution in the company of the controlled party;
(2) examine documents and other evidence material relevant to the scope of the performed control and to receive confirmed copies thereof;
(3) demand oral and written explanations from personnel of the obligated institutions relevant to the scope of the performed control.

437. In connection with the performance of control activities, inspectors shall be under protection provided by the Penal Code for public officers. In addition, Inspectors shall have the right to move about freely in the premises of the obligated institution without the need to obtain a pass, and they shall not be subject to personal control (see Article 23 of the AML Act).

Banks

438. The activity of banks, branches and representative offices of foreign banks, as well as of branches and representative offices of credit institutions are subject to supervision exercised by the Commission for Banking Supervision, the scope and principles of such supervision being set out in the Banking Act and the Act on the National Bank of Poland (see Article 131 of the Banking Act).

439. According to Article 138, para. 3, of the Banking Act where the bank's activity is in contravention of the law or its articles, or is endangering the interests of accountholders, the BSC may, after first cautioning the bank in writing:

1) apply to the appropriate directing body of the bank for the recall of the president, vice president or other member of the management board directly responsible for the irregularities noted,
2) suspend from office the members of the management board referred to in subpara. 1 above pending the adoption of a resolution on the application for their recall at the next meeting of

the supervisory board; suspension from office shall involve such persons being excluded from participation in decisions of the bank in respect of its financial rights and obligations,
3) restrict the scope of the bank's activity,
3a) impose on the bank a financial penalty of up to 1,000,000 Złoty;
4) revoke authorisation to establish the bank and order the bank's liquidation.

440. In addition, if the bank does not implement the recommendations concerning the activities violating the law or the statute, refuses to provide explanations or information, the BSC may impose financial penalties on the members of the board and the value of those penalties may amount to the triple gross monthly salary of a given person calculated on the basis of the salary for the last three months before the penalty was imposed. The penalty cannot be imposed if the banking supervision received the information about such an act more than six months ago or the act was committed more than two years ago. The financial penalty does not exclude the use of other measures provided for in the Banking law.

441. According to Article 138 para. 5 of the Banking Act the BSC shall recall a member of the management board in the event of that person's final and conclusive conviction of a wilful criminal offences or fiscal offences, excluding offences that are prosecuted upon private accusation. The BSC may also suspend from office a member of the management board where that person has been charged with a criminal offence or with a fiscal offence (Article 138 par. 4 of the Banking Act).

Insurance companies and pension funds

442. According to the Act on Insurance and Pension Supervision, insurance companies and pension funds are supervised by the Insurance and Pension Funds Supervisory Commission (hereinafter referred to as "Insurance Commission"). Pursuant to Article 8 of this Act the duties of the Insurance Commission shall be:
1) to undertake, in cases foreseen by other acts, actions aimed to maintain the conformity of supervised units' actions with stipulations of law;
2) to inspect the activities and the financial standing of supervised subjects;
3) to undertake other statutory duties provided for.

443. The Insurance Commission is empowered to impose penalties on pension companies, insurance undertakings or members of their statutory authorities, and suspend members of the board, to make the motions for dismissal of a member of the board or to withdraw issued proxy or to make a motion to the effect of call of the general meeting, supervisory board or management board (Article 12 of the Act).

Securities Market

444. The Polish Securities and Exchange Commission (PSEC) is allowed to conduct inspections in capital market supervised entities, pursuant to Article 26 of the Act on capital market supervision (Annex 19). In the course of inspection, a statement (in the form of questions) on "money laundering" is taken.

Money exchange services

445. According to Chapter 9 of the Foreign Exchange Law control is exercised by the NBP.

Recommendation 17 (sanctions)

446. The sanction regime in the AML Act is a criminal sanction regime.

447. Chapter 8 of the AML Act contains penal provisions and describes sanctions. According to Article 35, para. 1, of the Act, any person acting in the name or in the interest of an obligated institution who in violation of this Act, fails to:

(1) register transactions or keep the transaction registers and the documents relating to the transaction;

(2) identify the client in keeping with the procedures referred to in Article 28 herein or keep the identification information;

(3) notify the financial information authority about the transaction or about keeping the account on behalf of the entity, referred to in Article 16a Paragraph 1;

(4) suspend a transaction or block the account,

shall be liable to a penalty of deprivation of liberty for a period of up to three years.

Article 35.2. of the Act stipulates that the "*same penalty shall be imposed on any person acting in the name or in the interest of an obligated institution who, in violation of this Act, should disclose any information obtained pursuant to this Act to unauthorised persons, holders of the account or persons involved in a transaction, or should otherwise use this information in violation of this Act.*" Should the offence referred to in Article 35.1 or. 35.2. be committed unintentionally, its perpetrator shall be liable to a fine (para. 3). Article 36 of the Act determines that any person acting in the name or in the interest of an obligated institution who, in violation of this Act, shall:

(1) refuse to provide the General Inspector with information or documents;

(2) provide the General Inspector with untrue data or withhold true data relating to transactions, accounts or persons;

shall be liable to a penalty of deprivation of liberty for a period of three months to five years.

Article 37 of the Act describes that persons committing acts referred to in Article 35 para. 1 or 2, or in Article 36 of the Act which shall lead to considerable damages shall be liable to a penalty of deprivation of liberty for a period of six months to eight years.

Article 37a.1 of the Act describes that any person, who foils or obstructs the performing of inspection activities, referred to in Chapter 6 of the Act, shall be liable to a fine. Article 37a.2 of the Act describes that any person, who does not accomplish the obligation to devise internal procedures for preventing the introduction into financial circulation of property values derived from illegal or undisclosed sources shall be liable to the same penalty. It is noted earlier that there may be some potential overlap with Article 299 (2) Penal Code in the sanctioning regime. Article 299 (2) is slightly broader (and with even severer penalties). It was unclear whether Article 299 (2) was considered in the range of possible sanctions (as well as A.35 AML Act, though statistics on Article 35 offences were not provided. The statistics provided earlier show Article 299 (2) has been used, though the particular circumstances of the cases in which it was applied were not explained. It is assumed it is used for the most egregious cases by employees of obliged entities. In any event all these criminal (sanctions) cases would be referred (either by GIFI or otherwise) to the Prosecution Service for consideration of criminal proceedings, as they can only be imposed by the Court (including the (unintentional) offences which are only liable to fines ("the GIFI fines").

448. A certain degree of confusion seems to exist between the penalties under the AML Act and the penalties in the Penal Code, which use very similar wording and also address the same circle of persons. During the discussions with the authorities, it could not be satisfactorily clarified in which case, which responsible authority would apply which sanction.

449. Although it seems that the sanction regime in the AML Act is applied in practice (see the statistics under Section 2.1), the effectiveness of this system is, at least, questionable. The confusion of roles might cause cases to be shifted back and forth between authorities, as the competences are unclear. Furthermore, the comparatively severe penalties seem, for minor cases, disproportionate and might lead to sanctions not being applied at all. As the range of possible breaches of AML/CFT requirements is very broad, it might be possible that the Polish sanction provisions for non-compliance could be perceived as too harsh. Thus, a high sanction for not

hitting the mark exactly right makes an authority vulnerable to appeals and can lead to reluctance to sanction at all. Finally, a range of sanctions, which includes light sanctions are very useful. This is especially the case when a new sector or a new obligation makes it necessary to develop obliged entities compliance, as it gives the authorities a wider range of action.

450. The general supervisory sanction framework is in line with international standards, however, except for the case already mentioned in prior Mutual Evaluations of Poland of closing a bank due to money laundering and two warning letters of the Banking Supervision Commission and one fine from the Insurance and Pension Funds Supervisory, no case of supervisory action against a supervised entity related to AML/CFT was made. However the Banking Supervision Commission issues recommendations for improvement of the AML/CFT area after each on-site inspection. During the pre-meeting, the Polish authorities informed that the PSEC revoked a brokerage licence (a breach of AML obligations was *inter alia* one of the reasons for this decision).

3.10.2 Recommendations and comments

Recommendation 17

451. There might be a place in the system for an additional regime of complementary administrative sanctions such as fines to enhance the AML/CFT compliance, particularly in the non financial sector.

452. The number of sanctions imposed by the PSEC and the Insurance and Pension Funds Supervision Commission is not satisfactory and does not seem appropriate. Administrative sanctions should be used more often by the financial supervisors in practice when obligated institutions fail to comply with AML/CFT requirements.

Recommendation 23 (23.1 and 23.2)

453. The legal approach of assigning to the GIFI a central supervisory role and involving also the prudential supervisors ensures a full coverage of all obliged entities by a supervisor, and, legally, a responsibility for sanctioning is in place for all obliged entities as well.

454. However, in practice, the engagement of the prudential supervisors, mainly of the PSEC, in AML/CFT supervision seems overly formal and very narrow, as they only see their role in inspecting on site based on a formalistic list of criteria. GIFI itself does not have the resources of personnel to effectively supervise the whole financial sector. Therefore, an important gap remains. A more detailed manual for onsite inspections in the AML/CFT area exists only for the banking supervisors and this manual is also available to the banking sector.

455. An involvement by the prudential supervisors in training, and their closer engagement where guidelines and regulations are necessary, would also strengthen the supervision of obliged entities which also have a prudential supervisor. Currently, prudential supervisors clearly and explicitly reject any involvement in this area. Sector specific regulation should be issued by financial supervisors and the PSEC should also be empowered to do so.

Recommendation 29

456. Again, the legal system foresees an involvement of the GIFI and would allow GIFI to be adequately active. The powers of going onsite in inspections and all rights connected therewith are also in existence. The prudential supervisors themselves also have all the relevant powers necessary.

457. However, as explained above under Rec. 23, the practical application of the legal regime is not sufficiently strong, due to the twin problems of GIFI not having enough resources and expertise to adequately supervise and inspect the financial sector, while the prudential supervisors are not sufficiently engaged to cover these issues from their side in a comprehensive manner.

458. Financial supervisors, particularly the PSEC, shall apply all necessary on-site tools (review of policies, procedures, books and records including sample testing) also in the AML/CFT area.

Recommendation 30

459. More AML/CFT experts are needed within the financial supervisory framework, particularly in PSEC to be able to cover the complex issue of AML/CFT (supervision, regulation and guidance). Experts should be trained also in the CFT area as this part is not covered at all by on-site inspections of Insurance Commission and PSEC.

Recommendation 32

460. The statistics related to the financial sector seem overall to be adequate so as to allow a clear understanding of the activities in the field of AML/CFT. There was no formal request for assistance made or received by supervisors relating to or including AML/CFT, thus no such statistics is maintained by Polish authorities on this issue.

3.10.3 Compliance with Recommendations 17, 23, and 29

	Rating	Summary of factors underlying rating
R.17	**Partially compliant**	• Few sanctions have been imposed which questions the effectiveness of the sanctioning system. • The sanction regime is disproportionate for minor cases which carries the risk that it is not applied and reduces its effectiveness. • Not all supervisory authorities are aware of their reporting obligations concerning violations of the AML Act by the obliged entities to the Prosecution authorities.
R.23 (23.1 and 23.2)	**Partially compliant**	• No sector specific regulation has been issued by financial supervisors; the PSEC is not even empowered to do so. • Due to the very reduced involvement of some supervisors (only onsite visits based on a list of formalistic criteria which do not cover adequately the full range of issues related to AML/CFT, such as internal risk management systems and analysis of suspicious patterns, monitoring, etc.) and their explicit unwillingness to be involved in training and regulation/guidelines, the system is not fully operational and satisfactory in practice.
R.29	**Largely compliant**	Complex AML/CFT on-site inspections including the review of policies, procedures and sample testing are missing, particularly in the securities sector.

3.11 Financial institutions - market entry and ownership/control (R.23)

3.11.1 Description and analysis

Recommendation 23 (criteria 23.3, 23.5, 23.7)

Banks

461. Regarding ownership of banks, when entering into the market, banks are required to obtain authorisation (licence) from the Banking Supervision Commission.

462. The bank, in the form of a joint stock company, may be established by legal and natural persons but their number cannot be less than three. This requirement does not apply to the bank established by the State Treasury, a domestic bank, a credit institution, a foreign bank, a domestic or foreign insurance undertaking or an international financial institution. Under the requirements of Art 30 para. 1 of the Banking Act, a bank may be established if:

(1) the bank is provided with:

(a) own funds the amount of which should be adjusted to the type of banking activities the bank is to carry out and to the scope of intended activities;

(b) premises equipped with appropriate technical devices which appropriately secure the assets kept at the bank taking into account the scope and type of conducted banking activities;

(2) founders and persons who are to be appointed as the members of the board, including the president, provide a warranty that the bank will be managed in a careful and stable way; at least two of the persons who are to be appointed as the members of the board have the appropriate education and professional experience required to manage the bank and a proven knowledge of Polish;

(3) the plan of the bank's activities for a period of at least three years presented by the founders indicates that the activities will be secure for cash kept at the bank.

463. A part of the initial capital may be provided in the form of non-monetary assets such as equipment or real estate if they will be directly useful for carrying out the banking activities, but the initial capital in cash cannot be lower than the PLN equivalent of EUR 5 million and the value of non-monetary contribution cannot exceed 15% of the initial capital. The bank's initial capital cannot come from a loan or from non-documented sources (Art 30 para. 3 of the Banking Act).

464. Article 25 of the Banking Act provides that the BSC´s permission must be obtained before acquisition of qualifying participation (over 10%, 20%, 25%, 33%, 50%, 66% or 75% of votes [threshold levels] at a general meeting in banks).

465. Pursuant to Article 22b of the Banking Act the appointment of two members of the management board, including the president, shall require the approval of the BSC. The application for such approval shall be submitted by the supervisory board. The BSC shall refuse approval for the appointment of these persons where they:

1) have been convicted of wilful criminal offences or fiscal offences, excluding offences that are prosecuted upon private accusation,

2) were responsible for documented financial losses at their places of employment or in connection with their functions as members of bodies of juridical persons,

3) have been prohibited from engaging in business activity on their own behalf or from fulfilling the functions of representatives or attorneys of a business, members of supervisory

boards or audit committees in a public limited company, private limited company or cooperative,

4) do not fulfil the requirements stipulated in Art. 30, para. 1, sub-para. 2, subject to the provisions of para. 4 (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 possess the education and professional experience necessary to direct a bank, as well as a proven knowledge of the Polish language).

466. According to Article 138 para. 5 of the Banking Act, the BSC shall recall a member of the management board in the event of that person's final and conclusive conviction of a wilful criminal offences or fiscal offences, excluding offences that are prosecuted upon private accusation. The BSC may also suspend from office a member of the management board where that person has been charged with a criminal offence or with a fiscal offence (Article 138 para. 4 of the Banking Act).

