Ministerstwo
Finansów

ANNEX NO. 1
THE METHODOLOGY OF DRAWING UP OF THE FIRST POLISH NATIONAL ASSESSMENT OF THE RISK OF MONEY LAUNDERING AND FINANCING OF TERRORISM

Introduction

According to Recommendation no. 1 of the Financial Action Task Force (FATF): „Countries should identify, assess, and understand the money laundering and financing of terrorism risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and financing of terrorism are commensurate with the risks identified".[1]

The fundamental objectives of such analyses are the indication of possible changes to the domestic system of combating money laundering and financing of terrorism, including changes to the law, as well as the determination of a suitable assignment of resources and determination of priorities of their use. Their periodic updating is also required. The results of these analyses should be made available to obliged institutions in order to simplify for them the execution of their assessment of the risk of money laundering and financing of terrorism.

Directive 2018/849[2] also obliges all entities engaged in combating money laundering and financing of terrorism to act based on risk analyses. One of the components of this policy is to recommend to European Union (EU) member states to undertake actions in order to „identify, assess, understand and mitigate the risks of money laundering and financing of terrorism" that are significant from the point of view of that member state. Such a risk assessment is to be updated regularly.

Considering the above, *the act of 1 March 2018 on counteracting money laundering and terrorist financing* (Journal of Laws of 2019, item no. 1115), includes provisions setting out the basic rules of preparation and updating of the national assessment of risk of money laundering and financing of terrorism (referred to in the text as the National Risk Assessment) and the strategy based upon it. They foresee that it is the General Inspector of Financial Information (GIFI) who develops this assessment and this strategy in cooperation with the

[1] International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, updated as of October 2018, p. 9 at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

[2] *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or financing of terrorism, amending Regulation (EU) no. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJEU L 141, of 05.06.2015., p. 73).*

Financial Security Committee, cooperating units, as well as obliged institutions. The National Risk Assessment is to be drawn up within 12 months from the date of the act entering into force.

Risk identification method

The FATF publication entitled „National Money Laundering and Financing of Terrorism Risk Assessment" indicates that there is no single, common methodology of conducting an assessment of the risk of money laundering. It depends mainly on the objectives and the scope of risk assessment[3].

Usually, money laundering (ML) and financing of terrorism (TF) risk assessment methods are based on the identification of three components, on the basis of which the risk is assessed: the threat, vulnerability and consequences (with probability being additionally indicated, understood as the function of threat and vulnerability). The fundamental difference between them entails the mode of their identification, in particular with respect to threat.

In terms of methodologies developed by the World Bank or the International Monetary Fund, threat identification is effected on the basis of a list of predicate offences for money laundering (additionally, the estimated volume of resources stemming from these crimes), the directions of flaw of illegal funds, the techniques of ML and their development trends. In terms of the assessment of risk of TF, threat identification takes place by reference to the terrorism threat assessment as well as information concerning identified sources of funds foreseen for TF (both legal and illegal) and the modes of their transfer.

The European Commission, working to develop a supranational risk assessment concerning ML and TF, focused in turn on the list of *modi operandi* used to perpetrate these crimes. The scenarios of criminal actions indicated in this list are then subjected to an assessment of threat understood as the evaluation of plans and capabilities of criminals to use them, as well as of vulnerability understood as the evaluation of means to counter them. In its methodology, the European Commission[4] has stated that the consequences of ML and TF will not be the subject of a detailed risk assessment. In this regard, it assumed that ML and TF generate fixed, significant, negative effects for transparency, good management and the reputation of public and private institutions operating in the EU and cause significant damage to the domestic security of EU member states and the EU economy.

For the purpose of the National Risk Assessment of ML and TF the following intermediate method was adopted, encompassing:

- the assessment of „basic risk" separately for ML and TF, in particular on the basis of evaluation of threats related to products and services offered on the market, estimates of the asset value subject to money laundering or being the object of financing of terrorism, information on the mode of operation of bodies encompassed by the national domestic system of anti-money laundering and countering the financing of terrorism (AML/CFT), statistical data concerning their operation, relevant legal provisions and their application;

---

3 National Money Laundering and Financing of Terrorism Risk Assessment, FATF, February 2013, p. 9.

4 Commission staff working document accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and financing of terrorism affecting the internal market and relating to cross-border situations, European Commission, Brussels, 26.06.2017, p. 235 (Annex 3 – Methodology for assessing money laundering and financing of terrorism risks affecting the internal market and related to cross-border activities), at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

- the assessment of „residual risk" related to the list of *modi operandi* (also separately for ML and TF*)*, compiled on the basis of both domestic as well as foreign experiences (similarly to the mode developed by the European Commission);
- the assessment of general risk separately for ML and TF, on the basis of the two assessments described above.

Assessing the risk of ML - assumptions

„Basic risk" of ML

The basic risk of ML for the assessment of „basic risk" shall be assessed according to the scheme set out in table no. 1.

Tab. no. 1 – ML threat levels for the purpose of assessment of „basic risk"

Threat level	**Threat level properties** ***(in order to assign a relevant threat level, conditions need to be met of at least two of the four assigned items)*** [5]
Low threat (1 p.)	1) The level of assessment of asset values from illegal activity (derived in Poland or transferred to Poland and stemming from crimes perpetrated abroad) per year: x < 0.05%*GDP 2) Assessment of the threat for Poland by crime generating profit (e. g. predicate offences for money laundering) as being low (inter alia on the basis of analyses of economic crime, corruption, illegal trade and trafficking of drugs, weapons, people, etc.). 3) ML risk level in the EU evaluated as low. 4) Poland is not indicated in known risk assessments of other countries as one of the countries, from which illegal asset values stem or to which these are transferred.
Medium threat (2 p.)	1) The level of assessment of asset values from illegal activity (derived in Poland or transferred to Poland and stemming from crimes perpetrated abroad) per year: 0.05%*GDP < x < 0.5%*GDP 2) Assessment of the threat for Poland by crime generating profit (e. g. predicate offences for money laundering) as being moderate/ medium (e. g. on the basis of analyses of economic crime, corruption, illegal trade and trafficking of drugs, weapons, people, etc.). 3) ML risk level in the EU evaluated as moderate/ medium. 4) Poland is indicated in known risk assessments of other countries as one of the countries, from which illegal asset values stem or to which these are transferred.
High threat (3 p.)	1) The level of assessment of asset values from illegal activity (derived in Poland or transferred to Poland and stemming from crimes perpetrated abroad) per year: 0, 5%*GDP < x < 1%*GDP 2) Assessment of the threat for Poland by crime generating profit (e. g. predicate offences for money laundering) as being high (e. g. on the basis of analyses of economic crime, corruption, illegal trade and trafficking of drugs, weapons, people, etc.). 3) ML risk level in the EU evaluated as high. 4) Poland is indicated in known risk assessments of other countries as one of the main countries, from which illegal asset values stem or to which these are transferred.
Very high threat (4 p.)	1) The level of assessment of asset values from illegal activity (derived in Poland or transferred to Poland and stemming from crimes perpetrated abroad) per year: x > 1%*GDP 2) Assessment of the threat for Poland by crime generating profit (e. g. predicate offences for money laundering) as being very high (e. g. on the basis of analyses of economic crime, corruption, illegal trade and trafficking of drugs, weapons, people, etc.). 3) ML risk level in the EU evaluated as very high. 4) Poland is indicated in known risk assessments of other countries as the main country, from which illegal asset values stem or to which these are transferred.

The level of vulnerability to ML to the evaluation of „basic risk" will be assessed according to the scheme set out in table no. 2.

[5] In case conditions are met from a lower and an upper level it is possible to average them out (e. g. from the low and the high threat levels – to the medium threat level).

Table no. 2 – ML vulnerability levels to the assessment of „basic risk"

Vulnerability level	**Vulnerability level characteristics** ***(in order to assign a relevant risk level, conditions should be met that are set out in at least four of six items assigned to it)*** [6]
Low vulnerability (1 p.)	1. The vulnerability of the economy is low. a) With respect to products and services: – Lack or relatively low volume of products and services facilitating quick and anonymous transactions. – Secured and monitored channels of flow of financial resources. – Relatively low volume of financial transactions, including cash transactions, as well as others, which may facilitate anonymity of originators and beneficiaries. – Relatively low volume of international transactions. b) With respect to entities offering these products and services: – All categories of entities that should be obliged institutions (OI) are subject to provisions in the scope of anti-money laundering and countering the financing of terrorism (AML/CFT) and oversight of public authorities in this regard. – OI are appropriately aware of their obligatory duties in terms of AML/CFT. No or relatively limited indications of the possible lack of compliance of the operation of OI with these provisions. – According to supervisory bodies, OI efficiently analyse transactions and apply Customer Due Diligence measures (CDD), and report information on their suspicions to Polish Financial Intelligence Units (PFIU) – none or rare cases of administrative penalties imposed for lack of compliance of OI with AML/ CFT provisions 2. The level of activity of OI supervisory bodies is high. a) Supervisory bodies have sufficient human and financial resources as well as hardware to conduct OI inspections. b) The results of conducted inspections form the basis to impose administrative penalties and to apply other supervisory measures over OI not adhering to AML/CFT provisions. c) All supervisory bodies provide information on the executed inspections to the PFIU. d) The level of cooperation with other domestic and foreign supervisory bodies is at high level. 3. PFIU operates at high level. a) PFIU has very good awareness of risk in terms of ML/TF. b) Relatively high capacity of PFIU to collect and analyse information on suspicious activities/transactions (assessed on the basis of the permits, human resources, hardware and finances held): – PFIU has direct access to all databases of public authorities required to analyse information on suspicious activities/transactions. – PFIU is empowered to receive from OI and cooperating units (CU) additional information upon request. – Analysts are trained in conducting analyses. – PFIU has sufficient human resources to execute tasks in the area of CFT. – PFIU has a computer system permitting efficient reception, collection and analyses of information on suspicious activities/transactions. – PFIU operations are financed in a manner sufficient for their needs. c) The level of international cooperation of PFIU with their foreign counterparts is good: – Replies provided by the PFIU are not limited in terms of the scope and type of data. – The average PFIU response time does not exceed three days calculated from the day of receipt of the inquiry. – Information received from the majority of foreign FIUs is not limited in terms of the scope and type of data, and the average time of their receipt does not exceed three days from the day of transfer of the inquiry. – PFIU has and uses electronic communication channels for fast and secure information exchange with all FIUs, with which it exchanges information, – PFIU exchanges information with all FIUs operating in the Egmont Group. d) The level of domestic cooperation of PFIU is good: – Replies provided by the PFIU are not limited in terms of the scope and type of data or the type of law enforcement or judicial authority. – The average PFIU response time does not exceed three days from the day of receipt of the inquiry.

[6] In case conditions are met from a lower and an upper level it is possible to average them out (e. g. from the low vulnerability and high vulnerability levels – to the medium vulnerability level).

	– Information acquired from authorities is not limited in terms of the scope and type of data, all authorities transfer information within deadlines set out by the GIFI. – PFIU has and uses electronic communication channels for fast and secure exchange of information with all types of law enforcement authorities. 4. The level of activity of law enforcement authorities is high. a) Law enforcement authorities possess very good awareness of risk in terms of ML/TF. b) Law enforcement authorities have relatively high capacity to counteract ML/TF risk (assessed on the basis of the held permits, human, hardware, financial resources): – They are empowered to obtain all information they require during their proceedings. – Have sufficient human resources to execute tasks in the area of CFT. – They have sufficient high-quality equipment to conduct operations. – Their activity is financed sufficiently compared to their needs. c) The level of domestic cooperation between law enforcement authorities is good: – Responses provided by these authorities are not limited in terms of the scope and type of data or the type of law enforcement authority. – The authorities have and utilise electronic communication channels for fast and secure exchange of information between each other. d) The level of international cooperation of law enforcement authorities with their foreign counterparts is good: – Responses provided by law enforcement authorities are not limited in terms of the scope and type of data. – The authorities have and utilise electronic communication channels for fast and secure exchange of information with all their foreign counterparts. 5. The level of activity of judicial authorities is good. a) The authorities possess very good awareness of risk in terms of ML/TF. b) Court proceedings take a relatively short time (on average up to a year from the submission of the indictment to court until the sentence is passed in the first instance). 6. The legal system - existing legal provisions correspond to the scope of the analysed risk and the requirements/standards of the EU and FATF recommendations.
Medium vulnerability (2 p.)	1. The level of vulnerability of the economy is medium. a) With respect to products and services: – Limited volume of products and services facilitating quick and anonymous transactions. – The channels of flow of financial resources are in most cases secured and monitored. – Relatively high volume of financial transactions, including cash transactions, as well as others, which may facilitate anonymity of originators and beneficiaries. – Limited volume of international transactions. b) With respect to entities offering these products and services: – Most categories of entities that should be OI, are subject to AML/CFT provisions and oversight of public authorities in this regard. – OI are aware of their obligatory duties in terms of AML/CFT. Rare indications of the possible lack of compliance of the operation of OI with these provisions. – According to supervisory bodies, OI analyse transactions and apply CDD, and report information on their suspicions to PFIU – however, there arise sometimes cases of administrative penalties for lack of compliance of OI with AML/CFT provisions. 2. The level of activity of OI supervisory bodies is good. a) Supervisory bodies have rather sufficient human and financial resources as well as hardware to conduct OI inspections, with occasional shortcomings in this regard. b) The results of conducted inspections form the basis to impose administrative penalties and other supervisory measures over OI not adhering to AML/CFT provisions. c) The majority of supervisory bodies provide information about the executed inspections to the PFIU. d) The level of cooperation with other domestic and foreign supervisory bodies is good. 3. PFIU operates well. a) PFIU possesses good awareness of risk in terms of ML/TF. b) Relatively good capacity of PFIU to collect and analyse information on suspicious activities/transactions (evaluated on the basis of the permits, human resources, hardware and finances held): – PFIU has direct or indirect access to all databases of public authorities required to analyse information on suspicious activities/transactions. – PFIU is entitled to receive from OI and CU additional information upon request. – Most analysts are trained in conducting analyses. – PFIU have sufficient human resources to execute tasks in the area of CFT, with occasional shortcomings in this regard. – PFIU have a computer system allowing reception, collection and analyses of information on suspicious activities/ transactions.