Insurance companies

467. The Insurance Commission is empowered to grant licences to insurance companies. According to Article 98 of the Act on Insurance Activity (Annex 20), the licence cannot be delivered if the

- management body or the supervisory body of the domestic insurance undertaking concerned includes persons, who do not meet the requirements specified in this Act;
- founders of the domestic insurance undertaking have been convicted for a wilful offence ascertained by a valid court sentence;
- founders make use of material assets deriving from illegal or undisclosed sources;
- pursuit of activity by that insurance undertaking constitutes a threat to the defence, state security or public order and security.

Securities firms

468. To conduct brokerage activity a licence from the Polish Securities and Exchange Commission (PSEC) is required. The provisions and the extent of the permit can be found for investment firms in Art. 69 and for custodian banks in Article 119 of the Act on trading in financial instruments (Annex 17).

Money transfer services

469. Neither a licence or a registration is required for entities providing money transfer services. At present, Western Union and Moneygram are active in Poland. The authorities have informed the evaluators that these companies act exclusively through banks as their agents. However, private sector representatives confirmed that bureaux de change are also contracting with Western Union. Although the aforementioned subjects are required to be either licensed or registered, the authorities were not able to exclude the possibility of the existence of subjects (not being a bank or a bureau de change) operating as money transfer service. Therefore, there appears to be a gap related to this element. As the Polish AML Act is careful to include even such entities which do not yet exist in Poland, such as electronic money institutions, and has a very complete and high coverage of entities which even goes beyond international requirements (e.g.; foundations), with the stated intention of ensuring very comprehensive coverage, the fact that money transfer services are not mentioned in the AML Act has to be seen as a serious gap, especially when the international typologies confirm that this is a high risk sector for AML/CFT.

470. Money transfer services are also provided by the Polish Post which is an obliged institution according to the AML Act.

Money exchange services

471. In 2004, the rules governing the granting of licences to conduct currency exchange activities were changed. The provisions of the Act on the freedom of economic activity (Annex 5) and the regulations implementing the Act on the freedom of economic activity (Dz. U. No 173, item 1807 and 1808), which became effective on 21 August 2004, repealed the licensing of those activities by the NBP and stated that such activities may be undertaken and conducted on condition that the entrepreneur will be entered into the Register of bureaux de change and will fulfil detailed requirements concerning the performance of those activities which are laid down in the foreign exchange law. The President of the National Bank of Poland was designated as the authority obliged to run the Register. It was reiterated that only persons not convicted of fiscal crimes against property or other crimes committed in order to achieve financial benefits are allowed to conduct foreign currency exchange activities and that they are obliged to document such status after each year of their activities. The competences of the NBP still include the inspection of the fulfilment of requirements laid down in the Foreign Exchange Law and specific regulations issued on its basis by the persons who conduct foreign currency exchange activities. If the foreign currency exchange activities which are carried out do not comply with the requirements specified in foreign exchange regulations, it may be a basis for a decision prohibiting those activities.

Co-operative Savings and Credit Unions

472. Co-operative Savings and Credit Unions are registered by the National Court, but there are no licencing procedures as recognized by the Basel Core Principles (criterion 23.4). The only element is included in Article 10 para. 1 of the Act on Co-operative Savings and Credit Unions (Annex 21), according to which membership of supervisory and management board may not include persons validly sentenced for intentional offences against property or documents, or for fiscal offence.

Electronic payment instruments

473. Article 15 of the Act on electronic payment instruments (Annex 22), obliges entities, apart from banks, to notify the NBP about the intention to begin activity consisting of issuing payment cards, at least one month prior to its beginning. According to Article 36 of this Act, an electronic money institution may be established in form of a joint stock company and carry out the activity to issue electronic money, on the basis of a permission by the BSC.

3.11.2 Recommendations and comments

474. A licensing or registering system should be introduced for MVT services as well as an effective system for monitoring and ensuring compliance with the AML/CFT requirements.

475. A licensing system as it is understood by the Basel Core Principles should be introduced for Cooperative Savings and Credit Unions.

3.11.3 Compliance with Recommendation 23 (Criteria 23.3, 23.5, 23.7)

	Rating	Summary of factors underlying rating
R.23	**Partially compliant**	• Natural and legal persons providing a money or value transfer service are not licensed or registered; apart from banks and the Polish Post, they are not subject to an effective system for monitoring and ensuring compliance with AML/CFT requirements. • The current registration system for Cooperative Savings and Credit Unions is not in line with the Basel Core Principles licensing requirements.

3.12 AML / CFT Guidelines (R.25)

3.12.1 Description and analysis

476. GIFI has made training a top priority. It has organised many training courses for various types of institutions designed to enhance their ability to spot suspicious transactions and to adopt internal policies, procedures and inspections that would deter money launderers. GIFI has drawn up and circulated warning signs and money laundering indicators appropriate for each sector. The work of GIFI in this field is exemplary, it shows a high degree of creative effort and dedication to outreach and good communication at various levels (book, internet, face to face training) which can serve as a model to other countries. It is very impressive and has also included a very intense effort of outreach to the newly obliged entities, which have special difficulties in all countries due to their small size, the fact that they have less regulation and the inherent diversity of their exposure to AML risks and their mostly very modest capability of risk management.

477. GIFI has developed a set of rules and methods which should be followed by the obligated institutions while reporting to the FIU transactions worth in excess of EUR 15,000, and suspicious transactions.

478. During trainings organised by GIFI, obligated institutions often reported the need to publish a study offering practical assistance in implementation of the tasks imposed on them (also related to the procedures of transmitting data to the General Inspector). In order to meet these demands an innovative publication entitled "Counteracting money laundering" was prepared by a team of the GIFI in 2004, addressed to entities obliged to implement tasks foreseen by the act. The GIFI distributed 10,000 copies of this guide among the obliged institutions and cooperating units. The guide presents a transparent typology of suspicious transactions, describes the methods of transaction identification, discusses the duties of the obliged institutions and cooperating units, contains practical guidelines and explains the rules of submitting the data from the register to the GIFI. Specific guidelines and examples of proper preparation for fighting the phenomenon of money laundering also have been given. In order to increase awareness and improve the qualifications of the staff from the obligated institutions, in 2005 the Polish FIU prepared and published a second edition of this handbook. In addition, an Internet site was launched containing replies to queries sent in by the obligated institutions regarding the interpretation of the provisions of the aforementioned Act. The Polish FIU publishes replies to questions sent in by the obligated institutions on the web-site of the GIFI. Some of the most frequently asked questions concern the understanding of the provisions of the Regulation of the Minster of Finance of 21 September 2001, on establishing the form of a register of transaction, the way of keeping the register and the procedure of conveying the registry data to the General Inspector of Financial Information

(Annex 11). Particularly numerous questions regard the rules of submitting information to the GIFI. The Internet site of the GIFI also contains information regarding the Polish FIU, legal acts establishing Poland's system aimed at preventing money laundering, as well as communiqués issued by the GIFI. Based on the observation of the ways of transferring information to the General Inspector, typical (and also technical) elements are identified that should be taken into particular consideration by obligated institutions, while registering transactions above the threshold (15,000 Euro). They are called technical requirements and are published on the GIFI's internet site.

479. In addition, the obligated institutions also used to receive during training courses an explanation of the rules and procedures to be followed by them when reporting information about transactions to the General Inspector.

480. In 2004, the training organised by the General Inspector was mainly dedicated to the presentation of the method of transferring information from the transactions registers by means of electronic information carriers. During 3 workshops under the umbrella of the EU PHARE (Poland and Hungary: Assistance for Restructuring their Economies) 2002 programme, 152 representatives of all Polish banks were trained and during another 2 training sessions, 102 representatives of the remaining obliged institutions (insurance companies, brokerage houses, Polish Post), the investment funds societies and investment funds, entities engaged in currency exchange and pawnshops, real estate agents, antique shops and entities engaged in the scope of precious and semi-precious metals or stones trade, enterprises conducting leasing and factoring activities, entities conducting activity involving games of chance, mutual betting and automatic machine games and public notaries) received training.

481. A comparison made between the number of irregularities related to the submission of information to the General Inspector before launching the Internet site and training, and the number of mistakes discovered in reports transferred to the GIFI, hereafter demonstrated an increase of the quality of transactions sent.

482. In connection with numerous queries from obliged institutions and cooperating units concerning the implementation of the statutory obligations, in 2004, as in the previous years, the submitted questions were answered in writing, the problems were solved within the groups established on the current basis and specialist workshops addressed mainly to the banking sector were arranged.

483. The results of the work of the GIFI are published in the form of reports containing statistical data. Up-to-date information on the activities of the GIFI is also published on its Internet site. The obligated institutions are informed of the measures adopted by the GIFI during training sessions.

Co-operation Programme

484. Bearing in mind the need to increase the effectiveness of cooperation with the obliged institutions and cooperating units, a programme entitled "*The Programme of cooperation of the General Inspector of Financial Information with chosen cooperating units and economic associations within the scope covered by the act of 16 November 2000 on counteracting introducing to the financial system of property assets stemming from illegal or undisclosed sources and on counteracting the financing of terrorism*" was developed and implemented in 2003 by the GIFI. The aim of this *Programme* was, among others:

- to help the cooperating units implement the tasks imposed by the law,
- to improve the work with the cooperating units and economic administrations rallying obligated institutions,
- to build confidence in the office and activities of the GIFI,

- to activate new sources of information on the attempts to introduce funds derived from illegal or undisclosed sources into the financial system and on the attempts to finance terrorism in Poland,
- to ensure the best possible conditions for cooperation between the General Inspector, cooperating units and obliged institutions,
- to increase the amount and quality of information on suspicious transactions.

485. In 2003 the first stage of implementation of the *Programme* constituted meetings between the General Inspector and the management of institutions, during which views on the application of the provisions of the act were exchanged, problems that occurred as a result of activities undertaken by the institutions were discussed and schedules and ways of achieving the abovementioned goals were specified. Cooperation with, among others, 15 associations and self-governments grouping obligated institutions, fulfilling the role of institutions coordinating or mediating in transferring information from the GIFI was established, and 13 working teams for solving submitted problems resulting from implementing the provisions of the act in practice were created. These teams dealt with *inter alia* elaborating a typology of suspicious transactions, and preparing a standard list of issues, which should be included in internal procedures.

486. Under the *Programme* in 2004, thirteen training courses were delivered for 461 persons employed at cooperating units. The trainings courses were as follows:

- 8 training courses for the heads of inland revenue: "*The Role and the Tasks of the inland revenue in Counteracting Money Laundering and Combating the Financing of Terrorism*" – 256 persons.
- 4 trainings for the employees of customs offices: "*Reorientation – the inspection of the entities"* conducting activity involving games of chance and *"automatic machine games"* – 200 persons,
- 1 training course for the employees of the Supervision and Inspection Unit of the Department of Games of Chance and Mutual Betting – "*The inspection of the compliance with the provisions of the AML Act*" – 5 persons.

Training

487. One of the statutory tasks of the GIFI, according to Article 4 para. 5 of the AML Act, is the initiating and taking of other actions serving to prevent the use of the Polish financial system for legalising revenues derived from illegal or undisclosed sources. This includes the training of personnel of obligated institutions within the scope of the responsibilities of these institutions. The efficiency of the functioning of the system of counteracting money laundering and financing of terrorism to a large degree depends on the knowledge of the obligated institutions' employees about this phenomenon, and the threat it presents to the financial system of the state, relevant binding regulations and practical methods of recognising and spotting the suspicious transactions. Taking this into consideration, special training has been prepared for specific obligated institutions (banks, insurance companies, currency exchange offices etc.) by the GIFI, in the scope of tasks imposed on those institutions. The objectives of the training designed for obligated institutions' employees were the following :
    - Learning the problems of money laundering
    - Learning the danger resulting from the laundering of money
    - Acquisition of knowledge about the AML Act's objectives
    - Learning the tasks and obligations of the obligated institutions
    - Knowing the rules of transmitting information to the General Inspector
    - Acquisition of competences concerning the application of the Act's provisions
    - Learning the ways and methods of money laundering by examples

488. In 2003, the GIFI prepared and implemented a new formula of training for obligated institutions in the field of the implementation of duties imposed by the Act. Its aim was to facilitate, for those interested, access to information on implementation of provisions of the Act in practice. Programmes for two categories of recipients from obligated institutions have been prepared - for obligated institutions' employees (basic training) and for obligated institutions' trainers (extended, specialised, including issues of training methodology).

489. The programme of basic training for employees included penal issues, Polish and international regulations pertaining to the combating of money laundering and issues relating to the registration of transactions and providing information to the GIFI. The object of these training courses was to acquaint the employees responsible for the enforcement of the regulations of the AML Act with the statutory tasks of the GIFI and the obligated institutions as well as with criminal responsibility for breaching the provisions of the AML Act. The training courses were designed to develop positive attitudes regarding the application of the AML Act and the importance of individual employees of the obligated institutions within the money laundering prevention system and the fight against the black economy. Specialised training for trainers ended with a test and the issuing of a certificate (with the name of participant given). Obligated institutions sent to such training sessions those employees who were to perform the function of a coach, i.e. the person training all other employees of the obligated institution in the scope of implementation of duties resulting from the provisions of the AML Act and from internal procedures.

490. In 2003, the GIFI trained representatives of the following categories of obligated institutions:
- banks - 263 trainers and 38 employees,
- insurance undertakings - 76 trainers,
- foreign exchange offices - 48 coaches and 276 employees,
- games of chance - 41 coaches,
- factoring - 7 employees,
- brokerage houses - 49 coaches,
- jewellers - 20 employees,
- real estate agents - 20 trainers,
- leasing - 50 employees,
- cooperative savings and credit unions - 18 trainers.

491. These training sessions were organised with reference to needs and applications sent by obligated institutions to the GIFI. Furthermore, the trainings were continuously modified. Emphasis was made on transmitting practical knowledge related to the implementation of the duties imposed by the AML Act, and on the specific character of activities of different institutions.

492. In 2004, the training organised by the GIFI (for the obligated institutions) was dedicated mainly to the presentation of the method of transferring information from the transactions registers by means of electronic information carriers. In 2004, the GIFI launched an "E-learning" course for obligated institutions. This course is a form of distant learning using *inter alia* the Internet as a transfer medium. Deciding on E-learning, the GIFI wanted to ensure the possibility of participation in the training for a large group of obligated institutions' employees - the 2-week virtual training cycle may cover 400 employees at a time (300 employees of obliged entities, 75 employees of cooperating institutions and 25 of other so called "interested entities") - without the need to increase costs connected with participation in "traditional training" (among others costs of per diem and travel of the employee) - at a time convenient for the trainees.

493. The course scenario was based on materials consisting of 9 lessons, prepared by the employees of the Department of Financial Information:

1) Basic issues of counteracting money laundering and financing of terrorism (preceded by an Introduction).