	– The level of activity of PFIU is financed in a manner sufficient for its needs, with occasional shortcomings in this regard. c) The level of international cooperation of PFIU with their foreign counterparts is appropriate: – Replies provided by the PFIU are not limited in terms of the scope and type of data. – The average PFIU response time is longer than three days, but shorter than seven days from the day of receipt of the inquiry. – Information received from most FIUs is not limited in terms of the scope and type of data, and the average time of their receipt is more than three days but not more than seven days from the day of transfer of the inquiry. – PFIU has and uses electronic communication channels for fast and secure exchange of information with the majority of FIUs, with which they exchange information, – PFIU exchanges information with most FIUs operating within the Egmont Group. d) The level of domestic cooperation of PFIU is good: – Replies provided by the PFIU are not limited in terms of the scope and type of data or the type of law enforcement or judicial authority. – The average PFIU response time is longer than three days, but shorter than seven days from the day of receipt of the inquiry. – Information acquired from authorities is not limited in terms of the scope and type of data, most authorities transfer information within deadlines set out by the GIFI. – PFIU has and uses electronic communication channels for fast and secure exchange of information with most types of law enforcement authorities. 4. The level of activity of law enforcement authorities is good. a) Law enforcement authorities have good awareness of risk in terms of ML/TF. b) Law enforcement authorities have good capacity to counteract ML/ TF risk (assessed on the basis of the held permits, human, hardware, financial resources): – They are entitled to obtain most information they require during their proceedings. – Have sufficient personnel resources to execute tasks in the area of CFT, with occasional shortcomings in this regard. – They have sufficient hardware to conduct operations. – Their activity is financed sufficiently compared to their needs, with occasional shortcomings in this regard. c) The level of domestic cooperation between law enforcement authorities is sufficient. – Responses provided by these authorities are not limited in terms of the scope and type of data or the type of law enforcement authority. – The authorities have and utilise electronic communication channels for fast and secure exchange of most information between each other. d) The level of international cooperation of law enforcement authorities with their foreign counterparts is good. – Responses provided by law enforcement authorities are not limited in terms of the scope and type of data. – Most authorities possess and utilise electronic communication channels for fast and secure exchange of information with their foreign counterparts. 5. The level of activity of judicial authorities is good. a) Authorities possess good awareness of risk in terms of ML/TF. b) Court proceedings take a moderate time (on average between a year and two years from the submission of the indictment to court until the sentence is passed in the first instance). 6. The legal system - existing legal provisions mostly correspond to the scope of the analysed risk and the requirements/standards of the EU and FATF recommendations.
High vulnerability (3 p.)	1. The level of vulnerability of the economy is appreciable. a) With respect to products and services: – Relatively high volume of products and services facilitating quick and anonymous transactions. – The channels of flow of financial resources are in many cases neither secured nor monitored. – Relatively high volume of financial transactions, including cash transactions, as well as others, which may facilitate anonymity of originators and beneficiaries. – Relatively high volume of international transactions. b) With respect to entities offering these products and services: – Most categories of entities that should be OI are not subject to provisions of AML/CFT and oversight of public authorities in this regard. – OI are insufficiently aware of their obligatory duties in terms of AML/CFT. Numerous indications of the possible lack of compliance of the operation of OI with these provisions. – According to supervisory bodies, OI analyse transactions and apply CDD, and report information on their suspicions to the PFIU insufficiently – numerous cases of administrative penalties imposed for lack of compliance of OI with AML/ CFT provisions 2. The level of activity of OI supervisory bodies is insufficient.

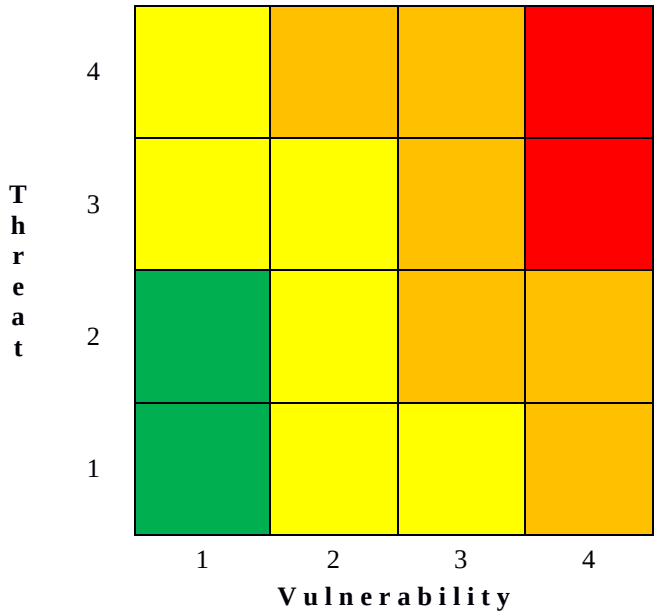
	a) Supervisory bodies have insufficient personnel measures, financial resources and hardware to conduct OI inspections. b) The results of conducted inspections are the basis to impose administrative fines and other supervisory measures over OI not adhering to AML/CFT provisions. c) The majority of supervisory bodies do transfer information about the executed inspections to the PFIU. d) The level of cooperation with other domestic and foreign supervisory bodies is insufficient. 3. PFIU operate insufficiently. a) PFIU possess insufficient awareness of risk in terms of ML/TF. b) Insufficient capacity of PFIUs to collect and analyse information about suspicious activities/ transactions (evaluated on the basis of the permits, human resources, hardware and finances held): – PFIU has direct or indirect access to a part of databases of public authorities required to analyse information about suspicious activities/ transactions. – PFIU does not have sufficient authority to receive from OI and CU additional information upon request. – Only a small fraction of analysts are trained in of analyses. – PFIU has insufficient human resources to execute tasks in the area of CFT. – PFIU have a IT system allowing reception, collection and analyses of information on suspicious activities/ transactions. – PFIU operations are financed in a manner insufficient as compared to their needs. c) The level of international cooperation of PFIU with their foreign counterparts is insufficient: – Responses given by PFIU are limited in terms of the scope and type of data. – The mean PFIU response time is longer than seven days, but shorter than 30 days from the day of receipt of the inquiry. – Information received from the majority of FIU is not limited in terms of the scope and type of data, and the mean time of their receipt is more than seven days but not more than 30 days from the day of transfer of the inquiry. – PFIU has and uses electronic communication channels for fast and secure exchange of information with a part of FIUs, with whom they exchange information, – PFIU exchanges information with some FIUs that operate within the Egmont Group. d) The level of domestic cooperation of PFIU is insufficient: – Replies provided by the PFIU are limited in terms of the data scope and type and the type of law enforcement or judicial authority. – The average PFIU response time is longer than seven days, but shorter than 30 days from the day of receipt of the inquiry. – Information acquired from authorities is not limited in terms of the scope and type of data, only some authorities transfer information within deadlines set out by the GIFI. – PFIU has and uses electronic communication channels for fast and secure exchange of information with some law enforcement authorities. 4. The level of activity of law enforcement authorities jest is insufficient. a) Law enforcement authorities have limited awareness of risk in terms of ML/TF. b) Law enforcement authorities have insufficient capacity to counteract ML/ TF risk (assessed on the basis of the held permits, personnel, hardware, financial resources): – They are entitled to obtain some information they require during their proceedings. – Have insufficient personnel resources to execute tasks in the area of CFT. – They have insufficient hardware to conduct operations (shortcomings in terms of quantity or quality). – Their activity is financed insufficiently compared to their needs. c) The level of domestic cooperation between law enforcement authorities is insufficient. – Responses provided by these authorities are limited in terms of the scope and type of data or the type of law enforcement authority. – The authorities have and utilise electronic communication channels for fast and secure exchange of some information between each other. d) The level of international cooperation of law enforcement authorities with their foreign counterparts is insufficient. – Responses provided by law enforcement authorities are limited in terms of the scope and type of data. – Some authorities possess and use electronic communication channels for fast and secure exchange of information with their foreign counterparts. 5. The level of activity of authorities of the justice system is insufficient. a) The authorities possess insufficient awareness of risk in terms of ML/TF. b) Court proceedings take a long time (on average 2-3 years from the submission of the indictment to court until the sentence is passed in the first instance). 6. The legal system - existing legal provisions only partially correspond to the scope of the analysed risk and the requirements/ standards of the EU and FATF recommendations.

Very high vulnerability (4 p.)	1. High level of economy vulnerability. a) With respect to products and services: – Decidedly high volume of products and services facilitating quick and anonymous transactions. – The channels of flow of financial resources are neither secured nor monitored. – Decidedly high volume of financial transactions, including cash transactions, as well as others, which may facilitate anonymity of originators and beneficiaries. – Decidedly high volume of international transactions. b) With respect to entities offering these products and services: – Only a small part of categories of entities that should be OI is subject to AML/CFT provisions and oversight of public authorities in this regard. – OI are not aware enough of their obligatory duties in terms of AML/CFT. Significant indications of the possible lack of compliance of the operation of OI with these provisions. – According to supervisory bodies, OI analyse transactions or apply CDD, or they report information on their suspicions to the PFIU insufficiently – high volume of cases of administrative penalties imposed for lack of compliance of OI with AML/ CFT provisions 2. The level of activity of OI supervisory bodies is at insufficient level. a) Supervisory bodies have insufficient human financial resources and hardware to conduct OI inspections. b) The results of conducted audits do not form the basis to impose administrative fines and other supervisory measures over OI not adhering to AML/CFT provisions. c) Supervisory bodies do not provide information about the executed audits to the PFIU. d) The level of cooperation with other domestic and foreign supervisory bodies is low. 3. PFIU operate in a limited manner. a) PFIU has no awareness of the risk related to ML/TF. b) Weak capacity of PFIUs to collect and analyse information about suspicious activities/ transactions (evaluated on the basis of the permits, personnel, hardware and finances held): – PFIU has no direct or indirect access to the majority of databases of public authorities required to analyse information about suspicious activities/transactions. – PFIU is not entitled to receive from OI and CU additional information upon request. – Analysts are not trained at all in the execution of analyses (or are trained insufficiently). – PFIU has insufficient personnel resources to execute tasks in the area of CFT. – PFIU does not have a computer system allowing the reception, collection and analyses of information on suspicious activities/transactions. – PFIU operations are financed insufficiently with respect to their needs. c) The level of international cooperation of PFIU with their foreign counterparts jest low: – Replies provided by the PFIU are limited in terms of the scope and type of data. – The average PFIU response time exceeds 30 days from the day of receipt of an inquiry. – Information received from the majority of PFIU is limited in terms of the scope and type of data, and the average time of their receipt exceeds 30 days from the day of transfer of the inquiry. – PFIU do not have electronic communication channels for quick and secure exchange of information with other PFIU or does not use them if it has them, – PFIU only exchanges information with FIU of EU member states. d) The level of domestic cooperation of PFIU is low: – Replies provided by the PFIU are limited in terms of the scope and type of data and the type of law enforcement or judicial authority. – The average PFIU response time exceeds 30 days from the day of receipt of an inquiry. – Information acquired from authorities is not limited in terms of the scope and type of data, most authorities do not transfer information within deadlines set out by the GIFI. – PFIU does not have electronic communication channels for fast and secure exchange of information with law enforcement authorities, or does not use them if it has them. 4. The level of activity of law enforcement authorities is low. a) Law enforcement authorities have no awareness of ML/ TF risk. b) Law enforcement authorities have weak capacity to counteract ML/ TF risk (assessed on the basis of the held permits, human resources, hardware, financial resources): – They are entitled to obtain a fraction of the information they require during their proceedings. – They have insufficient human resources to execute tasks in the area of CFT. – They have insufficient hardware to conduct operations (significant shortcomings in terms of quantity or quality). – Their activity is financed insufficiently compared to their needs. c) The level of domestic cooperation between law enforcement authorities is low. – Responses provided by these authorities are greatly limited in terms of the scope and type of data or the type of law enforcement authority. – The authorities do not possess electronic communication channels for fast and secure exchange of information between each other, or if they do, they do not utilise them.