2) Entities participating in counteracting money laundering.
3) The tasks of Obliged Institutions.
4) The identification of suspicious transactions
5) ”Get to know your client” programme in the entities covered by the Act.
6) The internal procedure in an obliged institution.
7) Transfer of information to the GIFI.
8) Inspection of compliance with the provisions of the Act
9) Criminal responsibility for the infringement of legal provisions.

494. The training course is completed by a test to check the participants' knowledge. After an employee of an obliged institution successfully passes the online test, he/she receives a certificate confirming of the course completion. Between 15 January and 31 December 2004, 2194 persons participated in the course and 1788 persons passed the final test. Between 21 March and 15 December 2005, 2913 employees of the obligated institutions participated in the course and 2659 employees passed the final test.

495. However, the BSC as supervisory body for banks considers that guidance on matters such as training and anti-money laundering governance is not part of its responsibilities. It takes the view that its responsibility is limited to ensuring that banks do provide training to the staff who need it and that they comply with their own internal inspection requirements as approved by the GIFI, and fulfil their reporting obligations. Nevertheless, the BSC participates in symposia and conferences for banks on anti-money laundering matters.

496. The PSEC in association with GIFI organises trainings for brokerage houses.

feedback

497. GIFI provides general feedback as such information is included in the annual report (which is published on the GIFI website), in trainings and the manual. Specific feedback to reporting entities is provided by acknowledgment of the receipt of an STR. For above threshold transaction reports which are submitted electronically, an automatic receipt message is released to the reporting entity.

3.12.2 Recommendations and comments

498. The intensity, depth and quality of training offered by the GIFI is exemplary. The manual for obliged entities, which is actually a book published by the GIFI, and widely distributed, is well written, contains many typologies described clearly including clear graphics, and the private sector confirms that it contains useful practical information. All private sector entities, including most of the DNFBP (the representatives of the casinos were not aware of this guidance), know the book and confirm that they have been trained and informed well by it.

499. The direct training, the information and support provided at the GIFI-website as well as the e-learning course show that this is a central issue for GIFI and managed with enthusiasm. The overall number of people trained and entities addressed is impressive.

500. However, the involvement of the financial supervisors in this area seems to be weak. The financial supervisors should be more proactive in this area and should consider issuing sector-specific AML/CFT guidance.

3.12.3 Compliance with Recommendation R.25

	Rating	Summary of factors underlying rating
R.25	**Largely compliant**	Sector-specific AML/CFT guidance issued by the financial supervisors is missing.

3.13 Ongoing supervision and monitoring (R.23 [Criteria 23.4, 23.6 and 23.7] and R. 32)

3.13.1 Description and analysis

General

501. Inspections performed either by the GIFI or other Supervisory Authorities focus primarily on verifying whether the obligated institutions observe the rules of registration and notification of transactions in accordance with the provisions of the Act. In addition, inspectors also verify: internal procedures designed to prevent the introduction into financial circulation of pecuniary values originating from illegal or undisclosed sources and counteracting financing of terrorism, and, in particular, check whether these procedures are used for determining the identity of persons participating in transactions; if in the organisational structure of the obligated institution there is a person responsible for the observance of the provisions of the Act; whether the correct measures have been applied; how transactions are registered and documents pertaining to registered transactions are stored; what is the access to such documents; what are the rules of registering transactions and passing information on the registered transactions to the GIFI; and if obligated institutions provided training to the employees within the scope of the tasks imposed by the Act.

502. A report is drawn up after the inspection which contains the findings of the inspectors. There exists an appeal procedure consisting in the submission by a representative of the inspected obligated institution of written objections in the event of any discrepancies.

503. The practice is that written information on the inspection is passed on to the agency performing supervision over the obligated institutions pursuant to separate regulations. These agencies are also obliged to provide information on the results of any audits that they have carried out. Written information about the results from the inspections, performed by the Supervisory bodies is presented to the GIFI in writing within 14 days of the inspection's conclusion.

a) Supervision and monitoring by the supervising institutions (apart from GIFI)

504. Pursuant to binding provisions of the law, supervising institutions forward to the GIFI the results of their inspections conducted in obligated institutions subject to their supervision, as related to AML/CFT issues. From 2003 to 2005 the following notifications about undertaken inspections were submitted to GIFI:

Notifications to GIFI about carried out on-site inspections of obliged institutions			
Supervising entity	**2003**	**2004**	**2005**
National Bank of Poland [1)]	1404	1301	1071
General Inspectorate of Banking Supervision (GINB) [2)]	15	17	20
National Association of Cooperative Savings and Credit Unions [3)]	33	23	23
The Polish Securities and Exchange Commission (PSEC)	2	11	9
Insurance and Pension Funds Supervisory Commission [4)]	2	9	11
Department of Games of Chance and Mutual Betting in the Ministry of Finance	6	1	-
President of the Court of Appeal [5)]	1	9	16
Total	**1463**	**1371**	**1150**

Explanatory Note:
1) Inspections of exchange offices
2) The GINB is an executive body of the Commission for Banking Supervision; it performs direct tasks in respect of the banking supervision; the data refer to the on-site inspections on banks
3) Inspections in Cooperative savings and Credit Unions
4) Inspections in insurance companies
5) Inspections of notaries public

505. The results submitted in respect of the inspections in **2003** pointed to irregularities in inspected institutions similar to those which were found by GIFI inspectors during their inspections. After analysing the documents received, GIFI submitted notifications in 33 cases to the public prosecutor's office of justified suspicions of committing the crime of non-fulfilment of duty of establishing internal procedures preventing introducing into the financial system of property assets stemming from illegal or undisclosed sources. These notifications were based on analysis of materials transferred by the NBP concerning inspections conducted in exchange offices.

506. In **2004**, the inspections were basically carried out in two main areas – direct inspection in an obliged institution and indirect inspection consisting of the analysis of the inspection results submitted by the institutions which have a mandatory obligation to supervise the implementation of the Act.

507. Also the submitted inspection results of 2004 confirmed irregularities similar to those revealed during the inspections carried out by the GIFI inspectors. In order to work out a uniform methodology and scope of inspection, the meetings with the representatives of supervising institutions initiated in the previous year were continued during the whole of 2004.

Banking Supervision Commission (BSC)

508. The BSC issued an 800-page methodology for on-site inspections which also covers AML/CFT issues. AML/CFT on-site inspections take 4-7 days with 3-4 inspectors on average. The BSC conducts
- full scope inspections in large banks once every 2 years, in medium banks once every 3 years, and in small banks once every 4 years;
- special area inspections (e.g. AML/CFT); and

- inspections of particular cases which can also cover AML/CFT issues.

The banking supervision of the BSC is executed by the General Inspectorate of Banking Supervision (Generalny Inspektorat Nadzoru Bankowego – GINB), which is an executive body of the Commission for Banking Supervision and is an organisationally independent structure of the National Bank of Poland.

Insurance and Pension Funds Supervisory Commission

509. AML on-site inspections are performed by 1-2 inspectors. During the interview with the Insurance and Pension Funds Supervisory Commission it was stated that inspections in insurance sector do not cover CFT issues.

Polish Securities and Exchange Commission (PSEC)

510. Compliance with the AML Act is checked only by providing questionnaires to the obliged entities during onsite visits (see Annex 27). The PSEC does not verify the answers provided by the private sector. The existence of internal AML/CFT procedures and their formal compliance with the AML Act is checked by the PSEC offsite. According to the information provided by the representatives of the PSEC during the onsite visit, CFT issues are not covered.

National Association of Credit and Savings Unions

511. A different, somewhat unusual regime of supervision is applied to credit unions. Supervision is performed by the National Association of Credit and Savings Unions. As these unions mostly undertake small retail customer business and only provide services to their members, who are usually associated to them via a large company (e.g. the Gdansk Shipyards), or through regional, small community connections, the risk of money laundering in this sector seems very low.

National Bank of Poland (NBP)

512. The inspection of obligations specified in the AML Act is still exercised by the NBP within the framework of the inspections of foreign exchange activities, as defined by the foreign exchange regulations. The inspection tasks are within the competence of 16 organisational units located throughout the country. The inspections are performed on the basis of internal inspection procedures established for this area. Since the last evaluation visit, the inspection procedures applied by the NBP were modified twice as a result of both the changes to the regulations on counteracting money laundering and the larger experience of the NBP in that regard. The inspection methodology, which has been in place since 2003, includes, apart from the examination of compliance with formal requirements of the AML Act on the part of bureaux de change, the evaluation of practical implementation to the relevant regulations in force.

513. The inspection activities in respect of regulations on counteracting money laundering in the bureaux de change include checks as to whether:
   - a person responsible for the performance of duties laid down in the Act was appointed in the bureau;
   - the internal procedure was introduced with regard to counteracting the introduction of assets derived from illegal or undisclosed sources into the financial system and counteracting the terrorist financing, and whether the internal procedure ensures the fulfilment of statutory obligations by the exchange bureau, in particular whether it complies with the legislation in force and takes into account the specific character of bureaux de change operations;
   - the rules governing the participation of employees in training programmes on transactions which may be related to crime were specified;
   - the register of transactions, the circumstances of which indicate that the assets are derived from illegal or undisclosed sources and transactions the value of which exceeds the

equivalent of EUR 15 000, is kept and whether the transactions are registered in accordance with the law;
- the transactions with the characteristics of the so-called suspicious transactions and since 1 January 2004 also the transactions in excess of the statutory threshold of an equivalent of EUR 15 000 are entered into the registers and whether the obligation to notify the GIFI about those transactions is fulfilled.

514. During its inspections the NBP also establishes whether the operations carried out by bureaux de change are analysed in term of legality of the funds origin, in accordance with criteria laid down in internal procedures.

b) On-site inspections carried out by GIFI

515. The inspections performed by GIFI are carried out by its employees. In the years 2004 and 2005, GIFI carried out the following on-site inspections (based on information submitted by the Analyses Unit or other organisational units of the Department):

On-site inspections carried out by GIFI		
Obliged institution	**2004**	**2005**
Banks	9	10
Insurance company	1	2
Polish Post Office	-	1
Casinos	1	4
Factoring companies	-	1
Brokerage houses	-	2
Credit union	-	1
Notaries	-	2
Leasing company	-	1
Investment fund society	-	1
currency exchange office	1	-
Total	**12**	**25**

516. The inspections of the year **2004** revealed the following:
a) formal irregularities with respect to Article 28 of the AML Act (namely, to adjust internal procedures and to appoint a responsible person),
b) substantial irregularities, i.e. poor implementation of provisions of the Act, mainly in respect of the obligation to record transactions, to identify entities participating in the transaction, to identify transactions and inform about them, to keep the register of the transactions complete including the documents related to the recorded transactions, as well as irregularities in keeping the registers of transactions and transmitting information from these registers to the GIFI.

517. In accordance with the binding provisions of the Act, the findings of the GIFI inspectors were submitted to the supervising institutions for further processing and use.

3.13.2 Recommendations and comments

518. The financial sector supervisors seem to be experienced, well managed and to know the supervised entities well, inspect them regularly and provide a generally good framework of supervision, information, regulation and control. However, in the AML/CFT area, while the number and depth of onsite inspections seems appropriate, these are conducted as a formal check of the obligations mentioned above in the law, without a material engagement into the less formal requirements of the Polish AML/CFT system, such as risk analysis, enhanced due diligence,

ongoing monitoring of customers, monitoring of unusual and complex behaviour, and detection of suspicion.

519. Inspections of the Insurance and Pension Funds Supervision Commission should cover CFT issues. The PSEC inspections of the AML/CFT area are purely formal and should be enhanced. The evaluators recommend that the questionnaire of the PSEC should explicitly address CFT issues.

3.13.3 Compliance with Recommendations 23 (Criteria 23.4, 23.6 and 23.7)

	Rating	Summary of factors underlying rating
R.23	**Partially compliant**	• Financial supervisors should not only check formal compliance with the AML Act but also overall effectiveness of the AML/CFT systems in the financial institutions. • Inspections of Insurance and Pension Funds Supervision Commission do not cover CFT issues. • The PSEC inspections of the AML/CFT area are purely formal.

3.14 Money or value transfer services (SR.VI)

3.14.1 Description and analysis

520. There is no system in place for registering and/or licensing natural and legal persons that perform money or value transfer services (MVT service operators) in Poland.

521. This applies to the formal money remittance, which is currently not covered by the AML Act. Additionally, no measures cover alternate remittances as well. As certain information is only available to the money remittance business itself, and not to its agents, this constitutes a significant gap in the coverage of the financial sector for AML/CFT.

522. The authorities informed the evaluators that this is due to the fact that Western Union and Moneygram, the companies active in Poland, act exclusively through banks and the Polish Post as their agents. However, private sector representatives confirmed that bureaux de change are also contracting with Western Union. It was not clear if it is prohibited by the Polish law to incorporate a company which would provide MVT services without contracting a bank or a bureau de change, but some of the experts seemed to think that such a company would be possible under the current legal system, without any restrictions on its business by supervision or AML/CFT rules.

523. Monitoring of the activities of MVT service operators can be performed only indirectly via checking compliance with the AML/CFT obligations in banks. This means, to give just one example of information that is missing, that structuring transactions below the threshold via different banks, a well-known typology related to money transfer business, cannot be detected in the current system.

524. As mentioned above, the Polish AML Act is careful even to include entities which do not exist yet in Poland, such as electronic money institutions, and has a very complete and high coverage of entities, which goes beyond international requirements (i.e. foundations), with the stated intention of ensuring very comprehensive coverage. Against this background, the fact that money transfer services are not mentioned in the AML Act is worrying. There seems to be an important gap also in the awareness of the authorities, which means that this internationally well known high-risk area is not adequately addressed in the Polish system.

3.14.2 Recommendations and comments

525. Poland should implement Special Recommendation VI.

3.14.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	**Non compliant**	• No system in place of registering and/or licensing MVT service operators. • MVT service operators are not subject to the applicable FATF Recommendations. • There is only indirect monitoring of MVT service operators with regard to compliance with the FATF recommendations. • There are no sanctions applicable to MVT service operators.

4 PREVENTIVE MEASURES – DESIGNATED NON FINANCIAL BUSINESSES AND PROFESSIONS NON-FINANCIAL BUSINESSES

4.1 Customer due diligence and record-keeping (R.12)
(Applying R.5 to R.10)

4.1.1 Description and analysis

Generally

526. Recommendation 12 requires DNFBP to meet the CDD and record-keeping requirements set out in Recommendations 5, 6 and 8 to 11 in the circumstances specified in Criterion 12.1. Overall it can be noted, that the deficiencies in the AML/CFT preventive measures framework as described for financial institutions also apply to DNFBP, since the core obligations for both DNFBP and financial institutions are based on the same law (the AML Act).

Applying Recommendation 5

527. DNFBP are obliged to register transactions in excess of EUR 15,000 and also when the transaction is executed involving more than a single operation, in circumstances suggesting that these operations are linked together (Article 8 para. 1 of the AML Act). The same applies in the case of suspicious transactions (without any threshold). The obligation of the obligated institutions to register transactions is connected with the obligation to identify these clients (Article 9 of the AML Act). However, the obligation to register above threshold transactions "*does not concern real estate agents ,[...] counsels, legal advisers and foreign lawyers*" (Article 8 para. 5 of the AML Act). Thus, CDD requirements applied by these categories of DNFBP cover only suspicious transactions. Accountants seem to be not covered by the AML Act at all. However, the evaluators were informed by the Polish authorities, that lawyers and real estate agents cover some elements of identification in practice for all kind of transactions.

528. In the case of a casino (within the meaning of the provisions of the Law of 29 July 1992 on games of chance, mutual betting and automatic machine games; *Journal of Laws* of 2004 No. 4, item 27, Annex 3) the obligation of Article 8 para. 1 of the AML Act (i.e. to register transactions in excess of EUR 15,000 and also when the transaction is executed involving more than a single operation, in circumstances suggesting that these operations are linked together) "shall refer to" (i.e. is applied to) purchase or sale of tokens amounting to, at least, the equivalent of 1,000 EUR (Article 8 para. 1a of the AML Act).

Applying Recommendation 6 and 8

529. Poland has no specific AML/CFT measures regarding PEPs; furthermore, it has no legislation or regulation that applies to DNFBP and adequately addresses Recommendation 8 (new technologies and non-face to face customers).

Applying Recommendation 9

530. Recommendation 9 is not applicable to Poland (see Section 3.3).

Applying Recommendation 10

531. According to Article 9 para. 4 of the AML Act, the information acquired as part of the identification procedure shall be kept for a period of five years, starting from the first day of the year following the year in which the last entry concerning the given transaction was made.

Applying Recommendation 11

532. The implementation of Recommendation 11 for DNFBP 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, to examine - as far as possible - their background and purpose, to set out their findings in writing and keep the findings available for competent authorities for at least 5 years, results partly and also only indirectly from the obligation imposed by Article 8 para. 3 of the AML Act ("*The obligated institution receiving instruction or order from a client to execute a transaction, if circumstances suggest that the property values involved in this transaction may originate from illegal or undisclosed sources, shall register such transaction regardless of its value and nature*"). But it has to be noted that there is not an obligation to examine the background and purpose of such transactions, or a requirement to keep any findings made by a financial institution regarding these or other suspicious transactions available for competent authorities and auditors.

4.1.2 Recommendations and comments

533. The coverage of DNFBP is very complete and in line with both international standards and the EU Directive. It comprises casinos, notaries public, legal advisers, statutory auditors, tax advisers, auction houses, antique shops, precious metals and stones traders, commission sales business, pawnshops, real estate agents. Additionally, the Polish Post and foundations, which are not required by international norms, have been included, this shows that Poland has considered adding other high risk categories to the obliged entities and done so.

534. However, the support for and understanding of the AML/CFT regime is very uneven. While the Polish Post and notaries seem engaged and are seen to be fulfilling their obligations in practice, other institutions, e.g. casinos, are not very much aware of ML/FT risks in their fields. In certain areas there is formal protest against the obligations; for instance, lawyers have initiated proceedings in the Constitutional Court against the AML Act, and are strongly opposed to their inclusion, echoed by the tax advisers and auditors. Having said that, the evaluators recommend working with the different sectors to improve awareness, and overcome any unwillingness to apply AML/CFT requirements. Information campaigns to this end are required. Poland has made some strong efforts in this direction already, by writing to all obliged identities that could be identified, by offering training, publications etc. – but this effort still needs to continue, as the results are not yet in line with the Recommendation.

535. Poland should fully implement Recommendations 5, 6, 8, 10 and 11 and make these measures applicable to DNFBP.

536. Real estate agents, counsels, legal advisers and foreign lawyers should be required to apply CDD measures in all relevant situations according to the FATF Recommendations and not only in the case of suspicious transactions. Accountants should also be covered by these obligations.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors underlying rating
R.12	**Non compliant**	• The same concerns in the implementation of Recommendation 5, 6, 8, 10 and 11 apply equally to obliged financial institutions and DNFBP (see section 3 of the report). • CDD requirements do not apply to accountants and do not fully apply to real estate agents, counsels, legal advisers and foreign lawyers.

4.2 Monitoring of transactions and other issues (R. 16)
(Applying R.13 - 15 and 21)

4.2.1 Description and analysis

Applying Recommendation 13

537. Criterion 16.1 requires Essential Criteria 13.1 – 4 to apply to DNFBP. Criteria 13.1-3 are marked with an asterisk. The first two require reports to the FIU where the obliged entity suspects or has reasonable cause to suspect funds are the proceeds of criminal activity or has reasonable grounds to suspect or suspects funds are linked to terrorism etc or those who finance terrorism. Article 8 para 3 in conjunction with Art 2 para 1 of the AML Act covers DNFBP making reports to the GIFI in respect of suspicious transactions. As broadly described under section 3.7 for financial institutions, the same issues and deficiencies apply equally for DNFBP. The Polish Post and notaries seem engaged and are seen to be fulfilling their obligations in practice; on the other hand, as noted above, some institutions like casinos are quite unconcerned about M/FT risks in their field and others, like lawyers, tax advisers and auditors do not accept their obligations (lawyers have initiated proceedings in the Constitutional Court against their inclusion in the AML Act[22]). The small numbers of STR from the DNFBP sector may be a result of this attitude and is a main concern. More outreach to this sector would be welcome.

Applying Recommendation 14

538. The issues of "Tipping off" and "safe harbour" provisions are extensively described under section 3.7.

Applying Recommendation 15

539. According to Article 28 of the AML Act, obligated institutions should devise internal procedures for preventing the introduction into financial circulation of property values derived from illegal or undisclosed sources or the financing of terrorism, in particular relating to the fulfilling of the requirement of a client's identification and keeping of information gathered as part of the identification process, should provide personnel with training in identifying transactions potentially linked to the offence referred to in Article 299 of the Penal Code, and should name individuals responsible for fulfilling the obligations resulting from this Act. In case

[22] The Polish authorities informed that after the onsite visit, the Constitutional Court rejected this claim.

of obligated institutions, being limited companies or joint-stock companies, the responsible person is a Managing Board member appointed by the Managing Board.

540. The deficiencies are the same as mentioned in Section 3.

Applying Recommendation 21

541. See Section 3.

4.2.2 Recommendations and comments

542. The same deficiencies in the implementation of Recommendations 13-15 and 21 in respect of financial institutions apply equally to DNFBP. Poland should fully implement Recommendations 13-15 and 21.

543. Generally the examiners believe that once formal provisions are in place, the effectiveness of implementation can only be developed by proper monitoring of implementation. It is also important to work with the different sectors to improve awareness, and overcome any unwillingness to apply AML/CFT requirements. Ongoing information campaigns to this end are required.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	**Non compliant**	• The same deficiencies in the implementation of Recommendations 13-15 and 21 in respect of financial institutions apply equally to DNFBP. • Some institutions like casinos are quite unconcerned about ML/FT risks in their field and others, like lawyers, tax advisers and auditors do not accept their obligations. This also results in the small numbers of STR from the DNFBP sector.

4.3 Regulation, supervision and monitoring (R.17, 24-25)

4.3.1 Description and analysis

Recommendation 24

544. In Poland, 140 entities conduct activities involving games of chance, mutual betting and automatic machine games, and automatic machine games with low prizes. Furthermore, at the time of the onsite visit 27 casinos operated in Poland. Companies which conduct activities in the area of games of chance are obliged to install in a casino a system for inspection and operating games, inclusive of a system for deciding doubts regarding organised games and verifying the correctness of issuing the certificates of the winnings by way of magnetic picture recording. The minister competent for public finance shall, by way of regulation, lay down detailed conditions for the installation and the use of such a system, taking particular account of the necessity to ensure the possibility of reconstructing each game.

545. The GIFI is entitled to check compliance of all DNFBP concerning the obligations set forth by the AML Act (Article 21 para. 1). The same responsibility is granted to:
    a) the Minister responsible for public finances with regard to entities organizing and operating games of chance, mutual betting, automatic machine games and automatic machines games with low prizes; and
    b) Presidents of Appeal Courts with regard to notaries public.

546. Concerning the number of inspections carried out by GIFI and the other supervisory bodies reference should be made to the tables as shown under Section 3.13.

547. There is an obligation to register with GIFI if the entity is an obliged entity under the law within 30 days of commencing the activity. GIFI seems to have made a strong effort to inform associations or representatives of DNFB when they became obliged entities under the Act, but the private sector does not perceive continued follow up by GIFI. GIFI itself makes an effort to check against registers and lists to contact all obliged entities, but there is no clarity on the percentage of DNFBP who are actually registered in less accessible areas such as jewellers, pawnshops, foundations. A few onsite inspections have been made, but no sanctions have been imposed yet.

Recommendation 25

548. The degree of effort, training, education and guidelines applied to DNFBP in Poland is exceptional. The manual of the GIFI for obliged institutions and cooperating entities entitled "Counteracting money laundering" is useful and practical; it has been widely distributed, and the DNFBP seem to know it and also have thought about it, as related to their own business. Overall the situation is quite similar as for financial institutions but, in contrast to the situation for financial institutions, sector-specific guidance was issued.

4.3.2 Recommendations and comments

Recommendation 24

549. The supervisory and enforcement structures for DNFBP exist. However, the number of controls in comparison to the number of DNFBP is not sufficient. Thus the system for monitoring and ensuring compliance with AML/CFT requirements cannot be assessed as effective. The authorities should consider if the human resources of the FIU are sufficient to perform its functions in this area.

Recommendation 25

550. Compliant – see Section 3.

4.3.3 Compliance with Recommendations 17 (DNFBP), 24 and 25 (Criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.5 underlying overall rating
R.17	**Partially Compliant**	• The sanction regime is disproportionate for minor cases which carries the risk that it is not applied and reduces its effectiveness. • Few sanctions have been imposed.
R.24	**Partially compliant**	More controls, and concurrently more resources would be needed to ensure compliance of DNFBP with AML/CFT requirements.
R.25	**Compliant**	

4.4 Other non-financial businesses and professions/ Modern secure transaction techniques (R.20)

4.4.1 Description and analysis

551. Criterion 20.1 states that countries should consider applying Recommendations 5, 6, 8 to 11, 13 to 15, 17 and 21 to non-financial businesses and professions (other than DNFBP) that are at risk of being misused for money laundering or terrorist financing.

552. In addition to the non-financial businesses and professions that are designated according to the FATF Recommendations, the obligations of the AML Act also apply to:
- tax advisors
- entrepreneurs running auction houses
- antique shops
- commission sale
- pawnshops
- foundations.

Compliance of the aforementioned entities with AML/CFT obligations is monitored by the GIFI.

Use of modern and secure techniques

553. Cash is still of large importance in the Polish economy. The banks actively promote the development of modern non-cash methods of payments for goods and services (payment cards /debit and credit cards, payment orders, access to the accounts through the Internet). The Polish authorities also aim at the gradual abandonment of cash payments and their replacement with non-cash settlements. The following acts provide examples of the activities undertaken in that regard:
- Article 4 para. 5 of the Banking Law which provides a definition of "electronic money;"
- Act of 12 September 2002 on electronic payment instruments (Annex 22);
- Act of 18 September 2001 on electronic signature (Annex 23).

4.4.2 Recommendations and comments

554. The Recommendation is fully observed.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	**Compliant**	

5 LEGAL PERSONS AND ARRANGEMENTS AND NON-PROFIT ORGANISATIONS

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

5.1.1 Description and analysis

555. 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.

556. As noted in Section 1.4, there are several forms of enterprises established in Poland for the purpose of undertaking business and which have to be registered in the National Court Register. 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 a voivodship[23] or a part thereof (Art 2 para. 1 of the Act of 20 August 1997 on the National Court Register, Annex 6). 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 shall also issue copies, excerpts and certificates from the Register; these documents have the validity of documents issued by a court. The Central Information collects fees for these documents (the fees are income of the state budget).

557. Everyone has the right to access data of the Register through the Central Information and also to 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).

558. Registration in the Register shall be made upon an application, unless a specific regulation stipulates registration *ex officio* (Article 19 para. 1); examples for *ex officio* registration can be found in Articles 74 para. 3, 277 para. 3, 464 para 3, 510 para. 1. 545 para. 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.

[23] voivodship is a Polish geographical unit of administration.

559. Specimens of signatures of persons authorised to represent an entity or proxy, certified by a notary or made in presence of a judge or an authorised court employee, have to be enclosed with an application for registration of the entity which has to be entered into the Register.

560. 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).

561. Central and local government bodies, courts, banks, court executive officers and notaries shall 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.

562. 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 para. 2).

563. Article 36 of the Act on the National Court Register deals with the types of entrepreneurs which have to be registered. 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.).

564. 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)

565. 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

566. 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

567. 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.

568. 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.

569. A lot of the information from the register of entrepreneurs can be found on-line, but complete shareholder information is not generally on-line. Only where the partners in a Limited Liability Company have at least 10% of the share capital and only where the joint stock company has only 1 shareholder, is information available on-line.

570. 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.).

571. In Poland legal persons are able to issue bearer shares mainly in public trading. Such trades 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. 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. 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.

5.1.2 Recommendations and comments

572. It is recommended that Poland reviews its commercial, corporate and other laws with a view to taking measures to provide adequate transparency with respect to beneficial ownership. 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	**Partially Compliant**	• 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.

5.2 Legal Arrangements – Access to beneficial ownership and control information

5.2.1 Description and analysis

573. Recommendation 34 requires countries to take measures to prevent the unlawful use of legal arrangements in relation to money laundering and terrorist financing, by ensuring that commercial trust and other laws require adequate transparency concerning the beneficial ownership and control of trusts and other legal arrangements.

574. Domestic trusts cannot be established in Poland. The evaluators were advised that the reason for that is that the different types of enterprises are provided for in Polish law and that there is no such type foreseen in Polish law and could not be registered on the National Court Register.

575. Foreign entities can act in Poland as a branch (see Section 1.4); in order to register at the National Court Register they need a statistical number; these numbers are regulated in the Council of Ministers' "Regulation of the 20 January 2004 about the Polish classification of activities". This Regulation lists certain activities under which commercial activity can be undertaken. If an activity is not listed in this Regulation, the entity cannot get a statistical number and as a consequence also not establish commercial activity. One such activity is "financial services/private banking". Though the Polish authorities indicated that full data needed to be provided for the obtaining of the statistical number, it was difficult for the examiners to satisfy themselves that some foreign trusts could not be administered in Poland.