	d) The level of international cooperation of law enforcement authorities with their foreign counterparts is low. – Responses provided by law enforcement authorities are significantly limited in terms of the scope and type of data. – The authorities do not possess electronic communication channels for fast and secure exchange of information with their foreign counterparts and if they do, they do not utilise them. 5. The level of activity of judicial authorities is low. a) The authorities have no awareness of ML/TF risk. b) Court proceedings take a very long time (on average over three years from the submission of the indictment to court until the sentence is passed in the first instance). 6. The legal system - existing legal provisions correspond in a limited fashion to the scope of the analysed risk and the requirements/ standards of the EU and FATF recommendations.

The probability level shall be assessed on the basis of the estimated threat and vulnerability levels, according to the rules given below.

Table no. 3 – Mode of calculation of the probability level of ML compared to the evaluation of „basic risk"



Probability level	
very high probability	3.6-4
high probability	2.6-3.5
average probability	1.6-2.5
low probability	1-1.5

Using the following formula: $P_{prp}=40\%*Z_{rp}+60\%*P_{rp}$;

where: P_{prp} – Level of probability of ML occurrence compared to the evaluation of „basic risk", Z_{rp} – ML threat level compared to the evaluation of „basic risk", P_{rp} – ML vulnerability level compared to the evaluation of „basic risk".[7]

Subsequently, the level of consequences of ML to the assessment of „basic risk" shall be assessed according to the scheme set out in table no. 4.

Table no. 4 – ML consequence levels for the evaluation of „basic risk"

Consequence level	Consequence level characteristics[8]
Weak consequences (1 p.)	No visible social, economic and political consequences.

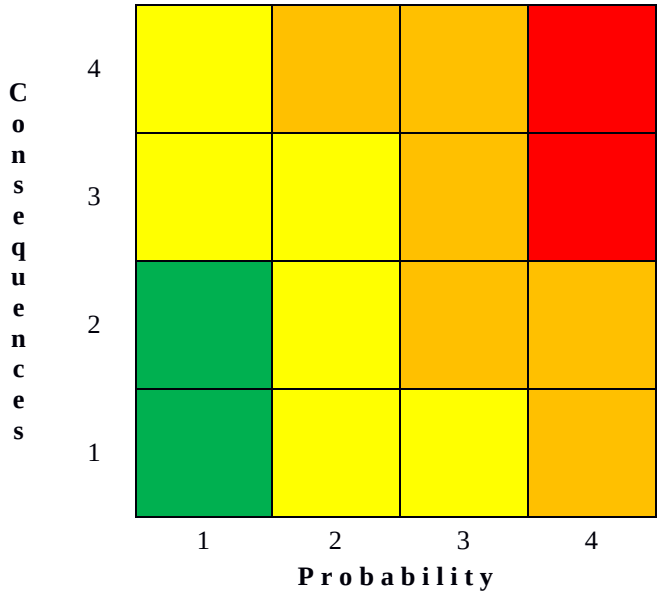
[7] Increased weight was assumed for the vulnerability level due to the fact that even if the threat of money laundering exists, the probability of its execution depends to a greater extent on the vulnerability of the AML/CFT system that should counter the execution of such threats.

[8] In order to assign the weak or significant or strong consequence levels, there should transpire at least four conditions set out in the subitems (including – for significant and strong consequences – at least one from the second item).

Moderate consequences (2 p.)	Emergence of short-term (up to one year) socio-economic consequences: – increase of criminal activity, – increase of the overall amount of resources from illegal sources legitimised domestically or/and transferred abroad, – increase of the costs of operation of public and private sector entities that are related to the assurance of security of their activity and of society, – reduction of public sector revenue.
Significant consequences (3 p.)	1. Emergence of short-term (up to one year) socio-economic consequences: – increase of criminal activity, – increase of the overall amount of resources from illegal sources legitimised domestically or/and transferred abroad, – increase of the costs of operation of public and private sector entities that are related to the assurance of security of their activity and of society, – reduction of public sector revenue. 2. Emergence of short-term (up to one year) political consequences: – increase of the popularity of the country as a criminal 'haven', – drop of the country's reliability in the international fora, – coverage of the country with political and economic sanctions.
Strong consequences (4 p.)	1. Emergence of long-term (over one year) socio-economic consequences: – increase of criminal activity, – increase of the overall amount of resources from illegal sources legitimised domestically or/and transferred abroad, – increase of the costs of operation of public and private sector entities that are related to the assurance of security of their activity and of society, – reduction of public sector revenue. 2. Emergence of long-term (over one year) political consequences: – increase of the popularity of the country as a criminal 'haven', – drop of the country's reliability in the international fora, – coverage of the country with political and economic sanctions.

The last step shall see the evaluation of the „basic risk" according to the rules presented below.

Table no. 5 – Mode of calculation of the level of „basic risk" of ML



Basic risk level	
very high risk	3.6-4
high risk	2.6-3.5
medium risk	1.6-2.5
low risk	1-1.5

According to the formula: $R_{rp}=60\%*P_{rp}+40\%*K_{rp}$

Where: R_{rp} – Level of „basic risk", P_{rp} – Level of probability of ML for the evaluation of „basic risk", K_{rp} – level of consequences of ML for the evaluation of „basic risk".[9]

„Residual risk" of ML

The assessment of „residual risk" will be primarily based on the evaluation of the level of threat and the vulnerability for each scenario.

The threat level for each scenario will be assessed on a scale from one point – minimum, up to four points – maximum. The evaluation of the threat level will take into account two constituent components: the intentions of perpetrators and the capacities and skills required to successfully transfer illegal or legal funds for the purpose of ML.