576. Poland has not signed the Hague Convention on the Law Applicable to Trusts and on their Recognition.

5.2.2 Recommendations and comments

577. Recommendation 34 is not applicable to Poland as trusts cannot be established in Poland.

5.2.3 Compliance with Recommendation 34

	Rating	Summary of factors underlying rating
R.34	**N/A**	As the Polish system does not allow to establish a (foreign or domestic) trust, Recommendation 34 is not applicable.

5.3 Non-profit organisations (SR VIII)

5.3.1 Description and analysis

578. As noted under Section 1.4, 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.

579. In the Polish legal system NPOs are foundations. 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
- 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).

580. 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.

581. A foundation can be established by private individuals, regardless of their citizenship or residence, or by legal entities. The headquarter 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.

582. 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.

583. 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.

584. 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.

585. 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).

586. The statutes, articles of association, or other internal documents of non-governmental organisations or entities specified in Article 3 para. 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.

587. 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.

588. 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.

589. According to Article 29 para. 1 in conjunction with Article 28 para. 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 para. 2).

590. 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.

591. 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.

592. 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.

593. It appears that - since Special Recommendation VIII was introduced - there has been no 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 that 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.

Additional elements

594. Most of the measures in the Best Practice Paper for SR VIII have not been implemented.

5.3.2 Recommendations and comments

595. 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 there are reporting structures and also steps to ensure financial transparency. 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. 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.

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 SR.VIII

	Rating	Summary of factors underlying rating
SR.VIII	**Non compliant**	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.

6 NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and co-ordination (R. 31)

6.1.1 Description and analysis

596. Recommendation 31 (and Criterion 13.1) is concerned with co-operation and coordination between policy makers, the FIU, law enforcement, supervisors and other competent authorities.

597. The legal basis for cooperation between the entities involved in counteracting money laundering is laid down in the Act of 16 November 2000 (the AML Act). It imposes an obligation on state and local administration authorities and other state organisational units, including the National Bank of Poland and the Commission for Banking Supervision (GINB), to cooperate within the scope of their competence with the General Inspector of Financial Information (GIFI) by notifying it immediately about the suspicion of money laundering, by submitting authenticated copies of documents concerning the suspicious transactions and the information about the persons who carry them out, by providing the information and authenticated copies of documents necessary to perform the tasks specified in the Act.

598. With respect to preventing money laundering and terrorist financing, the supervisory authorities cooperate with the GIFI. GIFI also provides supervisory authorities with information on inspections and moreover with the interpretation of legislation on money laundering. Chapter 7 of the Act of 16 November 2000 concerns the protection and disclosure of data by GIFI, including cooperation and the sharing of information with the public prosecutor, intelligence and security agencies, and various regulatory agencies. However, the GIFI does not provide information directly to the police, which must obtain such financial data through the public prosecutor. It is the prosecutor that is responsible for supervising and coordinating the work of the police and other law enforcement authorities (e.g., Customs Service, Border Guard) during both the operational and investigative phases. The supervision and coordination authority is contained in the Code of Criminal Procedure.

599. Domestic cooperation among financial supervisors is covered by sectoral laws (e.g. Article 131/4 of the Banking Act) and details of cooperation are included in Memoranda of Understanding.

Additional Elements

600. This covers mechanisms in place for consultation between the competent authorities and the financial and other sectors, including DNFBP that are subject to AML/CFT Laws, Regulations, Guidelines or other measures.

601. The Commission for Banking Supervision is obliged to prepare the instructions to be followed if the banking supervision inspectors suspect that a bank's activities are being used for the purpose of money laundering (Resolution No 4/2001 of the Commission for Banking Supervision; Annex 25). The Commission for Banking Supervision imposed an obligation on the GINB to check the compliance with the provisions of the Act within the framework of conducted supervision. Written information about the results of the inspection is submitted to the GIFI.

602. In February 2006, to facilitate internal coordination, a "horizontal working group for international sanctions" was established in the Ministry of Foreign Affairs. Though its main responsibility is focused on the legal aspects of the implementation of international sanctions, it may provide additional scope for inter-agency coordination through its advice to the Council of Ministers.

There is also an inter-agency Working Group for Co-ordination of Recognised Operational Activities in Combating of Terrorism (replaced in 2006 by Interagency Group for Terrorism Threats), which includes the Police, the Internal Security Agency, border guards and other agencies, as well as the Ministry of Finance (including the Polish FIU). It is responsible for developing strategies to combat terrorism.

6.1.2 Recommendations and comments

603. Poland has appropriate mechanisms in place but does not appear to be utilising them effectively. In the first instance, more support could be given to the horizontal working group established in February 2006 for international sanctions.

604. On a broader issue, Poland has an intergovernmental Working Group that is reviewing the gaps in its AML/CFT regime and making recommendations for improvement. The assessors recommend that the Group be continued and that this type of interdepartmental coordination additionally be raised to a more senior strategic level to include other key stakeholders. The examiners have in mind a strong coordinating body of the main senior players (the policy makers, the FIU, law enforcement, prosecutors and supervisors). It is suggested that such a Group is chaired at a suitably senior level (perhaps by the FIU). It could have the authority to review systematically and collectively money laundering and terrorist financing vulnerabilities, to resolve interdisciplinary issues, to review periodically the performance of the system as a whole against some key strategic performance indicators and report to the Government; and to review collectively, where appropriate, the available statistical information to better carry out each agency's tasks and thereby enhance the AML/CFT framework. It would be useful to agree precisely which meaningful statistics need to be kept in each agency to properly assess the performance of the system as a whole. Equally such a Group might give policy consideration to feedback to the financial sector and other reporting entities (particularly the current stance on case-specific feedback).

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	**Partially compliant**	Existing coordination measures are not completely effective. It would be helpful to have more coordination of the main AML/CFT players to ensure a consistent approach.

6.2 The Conventions and United Nations Special Resolutions (R. 35 and SR.1)

6.2.1 Description and analysis

605. 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 fully implemented the Vienna Convention, but not the other two. 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.

606. Concerning the Terrorist Financing Convention, Poland has failed to implement several of its provisions, notably the terrorist financing offence (see Section 2.2), some of 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).

607. Poland has implemented UNSCR 1267 and UNSCR 1373 under European Union legislation (subject to the shortcomings described under Section 2.4). With respect to UNSCR 1373, Poland has provided the United Nations' Counter-Terrorism Executive Directorate (CTED) with five periodic 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 obliged entities. The examiners were not advised of any 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. A clear designating mechanism in such circumstances should be created. The US lists were automatically circulated. It appeared the obliged 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.

Additional elements

608. 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 but not yet ratified 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

609. Poland still needs to implement many of the provisions of international conventions that it has ratified.

6.2.3 Compliance with FATF Recommendations

	Rating	Summary of factors underlying rating
R.35	**Partially compliant**	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.
SR.I	**Partially compliant**	Poland has ratified the Terrorist Financing Convention but failed to implement several of its provisions, notably a full terrorist financing offence and the European Union mechanisms for freezing under the UNSC Resolutions need supplementing by domestic procedures for European internals.

6.3 Mutual legal assistance (R.32, 36-38, SR.V)

6.3.1 Description and analysis

Recommendation 36 and SR.V

610. Mutual legal assistance in criminal cases is addressed in the provisions of Chapter 62 of the Code of Criminal Procedure:

Chapter 62 Legal assistance and deliveries in criminal cases

Article 585. *In the course of legal assistance, the required activities of criminal proceedings may be taken, in particular:*

(1) delivery of letters to persons abroad or institutions with an official seat abroad,
(2) hearing of persons as defendants, witnesses or experts,
(3) undertaking viewings and searches of rooms, other places and persons, seizure objects and deliver them abroad,
(4) summoning of persons abroad to a voluntary appearance in court or before a public prosecutor in person in order to hear a witness or for the purposes of confrontation, as well as obligatory appearance of persons subject to custodial sentence,
(5) providing files and documents, as well as information on the criminal records of the defendants,
(6) providing legal information.

Article 586. *1. The court or public prosecutor shall direct a request to deliver a letter to a person having polish citizenship staying abroad, or to hear such a person as a defendant, witness or expert, to a Polish diplomatic posts or consulate.*

2. Where it is impossible to undertake these actions in a way specified in paragraph 1 above, a request may be sent to a court, public prosecutor's office or other competent body of the foreign country. In case of searches, confiscations and delivery of objects, such request should be appended with a court order or order of the public prosecutor ordering undertaking such action in a given case.

Article 587. *Reports from viewings, hearings of persons as defendants, witnesses, experts or reports form other evidence activities undertaken by courts or public prosecutors of a foreign country or bodies under their supervision, produced upon a request of a Polish court or public prosecutor, may be read at a hearing pursuant to the provisions of Articles 389, 391 and 393, if the manner in which the actions were carried out is not incompliant with the principles of the legal order in the Republic of Poland.*

Article 588. *1. Courts and public prosecutors shall provide legal assistance upon a request of courts and public prosecutors of foreign countries.*

2. The court and the public prosecutor shall refuse to provide legal assistance and submit such refusal to the competent authorities of the foreign country if the requested activity is incompliant with the principles of the legal order of the Republic of Poland or if it interferes with its sovereignty.

3. The court and the public prosecutor may refuse to provide legal assistance, if:

(1) pursuant to the Polish legal system, carrying out the activity does not lie within the competence of the court or public prosecutor,

(2) country requesting legal assistance does not provide reciprocal legal assistance,

(3) the request refers to an act, which is not a crime in the light of Polish legal system.

4. Prosecution undertaken upon the request of the court or public prosecutor of a foreign country, shall be governed the provisions of the Polish legislation. Wishes and needs of these bodies should be taken into account, should they request that a particular course of action of specific form is applied while carrying out prosecution activities if it is not incompliant with the legal order of the Republic of Poland.

5. The costs of providing such legal assistance shall be determined in accordance with Articles 616-619.

***Article 589.** 1. A witness or expert, who is not of Polish citizenship and has been summoned from abroad, and who voluntarily appears in court in person may not be prosecuted, detained or temporarily arrested for a crime which is a subject of the criminal proceedings in question or any other crime committed before crossing the Polish national border. A sentence for such a crime may not be executed on that person either.*

2. A witness or expert shall lose the protection referred to in paragraph 1 above if he/she does not leave the territory of the Republic of Poland within a period of 7 days of the date, when the court expressed an opinion, that his/her presence is no longer required.

3. A witness or expert summoned shall be entitled to the return of travel and accommodation expenses and to a return of lost income, and in case of experts – remuneration for his/her expert opinion.

4. The summons delivered to a witness or expert living abroad should contain an instruction on the content of provisions of paragraph 1-3. A warning on the consequences of the application of coercive measures applicable in case of non-appearance.

***Article 589a** 1. A person subject to custodial sentence in the territory of a foreign country, temporarily extradited to take part in a hearing as a witness or to take part in other prosecution activity before a Polish court or public prosecutor, the Regional Court competent for the location, where the activity is to take place shall order the person to be placed in a penal institution or in detention on remand for the time of his/her stay at the territory of the Republic of Poland, not longer, however, than the custodial sentence issued in the extraditing country.*

2. The decision of the court shall not be subject to a complaint.

611. 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.

612. A special unit in the National Prosecutor's Office, the Preliminary Proceedings Supervision Bureau (since 2006 this work is covered by the Bureau of International Legal Co-operation), is primarily responsible for timely and constructive assistance, along with the Ministry of Foreign Affairs and the Ministry of Justice.

613. The provisions on mutual legal assistance are addressed in Article 588 of the Criminal Procedure Code. 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 assessors were assured that this discretionary provision was rarely applied in practice.

614. 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. 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. Moreover, pursuant to Paragraph 232 of "An Instruction on internal organization of public prosecutor's authority offices" set by the Minister of Justice on 28 January 2002, requests for legal assistance are dealt with by the Regional Prosecutor' Office or under the supervision of the Bureau of International Co-operation, which is an additional guarantee of timely execution of the requests. However, under Paragraph 4 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 obliged to give priority in the area of international legal cooperation.

615. A request for assistance is not refused on the sole ground that the offence is also considered to involve fiscal matters (and is in line with Criterion 36.4). In the course of execution of foreign requests issues of secrecy or confidentiality do not present obstacles. Pursuant to Article 105 para 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.

616. The powers of competent authorities required under Recommendation 28 are generally available for use in response to requests for mutual legal assistance.

617. 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.

Statistics (Recommendation 32)

618. The National Prosecutor's Office maintains statistics concerning the number of requests for legal assistance sent from Poland and received by Poland in the years 2001-2005 and the following statistics were provided:

	Requests sent	Requests received
2001	1327	535
2002	1475	675
2003	1268	622
2004	1168	681
2005	1116	659

619. However, the Polish authorities informed the evaluators that the National Prosecutor's Office does not keep statistics indicating how many of the aforementioned requests referred to money laundering cases or securing / seizure of property. Also the timescales for responses are not recorded and therefore uncertain.

620. It is unknown whether Poland has taken over money laundering cases from other countries or transferred them.

621. Turning to criteria V.6 and V.7, 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, except that terrorist financing is not currently an autonomous offence in Poland, and the lack of criminality is one of the discretionary bases for denying mutual legal assistance. As noted above, however, the assessors were assured that denial of assistance for such reasons occurs rarely, if ever.

Additional elements

622. The competent judicial authorities have the powers required under Recommendation 28.

Recommendation 37 - Dual criminality relating to mutual legal assistance

623. The provisions on mutual legal assistance are addressed in Articles 585 to 589f of the Criminal Procedure Code. Article 588 para 2 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." Article 588 para 3 provides three circumstances under which assistance may be denied, including the absence of dual criminality. However, the assessors were assured that this discretionary provision was rarely applied in practice.

624. For extradition and those forms of MLA where dual criminality is required, technical differences in the laws do not prevent Poland from rendering assistance.

Recommendation 38 - Confiscation / Freezing

625. Poland has appropriate laws and procedures in place with respect to the identification of such property or proceeds, and in terms of executing valid and final decisions of other states. Poland is party to the Vienna Convention, the Strasbourg Convention and the Palermo Convention - all of which have specific requirements in this regard. Article 585 para 3 of the Criminal Procedure Code constitutes a primary internal basis for affecting foreign requests for identification, freezing and seizure. Seizure will, in line with the Strasbourg Convention, be conducted on the ground of internal procedures (production of things and security of property). Additionally, as a European Union member state, Poland has implemented the European Union framework decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence. Articles 589g to 589w of the Criminal Procedure Code provide for this simplified execution of freezing orders from European Union countries. These articles entered into force on 2 August 2005.