Table no. 6 – Threat levels

Threat level	Threat level characteristics
Low threat (1 p.)	There is no information that perpetrators might (or plan to) utilise the analysed *modus operandi* and possess suitable resources to do this. This mode of action is perceived by perpetrators as being unattractive and highly dangerous. It is very difficult to use due to the necessary planning, highly specialised knowledge and skills. The usage of other methods (alternatives to the analysed *modus operandi*) costs less.
Medium threat (2 p.)	There is certain scarce information that perpetrators might (or plan to) utilise the analysed *modus operandi* and possess suitable resources to do this. The analysed *modus operandi* is perceived by perpetrators as being unattractive and dangerous. It is difficult to utilise due to the necessary planning, knowledge and skills. The usage of other *modi operandi* (alternatives to the analysed one) may cost less.
High threat (3 p.)	There is information that perpetrators utilise the analysed *modus operandi* and possess suitable resources to do this. The analysed *modus operandi* is perceived by perpetrators as being attractive (in terms of finances as well) and quite safe. This *modus operandi* requires medium-level planning, knowledge and skills.
Very high threat (4 p.)	There is information that perpetrators periodically utilise the analysed *modus operandi*. This mode of action is broadly available and its application costs relatively little as compared to other *modi operandi*. The analysed *modus operandi* is perceived by perpetrators as being attractive and secure. It requires little planning, knowledge and skills.

[9] Assumed was a greater weight for the probability level due to the fact that it is a function both of the threat and vulnerability levels, and hence it should influence the level of basic risk more strongly than the consequence level.

The level of vulnerability for each risk scenario will also be assessed on a scale from one point – minimum, to four points – maximum. The assessment of weak properties will be based on an analysis of prevalence and efficiency of existing security measures, considering the legal situation (in particular in terms of financial market regulation, powers of domestic entities of the AML/CFT system), information about the practical functioning of the financial market and the domestic AML/ CFT system.

Table no. 7 – Vulnerability levels

Vulnerability level	**Vulnerability level characteristics** **To assign a given risk level, the conditions must be fulfilled that are stated in at least two of four points assigned to it[10]**
Low vulnerability (1 p.)	1. Products and services that may be utilised as part of the risk: **a)** The above mentioned products and services are difficult to acquire. **b)** The above mentioned products and services do not allow the data of the entities using them to be hidden. **c)** The above mentioned products and services do not provide capacities to execute international transactions. 2. Activity of entities offering products and services that could be utilised as part of the risk: **a)** All entities offering products and services utilised as part of the scenario are OI. **b)** The OI, to which the scope of the analysed risk applies, have a suitable level of awareness of their obligatory duties in terms of AML/CFT. Lack or relatively limited information about the lack of conformity of the operations of these OI with AML/CFT provisions. **c)** According to supervisory bodies, the OI effectively analyse transactions and apply CDD, and also report information about their suspicions to the PFIU. 3. Activity of public administration authorities and entities: **a)** Public authorities possess an exhaustive risk assessment concerning money laundering and financing of terrorism (ML/TF). Law enforcement authorities have relatively high capacity to counteract ML/TF risk related to the given scenario (meaning, the probability is high that a case of ML/TF in terms of the analysed risk is detected, and that then as a result of proceedings/investigations the perpetrators of the crime are indicted and convicted). **b)** Relatively high capacity of PFIU to collect information about suspicious activities/ transactions from OI and CU, detect and analyse cases suspected of ML/TF in terms of the analysed risk (evaluated on the basis of the powers, human resources, hardware and finances held). **c)** Domestic and international cooperation of bodies engaged in the domestic AML/CFT system, in particular PFIU, supervisory bodies and law enforcement authorities (also with their foreign counterparts) is good. The exchange of information is not limited due to the scope and type of data. 4. The legal system - Existing legal provisions correspond to the scope of the analysed risk.
Medium vulnerability (2 p.)	1. Products and services that may be utilised as part of the risk: a) Access to the above mentioned products and services is difficult. b) The above mentioned products and services provide certain capacities for the data of the entities using them to be hidden. c) The above mentioned products and services permit the execution of international transactions. 2. Activity of entities offering products and services that could be utilised as part of the risk: a) The majority of entities offering products and services utilised as part of the scenario are OI. b) The OI, to which the scope of the analysed risk applies, are aware of the duties imposed on them as part of AML/CFT. There is certain information about the lack of conformity of the operation of these OI with AML/CFT provisions.

[10] In case of emergence of conditions from the lower and higher levels it is possible to average them out (e. g. from lower and higher vulnerability – to medium vulnerability).

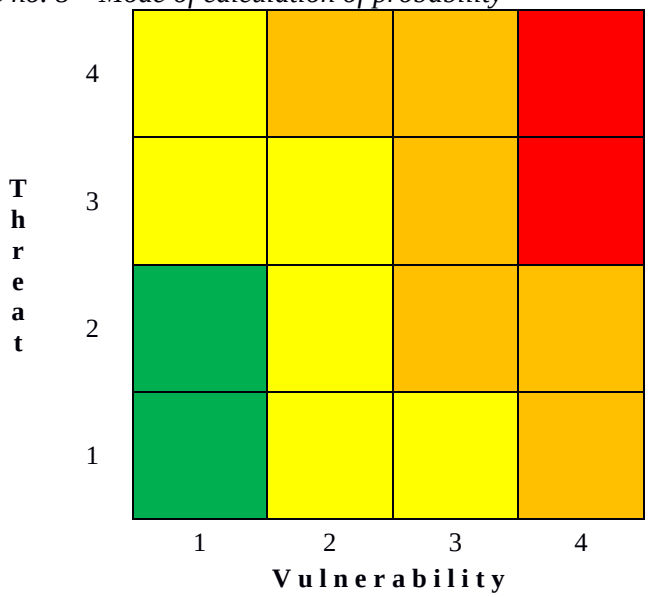
	c) According to supervisory bodies OI analyse transactions and apply CDD, there is, however, information on shortcomings in identification and verification of customers. OI transfer relatively little information on their suspicions to the PFIU. 3. Activity of public administration authorities and entities: a) Public authorities possess a risk assessment concerning ML/TF. Law enforcement authorities have the capacity to counteract ML/TF risk (meaning, the probability is high that a case of ML/TF in terms of the analysed risk is detected, and that then as a result of proceedings/investigations the perpetrators of the crime are indicted and convicted). b) PFIU is capable of collecting information about suspicious activities/ transactions from OI and CU, detect and analyse cases suspected of ML/TF in terms of the analysed risk (capacities evaluated on the basis of the powers, human resources, hardware and finances held). c) Domestic and international cooperation of bodies engaged in the domestic AML/CFT system, in particular PFIU, supervisory bodies and law enforcement authorities (also with their foreign counterparts) works. The exchange of information is partly limited in terms of the scope and type of data. 4. The legal system - existing legal provisions largely correspond to the scope of the analysed risk.
High vulnerability (3 p.)	1. Products and services that may be utilised as part of the risk: **a)** Access to the above named products and services is relatively easy. **b)** The above named products and services provide certain capacities for the data of the entities using them to be hidden. **c)** The above mentioned products and services permit the execution of international transactions. 2. Activity of entities offering products and services that could be utilised as part of the risk: **a)** Only part of entities offering products and services utilised as part of the scenario are OI. **b)** The OI, to which the scope of the analysed risk applies, have relatively low awareness of their obligatory duties in terms of AML/CFT. There is relatively broad information about the lack of conformity of the operation of these OI with AML/ CFT provisions. **c)** According to supervisory bodies OI analyse transactions and apply CDD to a relatively limited extent. There is relatively broad information about shortcomings in customer identification and verification. OI transfer relatively little information on their suspicions to the PFIU. **3.** Activity of public administration authorities and entities: **a)** Public authorities possess limited risk assessment concerning ML/TF. Law enforcement authorities have relatively limited capacity to counteract ML/ TF risk (meaning, there exists the probability that a case of ML/TF in terms of the analysed risk will not be detected or in case of detection that the proceedings/investigation would not lead to an indictment and conviction of the perpetrators of the crime). **b)** PFIU is capable of collecting information about suspicious activities/ transactions from OI and CU, detecting and analysing cases suspected of ML/TF in terms of the analysed risk only in a limited manner (capacities evaluated on the basis of the powers, human resources, hardware and finances held). **c)** Domestic and international cooperation of bodies engaged in the domestic AML/CFT system, in particular PFIU, supervisory bodies and law enforcement authorities (also with their foreign counterparts) works. The exchange of information is relatively broadly limited in terms of the scope and type of data. **4.** The legal system - existing legal provisions largely do not correspond to the scope of the analysed risk.
Very high vulnerability (4 p.)	1. Products and services that may be utilised as part of the risk: **a)** Access to the above mentioned products and services is common. **b)** The above mentioned products and services allow data of the entities using them to be hidden. **c)** The above mentioned products and services permit the execution of international transactions. 2. Activity of entities offering products and services that could be utilised as part of the risk – the above-indicated entities are not OI. 3. Activity of public administration authorities and entities:

	a) Public authorities possess no risk assessment concerning ML/TF. Law enforcement authorities have decidedly limited capacity to counteract ML/TF risk (meaning, the probability is high that a case of ML/TF in terms of the analysed risk will not be detected, or in case of detection that the proceedings/investigation would not lead to an indictment and conviction of the perpetrators of the crime). **b)** PFIU is capable of collecting information about suspicious activities/transactions from OI and CU, of detecting and analysing cases suspected of ML/TF in terms of the analysed risk only to a definitely limited extent (capacities evaluated on the basis of the powers, human resources, hardware and finances held). **c)** Domestic and international cooperation of bodies engaged in the domestic AML/CFT system, in particular PFIU, supervisory bodies and law enforcement authorities (also with their foreign counterparts) does not work. The exchange of information is not conducted. 4. The legal system - existing legal provisions do not correspond to the scope of the analysed risk.

In course of determination of the „residual risk" the assumption shall be made that consequences of ML (considered as the third constituent component of the assessment of risk besides threats and vulnerabilities) will not be calculated separately due to the difficulty in distinguishing between them for the individual scenarios. An estimation of these shall be made in the same manner as it was done for the basic ML risk level.

The level of probability will be estimated on the basis of estimates of the threat and vulnerability levels.

Table no. 8 – Mode of calculation of probability



Probability level	
very high probability	3.6-4
high probability	2.6-3.5
average probability	1.6-2.5
low probability	1-1.5

Using the formula: $P_{ps}=40\%*Z_{ps}+60\%*P_{ps}$

Where: P_{ps} – Probability level for the scenario, Z_{ps} – threat level for the scenario, P_{ps} – vulnerability level for the scenario.[11]

The subsequent step shall estimate the general probability level for the scenarios based on the estimates of probability levels of each scenario. This shall take place on the basis of the formula (the list of probability levels presented in table no. 8 shall be used):

n

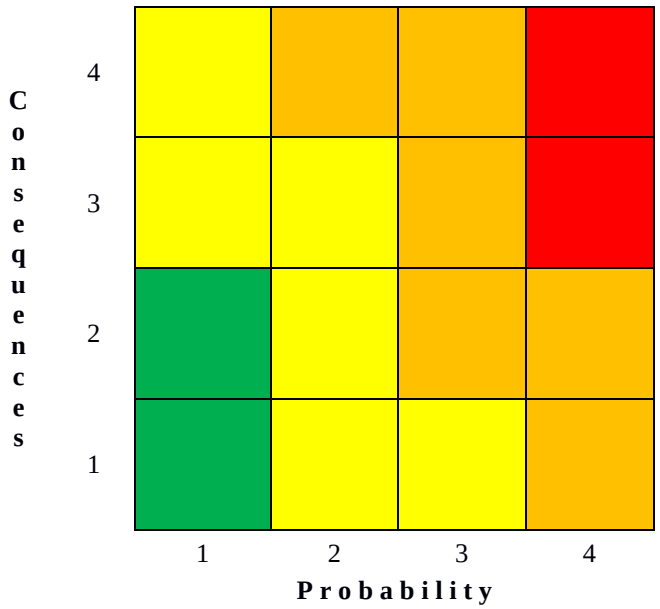
[11] A higher weight was assumed for the vulnerability level due to the fact that even if a high threat of money laundering exists, the probability of its implementation depends to a larger extent on the vulnerability of the AML/CFT system, which should counter the execution of these threats.

$P_p = \sum (P_{ps})/n$

Where: P_p – General probability level for the scenarios, n – scenario count

The next step shall estimate the level of „residual risk" in the manner presented below.