626. Other relevant provisions include:

> ***Article 607.*** *1. The competence to decide on the requests of a foreign country to deliver objects and property constituting exhibits in criminal proceedings or which have been obtained as a result of a crime shall lie in the public prosecutor or the court, depending on the authority ordering the deposition of these objects. The provisions of Article 588, paragraphs 2 and 4, shall be applicable accordingly.*
> *§ 2. Decision on delivery of objects should include a list of objects subject to delivery to foreign country and indicate objects subject to return after completion of the criminal proceedings carried out by the foreign country authorities.*

Article 611d. 1. *If, in the course of proceedings events occur, which justify the issuing of an order for a security on property because of the possible forfeiture of objects or property constituting a material benefit gained as a result of committing a crime, and the objects or elements of property are located within the territory of a foreign country, the court (or public prosecutor in preparatory proceedings) may request – through the Minister of Justice – from a competent authority of that country to secure these objects or property in danger of forfeiture.*

2. If an authority of the foreign country requests for the execution of a valid sentence to secure property, where the property subject to securing is located at the territory of the Republic of Poland, the competent District Court or public prosecutor of the district, where the property is located, shall be competent for securing that property.

Article 611e. *If a person convicted by a court judgment or against whom a legal measure has been ordered with a valid order, shall leave the territory of the country, where he/she was sentenced and enter the territory of the country of his citizenship before he/she serves the sentence or before the measure ordered is executed, the provisions of the present chapter shall apply accordingly. Provisions of Article 611b paragraph 1 (3) and paragraph 2 (2) shall not apply.*

627. Turning to criterion 38.2, a final judgment can be enforced via property of corresponding value. The Polish authorities indicated that if a requesting state identifies property in Poland allegedly belonging to a defendant in the requested country, they can effect the freezing order with a view to a value confiscation order in the requesting state. Under Article 609 para 2 Code of Criminal Procedure and subject to Article 611b para 1 Code of Criminal Procedure a foreign confiscation order can be enforced by a domestic Polish court.

628. No statistical information has been provided with respect to the execution in Poland either of provisional measures on behalf of a foreign country or of the execution of foreign confiscation orders (both property and value based).

629. Poland has no arrangements for coordinating seizure and confiscation actions with other countries.

630. Criterion 38.4 requires countries to consider establishing an asset forfeiture fund into which all or a portion of confiscated property will be deposited and will be used for law enforcement, health, education or other appropriate purposes. At the time of the on-site visit confiscated funds were deposited in the State Budget and a separate asset forfeiture fund was not yet established. However, the evaluators were informed that Poland has considered establishing such a fund, but there is none at present.

631. In Poland, the sharing of confiscated assets between countries when confiscation is directly or indirectly a result of co-ordinated law enforcement actions is possible on the basis of international and bilateral agreements in mutual legal assistance, and it has been done in at least one instance.

Terrorist financing (SR V)

632. There is no difference in the approach of cooperation in the matter, except that terrorist financing is not currently an autonomous offence in Poland, and the lack of criminality is one of the discretionary bases for denying mutual legal assistance. As noted above, however, the assessors were assured that denial of assistance for such reasons occurs rarely, if ever.

Additional elements

633. Foreign non-criminal confiscation orders cannot be recognised and enforced.

6.3.2 Recommendations and comments

634. Poland can provide a wide range of mutual legal assistance and co-operation. However, in the absence of any statistics in respect of mutual legal assistance relating to money laundering and terrorist financing offences, the evaluators cannot comment on either the effectiveness of current provisions or the timeliness of the provision of mutual legal assistance in such cases. 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.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors underlying rating
R.36	**Largely compliant**	Though Poland can provide a wide range of mutual legal assistance the lack of statistics means there is a reserve on effectiveness.
R.37	**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.
R.38	**Largely compliant**	There are provisions 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).
SR.V	**Partially compliant**	Since terrorist financing is currently not an autonomous offence in Poland, that lack of criminality could be used as the basis for denying mutual legal assistance.

6.4 Extradition (R.32, 37 and 39, SR.V)

6.4.1 Description and analysis

635. 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 it has ratified the
    - Council of Europe Convention on Extradition (ETS 24)
    - Additional Protocol to the European Convention on Extradition of (ETS 86)
    - Second Additional Protocol to the European Convention on Extradition (ETS 98)
    - Convention implementing the Schengen Agreement of 19 June 1990

636. Extradition in the Polish legislation is mainly covered by Articles 602-607 of the Criminal Procedure Code (Annex 8).

637. 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, in Chapter 65a ("Requesting European Union Member State for surrender of prosecuted person on the basis of the European

Arrest Warrant") of the Criminal Procedure Code. These Articles (607a-607zc) entered into force on 1 May 2004 (the date of Poland's accession to the European Union).

638. Pursuant to Article 55 of its Constitution, Poland does not extradite its own nationals. Only with respect to European Union countries, and only under certain conditions, is it possible for Poland to extradite one of its nationals. Under Article 607t of the Criminal Procedure Code, such extradition would be possible if the person was surrendered only for the purpose of conducting a criminal proceeding and only if the person was returned to Poland for the execution of any sentence imposed. But it has to be noted that the Polish Constitutional Tribunal with Decision of 27 April 2005 (P 1/05) (Annex 26) stated that "*Article 607t § 1 of the Criminal Procedure Code, insofar as it permits the surrendering of a Polish citizen to another Member State of the European Union on the basis of the European Arrest Warrant, does not conform to Article 55(1) of the Constitution*". Furthermore, the Tribunal ruled that the loss of binding force of Article 607t § 1 shall be delayed for 18 months following the day on which this judgment was published in the Journal of Laws which was on 4 May 2005. Although the aforementioned Constitutional prohibition is currently under review and Article 607t still in force until 3 November 2006, at present it seems practically impossible to extradite Polish nationals[24]. Aside from this uncertain situation concerning the extradition of Polish nationals, money laundering is an extraditable offence.

639. If a country does not extradite its own nationals solely on the grounds of nationality, criterion 39.2b) requires countries – in the case of a request of a country seeking extradition - to submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. In such cases, the competent authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. With respect to this requirement, Poland's laws allow it to undertake its own prosecution. As Poland is a party to the Council of Europe Convention on Extradition (ETS 24), the Polish authorities are - in the case of a request of a requesting Party to this Convention - bound to submit such a case to its competent authorities in order that proceedings may be taken if they are considered appropriate (Article 6 para. 2 of the Convention). Where such a prosecution is undertaken, Poland is able to cooperate on procedural and evidentiary aspects of the prosecution according to its rules governing mutual legal assistance.

640. Pursuant to Article 604 para 1 subsection 2 of the Criminal Procedure Code, Poland cannot extradite a person for conduct that does not constitute an offence in Poland. It could not try such a person in its own courts, either.

641. Consistent with principles of its own domestic law, Poland has procedures in place that allow extradition requests and proceedings relating to money laundering to be handled without undue delay. The execution of all extradition requests is supervised by the Ministry of Justice.

642. The following bilateral treaties have been negotiated:

- Agreement between the Republic of Poland and the Federal Republic of Germany amending and facilitating the appliance of the European Convention of Extradition, signed on 17.07.2003;
- Agreement between the Republic of Poland and the Slovak Republic amending and facilitating the appliance of the European Convention of Extradition, signed on 23.08.1996;

[24] Polish authorities informed the evaluators that the Constitution was amended on 8 September 2006 (entering into force on 7 November 2006) and that this shortcoming no longer applies.

- 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;
- Agreement between the Republic of Poland and the Commonwealth of Australia on extradition**,** signed on 03.06.1998;
- 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;
- 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;
- Agreement between the Republic of Poland and the Republic of Iraq on legal assistance in civil and criminal matters, signed on 29.10.1988;
- Agreement between the Republic of Poland and the Republic of India on extradition , signed on 17.02.2003;
- Agreement between the Republic of Poland and the Democratic People's Republic of Korea Koreańska Republika Ludowo-Demokratyczna on legal assistance in civil, family and criminal matters, signed on 28.09.1986;
- 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;
- 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;
- Agreement between the Republic of Poland and the Kingdom of Morocco on legal assistance in civil and criminal matters, signed on 21.05.1979;
- Agreement between the Republic of Poland and Mongolia on legal assistance in civil, family, labour and criminal matters, signed on 19.10.1998;
- Agreement between the Republic of Poland and the United States of America on extradition, signed on 10.07.1996;
- Agreement between the Republic of Poland and the Syrian Arab Republic on legal assistance in civil and criminal matters, signed on 16.02.1985;
- Agreement between the Republic of Poland and the Tunisian Republic on legal assistance in civil and criminal matters, signed on 22.03.1985;
- 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.

643. Whereas the lack of reciprocity and dual criminality are merely discretionary grounds for the denial of mutual legal assistance under Article 588 of the Criminal Procedure Code, they are mandatory grounds for the denial of extradition under Article 604. The lack of dual criminality is also a mandatory ground for the denial of execution of a foreign judgement under Article 611b. However, with respect to European Union countries, dual criminality does not apply for 33 offences listed in the implementation provisions of the European Union framework decision on the European arrest warrant.

644. There are at least two discretionary grounds for the denial of extradition under Article 604 of the Criminal Procedure Code that might conflict with criterion 37.2: Article 604, para. 2 Subsection 4, which applies if the offence is subject to prosecution on a private charge; and Subsection 5, which applies if the offence in the requesting state is punishable by a term of imprisonment of less than one year. However, these distinctions are discretionary, not mandatory. With respect to European Union countries, there are also a limited number of grounds for discretionary refusal in the provisions implementing the European Union framework decision on the European arrest warrant.

645. Criterion V.4 requires countries to ensure that criteria 39.1 – 39.4 also apply to extradition proceedings related to terrorist acts and terrorist financing. The Polish laws and procedures

relative to the criteria under Recommendation 39 would apply to extradition proceedings relating to terrorist acts, which are defined in Article 2(7) of the Act of 16 November 2000, and to terrorist offences defined in Article 115 (Section 20) of the Penal Code. Whether they would apply in the case of terrorist financing is more problematical, since terrorist financing is not an autonomous offence. The Polish authorities contend that they could apply by resorting to the use of Article 18, Section 3 of the Penal Code ("aiding and abetting"), and thereby treating terrorist financing as the aiding and abetting of a terrorist act. However, this argument has yet to be successfully used in a Polish prosecution, much less in an extradition request.

Additional elements

646. The additional element 39.5 (i.e. simplified procedures of extradition by allowing direct transmission of extradition requests between appropriate ministries; extradition of persons based only on warrants of arrests or judgements; simplified procedures of extradition of consenting persons who waive formal extradition proceedings) would apply in the case of terrorist acts. In the case of terrorist *financing*, the same issue would arise as described above. Under these circumstances, it is difficult to conceive that any person would agree to the use of any simplified procedures, given the fact of so many legal uncertainties in the absence of terrorist financing being an autonomous offence.

647. Poland has some simplified extradition procedures in place, in addition to those in Chapter 65a of the Criminal Procedure Code, implementing the framework decision on European arrest warrants. For example, under some of its international agreements, requests for extradition can be in the form of a request for preventive detention and can be made directly to the Ministry of Justice. Consenting persons may waive formal extradition proceedings in place (Article 603a of the Criminal Procedure Code).

6.4.2 Recommendations and comments

648. Though Poland keeps some principal statistics on legal assistance, there are no statistics available regarding extradition requests for money laundering or financing of terrorism.

649. Poland has implemented the European Arrest Warrant, which introduced a legal basis that – in principle - Polish nationals can be returned within the European Union for money laundering and terrorist financing without a strict application of the dual criminality principle. However, as the Polish Constitutional Tribunal recently stated that the relevant provision of the Criminal Procedure Code, insofar as it permits the surrendering of a Polish citizen to another Member State of the European Union on the basis of the European Arrest Warrant, does not conform to Article 55(1) of the Constitution, it is questionable if it is possible to extradite Polish nationals[25]. Aside from this uncertain situation concerning the extradition of Polish nationals, money laundering is an extraditable offence.

[25] see footnote above.

6.4.3 Compliance with Recommendations 37, 39 and SR.V

	Rating	Summary of factors relevant to Section 6.4 underlying overall rating
R.37	**Largely Compliant**	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.
R.39	**Largely Compliant**	In the absence of statistics it is not possible to determine whether extradition requests are handled without undue delay.
SR.V	**Partially Compliant**	Since terrorist financing is not an autonomous offence, it is also not possible to prosecute the offences set forth in the requests of foreign countries.

6.5 Other forms of international co-operation (R.32, R.40 and SR.V)

6.5.1 Description and analysis

650. Since Poland's accession to the European Union on 1 May 2004, the GIFI cooperates with its counterparts in the European Union Member States on the basis of the Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA). This provides a formal basis for GIFI's cooperation with the nine countries with which Poland did not enter into separate agreements. On this basis, subject to reciprocity and confidentiality, the GIFI exchanges information with FIUs from Austria, Denmark, France, Greece, Hungary, Luxemburg, Malta, Netherlands and Sweden. The cooperation with FIUs from other European Union Member States is being executed according to Memoranda of Understanding (MOUs) concerning cooperation in the exchange of financial intelligence related to money laundering and financing of terrorism. The GIFI cooperates also with counterparts outside the European Union (i.e. Australia, Israel, Ukraine, Republic of Korea, Romania, Russian Federation, Switzerland and the USA) on the basis of MOUs. The GIFI can sign MOUs on its own authority. Currently GIFI has signed 33 MOUs[26]. The signed MOUs are based on the Model of the Egmont Group (the Polish FIU has been a member of the Egmont Group since June 2002) and provide the possibility of exchanging information both spontaneously and upon request, and also in relation to both money laundering and the underlying predicate offences. In 2006, no information was exchanged spontaneously; for the previous years no data of such spontaneous information exchange was available. Many of the bilateral information-exchange agreements entered into by GIFI specifically include terrorist financing as a subject of mutual assistance.

651. The GIFI cooperates with FIUs from other countries of any type by using the rules and terms prepared by the Egmont Group (also using the Egmont Secure Web System, which is used for the sending and answering of requests). Due to the responses of other jurisdictions, all of the requests to the Polish FIU have been answered. The received answers were considered as substantial and informative. The quality and promptness of responses were perceived as average.

652. In 2002, GIFI sent official requests to foreign FIUs on 35 queries concerning domestic and foreign entities suspected of money laundering. Responses were received concerning 15 entities. Foreign FIUs sent GIFI queries concerning 77 domestic and foreign entities suspected of money laundering, and GIFI's responses covered 47 entities. In 2003, GIFI sent official requests to foreign FIUs in 48 cases concerning 104 national and foreign entities suspected of money laundering. Foreign FIUs sent GIFI 46 queries relating to 208 national and foreign entities. In 2004, GIFI sent official requests to foreign FIUs on 102 cases concerning 224 national and foreign entities suspected of money laundering. Foreign FIUs sent 51 requests to GIFI concerning 163 national and foreign entities. In 2005, GIFI sent official requests to foreign FIUs on 155 cases concerning 284 national and foreign entities suspected of money laundering. Foreign FIUs sent 59 requests to the GIFI concerning 164 national and foreign entities. The average response time was said to be three weeks. No requests were refused. Reportedly, the most frequent exchange of information is being developed with the FIUs from Belgium, the Czech Republic, Germany, Lithuania, the Netherlands, the United Kingdom and the USA.

653. Concerning comprehensive statistics on other formal requests for assistance made or received by law enforcement authorities relating to money laundering or terrorist financing, including whether

[26] as of 10 November 2006: 36.

the request was granted or refused, the assessors are not aware of such figures maintained on the part of law enforcement authorities, except for those kept by GIFI.

654. The GIFI is authorised to make inquiries on behalf of foreign counterparts which includes (a) searching its own databases, including information related to suspicious transaction reports; (b) searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

655. According to the AML Act, Poland does not refuse to assist solely on the ground that the request is considered to involve fiscal matters. Poland would also not refuse requests for cooperation on grounds of secrecy laws or confidentiality requirements (other than where legal professional privilege applies) as long as reciprocity applies, which is the main rule concerning international exchange of information.

656. Cooperation of domestic financial supervisors with foreign financial supervisors is enabled by sectoral laws, for the Banking Supervision it is Article 131 par. 2 and 3 of the Banking Act, for the Securities Commission it is Article 20 of the Act on Capital Market Supervision. Details of cooperation on money laundering and terrorist financing are covered by Memoranda of Understanding between Polish and foreign authorities, for example the Banking Supervision Commission has signed Memoranda of Understanding with the Netherlands, Lithuania, Ukraine, the United States. Where there are Memoranda of Understanding, information concerning banking secrecy can be exchanged. The Polish authorities referred to one such exchange with the Isle of Man. However, no statistics were available covering this issue generally.

657. The Polish Law Enforcement Authorities are entitled to co-operate with their foreign counterparts and, if necessary, they can also conduct investigations on behalf of them. The Polish Police can directly exchange information with Police authorities of foreign countries using Europol and Interpol Channels. In the field of combating financing of terrorism, the Polish Police share information with relevant authorities in EU Member States using PWGT (Police Working Group on Terrorism) cryptofax and BdL (Bureau de Liaison) network.

6.5.2 Recommendation and comments

658. The supervisory authorities should keep statistical information on exchange of information with foreign counterparts (including spontaneous exchanges of information).

6.5.3 Compliance with Recommendations 40 and SR.V

	Rating	Summary of factors relevant to Section 6.5 underlying overall rating
R.40	**Largely Compliant**	Broad capacity for exchange by the FIU and supervisory bodies but no data on information exchange between supervisory bodies.
SR.V	**Partially Compliant**	No information in respect of supervisory information exchange provided.

7 OTHER ISSUES

7.1 Resources and Statistics

659. 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 the boxes showing the rating and the factors underlying the rating.

	Rating	Summary of factors relevant to Section 6.5 underlying overall rating
R.30	**Largely compliant**	**Law enforcement:** • More resources for financial investigation and focused money laundering training required. **Financial Supervisory Authorities:** • Not sufficient number of AML/CFT experts, especially in PSEC. • CFT training is needed for financial supervisors, particularly for insurance and securities sector.
R.32	**Partially compliant**	• More detailed statistics should be kept concerning the nature of money laundering investigations, prosecutions and convictions and sentences. • Insufficient statistics to demonstrate the effectiveness of the FIU internally. • More detailed statistical data is required to demonstrate the effectiveness of the law enforcement response. • There is no precise statistical data on the nature of mutual assistance requests, on the time required to handle them, and on predicate offences related to requests. • No statistics regarding extradition requests for money laundering or financing of terrorism. • Lack of statistics on information exchange by supervisory bodies.

IV. TABLES

Table 1: Ratings of Compliance with FATF Recommendations
Table 2: Recommended Action Plan to improve the AML/CFT system
Table 3: Authorities' Response to the Evaluation (if necessary)

1 TABLE 1. Ratings of Compliance with FATF Recommendations

Forty Recommendations	Rating	Summary of factors underlying rating[27]
Legal systems		
1. Money laundering offence	**Largely compliant**	• Some of the legislative provisions need further clarification on the physical aspects of money laundering (conversion, acquisition, possession or use). • Not all essential criteria are 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.
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	**Partially compliant**	• 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

[27] These factors are only required to be set out when the rating is less than Compliant.

		measures and confiscation are needed.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	**Compliant**	
5. Customer due diligence	**Non compliant**	- The AML Act does not cover: • Customer Identification when starting a business relationship; • when carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII; • when the financial institution has doubts about the veracity or adequacy of previously obtained identification data; - Identification requirements do not cover above threshold transactions of electronic money institutions´ customers; - Although there are regulations in respect of proxies, there is no requirement to ascertain beneficial ownership, including no general requirement to identify and verify the identity of the beneficial owner and no requirements to take reasonable measures to determine the natural person with ownership or control over a legal person; - There is no requirement regarding: • the purpose and nature of the business relationship, • ongoing CDD, • enhanced CDD or conducting CDD on existing customers; - There is no requirement not to open accounts when satisfactory CDD cannot be completed; - No requirement to terminate the relationship with an existing customer when the financial institution is unable to comply with CDD.
6. Politically exposed persons	**Non compliant**	Poland has not implemented any AML/CFT measures concerning the establishment of customer relationships with politically exposed persons (PEPs).
7. Correspondent banking	**Non compliant**	Poland has not implemented any AML/CFT measures concerning establishment of cross-border banking relationships.
8. New technologies and non face-to-face business	**Partially compliant**	Financial institutions are not directly required to have policies in place to prevent the misuse of technological developments in ML and TF schemes.
9. Third parties and introducers	**N/A**	As the Polish legislation does not allow for reliance on third parties and introduced business, Recommendation 9 is not applicable.
10. Record keeping	**Partially compliant**	• As the AML Act is only transaction based, there is no guarantee that all necessary documents are kept, e.g. there is no explicit requirement in law or

		regulation to maintain records of the identification data for at least five years following the termination of an account or business relationship. • There is no requirement in law or regulation to keep documents longer than five years if requested by a competent authority.
11. Unusual transactions	**Partially compliant**	Recommendation 11 is only indirectly covered by Polish law.
12. DNFBP – R.5, 6, 8-11	**Non compliant**	• The same concerns in the implementation of Recommendation 5, 6, 8, 10 and 11 apply equally to obliged financial institutions and DNFBP (see section 3 of the report). • CDD requirements do not apply to accountants and do not fully apply to real estate agents, counsels, legal advisers and foreign lawyers.
13. Suspicious transaction reporting	**Partially compliant**	There is a direct mandatory reporting requirement in the AML Act, though • attempted transactions not covered; • financing of terrorism only partially covered, though reports had been received; • low number of reports outside the banking sector raises issues of effectiveness of implementation.
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 sector) are obliged to have an 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. DNFBP – R.13-15 & 21	**Non compliant**	• The same deficiencies in the implementation of Recommendations 13-15 and 21 in respect of financial institutions apply equally to DNFBP. • Some institutions like casinos are quite unconcerned about ML/FT risks in their field and others, like lawyers, tax advisers and auditors do not accept their obligations. This also results in the small numbers of STR from the DNFBP sector.
17. Sanctions	**Partially compliant**	• Few sanctions have been imposed which questions the effectiveness of the sanctioning system. • The sanction regime is disproportionate for

		minor cases which carries the risk that it is not applied and reduces its effectiveness. • Not all supervisory authorities are aware of their reporting obligations concerning violations of the AML Act by the obliged entities to the Prosecution authorities.
18. Shell banks	**Partially compliant**	There is no legally binding prohibition on financial institutions to enter or continue correspondent banking relationships with shell banks nor is there any obligation on financial institutions to satisfy themselves that a respondent financial institution in a foreign country is not permitting its accounts to be used by shell banks.
19. Other forms of reporting	**Compliant**	
20. Other DNFBP and secure transaction techniques	**Compliant**	
21. Special attention for higher risk countries	**Non compliant**	No obligation in law or regulation or other enforceable means to • pay close attention to any country that fails or insufficiently applies FATF recommendations. • examine the background and purpose of transactions connected with such countries if those transactions have no apparent economic or visible lawful purpose. • have written findings available to assist competent authorities and auditors.
22. Foreign branches and subsidiaries	**Non compliant**	• There is no explicit obligation for foreign branches and no obligation for subsidiaries to observe AML/CFT measures consistent with Polish requirements and the FATF recommendations to the extent that host country's laws and regulations permit. • There is no requirement that particular attention has to be paid to branches and subsidiaries in countries which do not or insufficiently apply FATF recommendations and that the higher standard has to be applied in the event that the AML/CFT requirements of the home and host countries differ.
23. Regulation, supervision and monitoring	**Partially compliant**	• No sector specific regulation has been issued by financial supervisors; the PSEC is not even empowered to do so. • Due to the very reduced involvement of some supervisors (only onsite visits based on a list of formalistic criteria which do not cover adequately the full range of issues related to AML/CFT, such as internal risk management systems and analysis of suspicious patterns, monitoring, etc.) and their explicit unwillingness

		to be involved in training and regulation/guidelines, the system is not fully operational and satisfactory in practice. • Natural and legal persons providing a money or value transfer service are not licensed or registered; apart from banks and the Polish Post, they are not subject to an effective system for monitoring and ensuring compliance with AML/CFT requirements. • The current registration system for Cooperative Savings and Credit Unions is not in line with the Basel Core Principles licensing requirements. • Financial supervisors should not only check formal compliance with the AML Act but also overall effectiveness of the AML/CFT systems in the financial institutions. • Inspections of Insurance and Pension Funds Supervision Commission do not cover CFT issues. • The PSEC inspections of the AML/CFT area are purely formal.
24. DNFBP - Regulation, supervision and monitoring	**Partially compliant**	More controls, and concurrently more resources would be needed to ensure compliance of DNFBP with AML/CFT requirements.
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	**Compliant**	
27. Law enforcement authorities	**Partially compliant**	There are designated law enforcement authorities but more emphasis should be placed on Police generated money laundering cases by proactive financial investigation in major proceeds-generating cases.
28. Powers of competent authorities	**Compliant**	
29. Supervisors	**Largely compliant**	Complex AML/CFT on-site inspections including the review of policies, procedures and sample testing are missing, particularly in the securities sector.
30. Resources, integrity and training	**Largely compliant**	**Law enforcement:** • More resources for financial investigation and focused money laundering training required. **Financial Supervisory Authorities:** • Not sufficient number of AML/CFT experts, especially in PSEC. • CFT training is needed for financial supervisors,

		particularly for insurance and securities sector.
31. National co-operation	**Partially compliant**	Existing coordination measures are not completely effective. It would be helpful to have more coordination of the main AML/CFT players to ensure a consistent approach.
32. Statistics	**Partially compliant**	• More detailed statistics should be kept concerning the nature of money laundering investigations, prosecutions and convictions and sentences. • Insufficient statistics to demonstrate the effectiveness of the FIU internally. • More detailed statistical data is required to demonstrate the effectiveness of the law enforcement response. • There is no precise statistical data on the nature of mutual assistance requests, on the time required to handle them, and on predicate offences related to requests. • No statistics regarding extradition requests for money laundering or financing of terrorism. • Lack of statistics on information exchange by supervisory bodies.
33. Legal persons – beneficial owners	**Partially Compliant**	• 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.
34. Legal arrangements – beneficial owners	**N/A**	As the Polish system does not allow to establish a (foreign or domestic) trust, Recommendation 34 is not applicable.
International Co-operation		
35. Conventions	**Partially compliant**	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.
36. Mutual legal assistance (MLA)	**Largely compliant**	Though Poland can provide a wide range of mutual legal assistance the lack of statistics means there is a reserve on effectiveness.
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 provisions 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	**Largely Compliant**	Broad capacity for exchange by the FIU and supervisory bodies but no data on information exchange between supervisory bodies.
Nine Special Recommendations		
SR.I Implement UN instruments	**Partially compliant**	Poland has ratified the Terrorist Financing Convention but failed to implement several of its provisions, notably a full terrorist financing offence and the European Union mechanisms for freezing under the UNSC Resolutions need supplementing by domestic procedures for European internals.
SR.II Criminalise terrorist financing	**Non compliant**	The Polish authorities rely on the possibility of proceeding for aiding and abetting an offence of terrorist character as indicated in Article 115 para. 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 para. 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.
SR.III Freeze and confiscate terrorist assets	**Partially compliant**	• The definition of funds (deriving from the European Commission Regulations) does 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 is 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 is 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 Act dealing with terrorist financing issues is unclear.
SR.IV Suspicious transaction reporting	**Partially compliant**	Reporting obligation in respect of financing of terrorism insufficiently wide.
SR.V International co-operation	**Partially compliant**	• Since terrorist financing is currently not an autonomous offence in Poland, that lack of criminality could be used as the basis for denying mutual legal assistance. • Since terrorist financing is not an autonomous offence, it is also not possible to prosecute the offences set forth in the requests of foreign countries. • No information in respect of supervisory information exchange provided.
SR.VI AML requirements for money/value transfer services	**Non compliant**	• No system in place of registering and/or licensing MVT service operators. • MVT service operators are not subject to the applicable FATF Recommendations. • There is only indirect monitoring of MVT service operators with regard to compliance with the FATF recommendations. • There are no sanctions applicable to MVT service operators.
SR.VII Wire transfer rules	**Non compliant**	Although some elements exist in practice, Poland has not implemented SR VII.
SR.VIII Non-profit organisations	**Non compliant**	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.

SR.IX Cash Couriers	**Largely compliant**	• More targeted co-operative enquiries are encouraged. • More sensitisation to terrorist financing issues is required.

2 TABLE 2: RECOMMENDED ACTION PLAN TO IMPROVE THE AML/CFT SYSTEM

FATF 40+9 Recommendations	Recommended Action (listed in order of priority)
1. General	
2. Legal System and Related Institutional Measures	
Criminalisation of Money Laundering (R.1 and 2; R. 32)	• Clarify legislative provisions to ensure that all physical and material aspects of money laundering (conversion, acquisition, possession or use) are covered. • Conspiracy to commit money laundering should be recognised as a criminal offence, unless this is not permitted by fundamental principles of domestic law. • Financing of terrorism in all its forms, as explained in the Interpretative Note to SR.II, should be clearly covered as predicate offences to money laundering. • Clarify in the criminal law that property being proceeds covers both direct and indirect property which represent the proceeds (or benefits) of the crime. • The evaluators advise to set out in legislation or guidance that knowledge (the intentional element) can be inferred from objective factual circumstances. • More emphasis should be placed on autonomous prosecution of money laundering by third parties. • 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. • The Polish authorities are encouraged to use the new powers providing corporate criminal liability proactively in money laundering cases. • More detailed statistics should be kept concerning the nature of money laundering investigations, prosecutions and convictions and sentences.
Criminalisation of Terrorist Financing (SR.II)	• An autonomous offence of terrorist financing should be introduced which explicitly addresses all the essential criteria in SR.II and requirements of the Interpretative Note to SR.II.
Confiscation, freezing and seizing of proceeds of crime (R.3; R. 32)	• The confiscation regime should clearly allow for confiscation of instrumentalities which have been transferred to third parties. • More statistics on provisional measures and confiscation is needed.
Freezing of funds used for terrorist financing (SR.III)	• A clear legal mechanism to act in relation to European Union internals should be introduced. • Guidance should be given to all financial intermediaries, DNFBP and the general public. • A clear and publicly known procedure for de-listing and

	unfreezing in appropriate cases in a timely manner should be developed. • A general administrative regime for the implementation of SR.III should be considered.
The Financial Intelligence Unit and its functions (R.26, 30 and 32)	• The FIU should further seek outreach to some parts of the financial sector (particularly exchange houses) and DNFBP (particularly casinos) to explain the concept of suspicion in more detail. Additionally, they should consider publishing more periodic reports with statistics, typologies and trends, as well as information about its activities. • More statistics (e.g. processing times) should be kept to demonstrate the effectiveness of the FIU internally.
Law enforcement, prosecution and other competent authorities (R.27, 28, 30 and 32)	• More emphasis should be placed on Police generated money laundering cases by proactive financial investigation in major proceeds-generating cases. • More use should be made of joint teams and co-operative investigations with the GIFI. • A specialised money laundering Unit with dedicated officers and financial investigators trained in modern financial investigative techniques should be considered to improve the performance of the Police in generating money laundering cases outside of the reporting regime. • More focused training is required of the Police and prosecutors in difficult evidential issues in money laundering cases; more officers should be trained in modern financial investigation. • More resources for financial investigation and focused money laundering training should be provided. • More detailed statistics should be kept to demonstrate the effectiveness of the law enforcement regime overall. Statistics need enhancing to ensure that those reviewing the system have a clearer picture of the types of money laundering cases that are being brought, whether they are prosecuted as autonomously or as self laundering, seize and number of confiscation orders and whether freezing occurs at early stages to prevent proceeds being dissipated.
Cross Border Declaration or Disclosure (SR.IX)	• Customs (and Border Guards) should be fully sensitized to all the issues involved in financing of terrorism.
3. Preventive Measures– Financial Institutions	
Risk of money laundering or financing of terrorism	
Customer due diligence, including enhanced or reduced measures (R.5, R.7)	• Financial institutions should be clearly required to identify customers when starting a business relationship, when carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII and when the financial institution has doubts about the veracity or adequacy of previously obtained identification data. • Identification requirements concerning above threshold

	transactions should be applicable also to customers of electronic money institutions. • The Polish authorities should introduce the concept of beneficial owner as it is described in the Glossary to the FATF Recommendations. Financial institutions should be required to take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from a reliable source. • Financial institutions should be required to obtain information on the purpose and intended nature of the business relationship. • Financial institutions should be required to conduct on-going due diligence on the business relationship and to ensure that documents, data or information collected under CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships. • Financial institutions should be required to perform enhanced due diligence for higher risk categories of customers, business relationship or transaction, including private banking, companies with bearer shares and non-resident customers. • Polish authorities should satisfy themselves that branches with headquarters abroad undertake the CDD process themselves as it is required by Polish Law and do not rely on their headquarters (as the Polish Law does not allow relying on third parties). • Financial institutions should not be permitted to open an account when adequate CDD has not been conducted. Where the financial institution has already started the business relationship and is unable to comply with CDD it should be required to terminate the business relationship. In both situations mentioned above financial institutions should be required to consider making a suspicious transaction report. • Financial institutions should be required to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times. • It is recommended that Poland implements legislation to deal with cross-border correspondent banking relationships.
(R.6)	• Poland should implement legislation to deal with PEPs.
(R.8)	• Financial institutions should be required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering and terrorist financing schemes.
(R.9)	As the Polish legislation does not allow for reliance on third parties and introduced business, Recommendation 9 is not applicable.
Record keeping and wire transfer	• The text of the law should clearly state that all necessary identification data has to be kept for at least five years

rules (R.10 and SR.VII)	after the end of the business relationship as required by Recommendation 10. • Financial institutions should be required to keep documents longer than five years if requested by a competent authority. • Poland should implement the whole concept of SR.VII
Monitoring of transactions and relationships (R.11 and 21)	• The examiners strongly recommend to address all the subcriteria of Recommendation 11; particularly financial institutions should be required 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, to examine as far as possible the background and purpose of such transactions and to set forth such findings in writing and to keep them available for competent authorities and auditors for at least five years. • A requirement to pay special attention to business relationships and transactions with persons from countries that do not or insufficiently apply the FATF Recommendations should be introduced. • Financial institutions should be also required to examine the background and purpose of transactions connected with such countries if those transactions have no apparent economic or visible lawful purpose. Written findings should be available to assist competent authorities and auditors.
Suspicious transaction reports and other reporting (R.13 and 14, 19, 25 and SR.IV)	• More guidance is needed to ensure that reporting entities place sufficient emphasis on the STR regime (as opposed to the above-threshold reporting regime). • More attention should be given to outreach to other parts of the financial and non banking financial sector to ensure that they are reporting adequately. • The AML Act should clearly provide for attempted suspicious transactions to be reported. • More guidance is required on the width of the financing of terrorism reporting obligation. • The reporting duty needs to be explicitly clarified in the law to include all funds where there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism. • It would be helpful to state explicitly in the law that all financial institutions, directors, officers and employees should be protected from both criminal and civil liability for breach of any restriction on bona fide disclosures of information. • The tipping off provision should clearly cover the transmission of related information, as well as the fact of reporting.
Internal controls, compliance, audit and foreign branches (R.15 and 22)	• The AML/CFT compliance officer and other appropriate staff should have timely access to customer identification data and other relevant information. • All financial institutions (not only the banking and

	securities sector) should be obliged to have an internal audit function, which also covers AML/CFT policies. • Financial institutions should be required to establish screening procedures to ensure high standards when hiring employees. • Poland should implement an explicit obligation to require financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with the Polish requirements and FATF recommendations. It should add provisions to clarify that particular attention has to be paid to branches and subsidiaries in countries which do not or insufficiently apply the FATF recommendations and that the higher standard have to be applied in the event that the AML/CFT requirements of the home and host country differ.
Shell banks (R.18)	• Poland should implement provisions with regard to a prohibition on financial institutions to enter or continue correspondent banking relationship with shell banks. • Financial institutions should be obliged to satisfy themselves that a respondent financial institution in a foreign country is not permitting its accounts to be used by shell banks.
The supervisory and oversight system – competent authorities and SROs / Roles, functions, duties and powers (including sanctions) (R.17, 23, 29 and 30)	• The evaluators advise to introduce an additional regime of complementary administrative sanctions such as fines to enhance the AML/CFT compliance, especially in the non financial sector. • The competences of the sanctioning authorities should be clarified to avoid double or no sanctioning; legal clarification is needed and working arrangements between the FIU and the supervisory authorities on sanctioning should be set out, preferably by Memoranda of Understanding and greater practical co-ordination. • Sector specific regulation should be issued by the financial supervisors (including the PSEC which should be also empowered to do so). • The engagement of the prudential supervisors in AML/CFT supervision should be enhanced. • The financial supervisors, particularly the PSEC, shall apply all necessary on-site tools (review of policies, procedures, books and records including sample testing) also in the AML/CFT area. • More AML/CFT experts are needed within the financial supervisory framework, particularly in PSEC, to be able to cover the complex issue of AML/CFT (supervision, regulation and guidance). • CFT training is needed for financial supervisors, particularly for insurance and securities sector.
Financial institutions – market entry and ownership/control (R.23)	• A licensing or registering system should be introduced for MVT services as well as an effective system for monitoring and ensuring compliance with the AML/CFT requirements. • A licensing system as it is understood by the Basel Core Principles should be introduced for Cooperative Savings

	and Credit Unions.
AML/CFT Guidelines (R.25)	• The financial supervisors should consider issuing sector-specific AML/CFT guidance.
Ongoing supervision and monitoring (R23, 29)	• Financial supervisors should not only check formal compliance with the AML Act but also overall effectiveness of the AML/CFT systems in the financial institutions. • Inspections of the Insurance and Pension Funds Supervision Commission should cover CFT issues. The PSEC inspections of the AML/CFT area are purely formal and should be enhanced. • The evaluators recommend that the questionnaire of the PSEC should explicitly address CFT issues.
Money or value transfer services (SR.VI)	• Poland should implement Special Recommendation VI.
4. Preventive Measures – Designated Non-Financial Businesses and Professions	
Customer due diligence and record-keeping (R.12)	• The evaluators recommend working with the different sectors to improve awareness, and overcome any unwillingness to apply AML/CFT requirements. Information campaigns to this end are required. Polish authorities should continue its efforts in this direction, by offering training, publications etc. • Poland should fully implement Recommendations 5, 6, 8, 10 and 11 and make these measures applicable to DNFBP. • Real estate agents, counsels, legal advisers and foreign lawyers should be required to apply CDD measures in all relevant situations according to the FATF Recommendations and not only in the case of suspicious transactions. Accountants should also be covered by these obligations.
Monitoring of transactions and relationships, internal controls, compliance and audit (R. 16)	• Poland should fully implement Recommendations 13-15 and 21 in respect to DNFBP.
Regulation, supervision and monitoring (R.17, 24-25)	• The evaluators advise to introduce an additional regime of complementary administrative sanctions such as fines to enhance the AML/CFT compliance. • The competences of the sanctioning authorities should be clarified to avoid double or no sanctioning; legal clarification is needed and working arrangements between the FIU and the supervisory authorities on sanctioning should be set out, preferably by Memoranda of Understanding and greater practical co-ordination.
Other designated non-financial businesses and professions (R.20)	
5. Legal Persons and Arrangements and Non-profit Organisations	
Legal Persons–Access to beneficial ownership and control information	• It is recommended that Poland reviews its commercial, corporate and other laws with a view to taking measures to

(R.33)	provide adequate transparency with respect to beneficial ownership. • 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.
Legal Arrangements–Access to beneficial ownership and control information (R.34)	
Non-profit organisations (SR.VIII)	• It is recommended to undertake a formal analysis of threats posed by the NPO-sector as a whole and then to 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. • Consideration should be given to the issuing of guidance to financial institutions on the specific risks of this sector, and of whether and how further measures need to be taken in the light of the Best Practices Paper for SR.VIII. Consideration might usefully be given as to whether and how any relevant private sector watchdogs could be utilised. • It would be helpful 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	
National Co-operation and Co-ordination (R.31)	• It is recommended to have more coordination of the main AML/CFT players to ensure a consistent approach. The work of the intergovernmental Working Group should be continued and additionally be raised to a more senior strategic level to include other key stakeholders.
The Conventions and UN Special Resolutions (R.35 and SR.I)	• Poland should (effectively) implement all the provisions of the relevant international conventions it has ratified; *inter alia* it should introduce a full terrorist financing offence and supplement the European Union mechanisms for freezing under the UNSC Resolutions by domestic procedures for European internals.
Mutual Legal Assistance (R.32, 36-38, SR.V)	• More statistical data (e.g. nature of mutual assistance requests; the time required to handle them; type of predicate offences related to requests) is needed to show the effectiveness of the system.
Extradition (R.32, 37 and 39, and SR.V)	• Poland should maintain statistics regarding extradition requests for money laundering or financing of terrorism including the time required to handle them. • All kinds of financing of terrorism offences should be made extraditable also for non-EU-countries.
Other forms of co-operation (R.32)	• The National Prosecutor's Office and other relevant authorities should consider to maintain statistical data of the mutual legal assistance requests referring to money laundering cases, or securing / seizure of property on request of foreign countries and on request of Polish authorities.

3 TABLE 3. AUTHORITIES' RESPONSE TO THE EVALUATION (IF NECESSARY)

Relevant sections and paragraphs	Country Comments

ANNEXES

ANNEX I

(Details of all bodies met on the on-site mission – Ministries, other government authorities or bodies, private sector representatives and others).

- General Inspector of Financial Information (GIFI)
- Ministry of Justice (Bureau of Organized Crime, Bureau of Preparatory Proceeding, Department of International Cooperation and European Law, National Court Register)
- Ministry of Finance (Department of Financial Information, Custom Excise Tax Audit Department, Fiscal Control Department, Games of Chance and Betting Department, Financial Institutions Department)
- Ministry of Foreign Affairs (Department of Legal and Treaty Issues, Department of European Union, Department of Foreign Economy Policy, Bureau of the General Director)
- Polish Securities and Exchange Commission
- Notaries, real estate agents, lawyers, barristers, tax advisors, statutory auditors
- General Headquarter of Police (Central Investigation Bureau, Criminal Bureau, Department of Security and Public Order, Department of Corruption and Organized Crime Counteracting)
- Judges
- General Inspectorate of Banking Supervision
- National Bank of Poland
- Commission for Insurance and Pension Funds Supervision
- Representatives from commercial banks, co-operative savings and Credit Banks
- Polish Bank Association
- Polish Post
- Representatives from Brokerage Houses
- Casino Poland
- Head of Polish delegation to MONEYVAL

ANNEX II

Designated categories of offences based on the FATF Methodology	Offence by the Criminal Code of Poland (unless otherwise noted)
Participation in an organised criminal group and racketeering;	Article 258
Terrorism, including terrorist financing	Articles 299, 282
Trafficking in human beings and migrant smuggling;	Article 253
Sexual exploitation, including sexual exploitation of children;	Article 199 to 201
Illicit trafficking in narcotic drugs and psychotropic substances;	Articles 53 to 67
Illicit arms trafficking	Article 263
Illicit trafficking in stolen and other goods	Articles 291 and 292
Corruption and bribery	Articles 228 to 231
Fraud	Article 286
Counterfeiting currency	Article 310
Counterfeiting and piracy of products	Articles 303 to 308
Environmental crime	Article 181 to 188
Murder, grievous bodily injury	Articles 148, 156
Kidnapping, illegal restraint and hostage-taking	Articles 189, 123, 252
Robbery or theft	Articles 278, 280
Smuggling	Article 86 of the Fiscal Penal Code
Extortion	Article 191
Forgery	Article 270
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