Table no. 9 – Mode of calculation of the level of „residual risk" of ML



Residual risk level	
very high risk	3.6-4
high risk	2.6-3.5
medium risk	1.6-2.5
low risk	1-1.5

Using the formula: $R_s = 60\% * P_p + 40\% * K_{rp}$

Where: R_s – Level of „residual risk", P_p – General probability level for the scenarios, K_{rp} – level of consequences of ML for the evaluation of „basic risk" (e. g. calculated for the basic level of risk of ML).[12]

„Overall risk" of ML

The evaluation of „overall risk" of ML would entail the correlation of the estimate of „residual risk" with the estimate of „basic risk" in the following manner:

$R_O = 33.3\% * R_P + 66.7\% * R_S$

Where: R_O – level of „overall risk", R_P – level of „basic risk", R_S – level of „residual risk".

The estimate of the level of „residual risk" is provided with double the weight due to the fact that it is based on information about specific methods that are or may be used for the purpose of ML. This information is also more easily confronted with data on the functioning of entities operating within the domestic AML/CFT system as well as legal provisions for the purpose of assessment of the level of vulnerability to their execution. Hence, the level of „residual risk" is probably better assessed than the level of „basic risk" as it is largely based on general information.

Assessment of TF risk – assumptions

„Basic risk" of TF

[12] A higher weight was assumed for the probability level due to the fact that it is a function of both the threat and the vulnerability levels, and hence it should influence the determination of the residual risk level more strongly.

The level of threat of TF for the evaluation of „basic risk" shall be assessed according to the scheme presented in table no. 10.

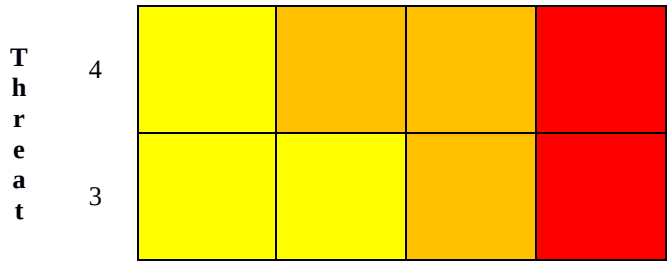
Table no. 10 – Threat levels of TF for the evaluation of „basic risk"

Threat level	**Threat level characteristics** ***(in order to assign a specific threat level, conditions should be fulfilled that are set out in at least three of four items assigned to it)***[13]
Low threat (1 p.)	1) Estimated level of asset value being the object of TF across the year: x < 0.000005%*GDP. 2) The level of risk of financing of terrorism in the EU determined to be low. 3) Information stemming from a single source about the possible utilisation of Poland to gain or transfer asset value for terrorist purposes. 4) Threat of emergence of terrorist act in Poland. None of the alarm levels foreseen by art. 15 *of the Polish act of June 10th 2016 on anti-terrorist operations* (Journal of Laws of 2019, item no. 796) was introduced in Poland.
Medium threat (2 p.)	1) Estimated level of asset value being the object of TF across the year: 0.000005%*GDP < x < 0.000025%*GDP 2) The level of risk of financing of terrorism in the EU determined to be medium. 3) Information stemming from multiple sources about the possible utilisation of Poland to gain or transfer asset value for terrorist purposes. 4) Threat of emergence of terrorist act in Poland. One of the alarm levels foreseen by art. 15 *of the Polish act of June 10th 2016 on anti-terrorist operations* indicated later was introduced in Poland: ALFA, ALFA-CRP.
High threat (3 p.)	1) Estimated level of asset value being the object of TF across the year: 0.000025%*GDP < x < 0.00005%*GDP 2) The level of risk of financing of terrorism in the EU determined to be high. 3) Information from a single source on the utilisation of Poland to gain or transfer asset value for terrorist purposes. 4) Threat of emergence of terrorist act in Poland. One of the alarm levels foreseen by art. 15 *of the Polish act of June 10th 2016 on anti-terrorist operations* indicated later was introduced in Poland: BRAVO, BRAVO-CRP.
Very high threat (4 p.)	1) Estimated level of asset value being the object of TF across the year: x > 0.00005%*GDP 2) The level of risk of financing of terrorism in the EU determined to be very high. 3) Information from multiple sources on the utilisation of Poland to gain or transfer asset value for terrorist purposes. 4) Threat of emergence of terrorist act in Poland. One of the alarm levels foreseen by art. 15 *of the Polish act of June 10th 2016 on anti-terrorist operations* indicated later was introduced in Poland: CHARLIE, CHARLIE-CRP, DELTA, DELTA-CRP.

The TF level of vulnerability for the purpose of evaluation of „basic risk" shall be assessed according to the scheme indicated in table no. 2.

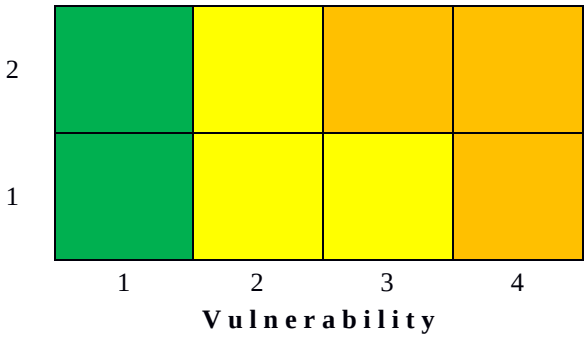
The level of probability shall be estimated on the basis of the assessed threat and vulnerability level, in accordance with the rules presented below.

Table no. 11 – Mode of calculation of the level of probability of TF for the evaluation of „basic risk"



Probability level	
very high probability	3.6-4

[13] In case of emergence of conditions from the lower and upper levels, they can also be averaged out (e. go from the low and high levels of threat – to the medium threat level).



high probability	2.6-3.5
average probability	1.6-2.5
low probability	1-1.5

According to the formula: $P_{prp\_ft}=40\%*Z_{rp}+60\%*P_{rp\_ft}$

Where: P_{prp_ft} – Probability level of emergence of TF for the evaluation of „basic risk", Z_{rp_ft} – threat level of TF for the evaluation of „basic risk", P_{rp_ft} – level of vulnerability to TF for the evaluation of „basic risk".[14]

Subsequently, the level of consequences of TF shall be assessed for the evaluation of „basic risk" according to the scheme presented in table no. 12.

Table no. 12 – Levels of consequences of TF for the evaluation of „basic risk"

Consequence level	**Consequence level characteristics**[15]
Weak consequences (1 p.)	No visible social, economic and political consequences.
Moderate consequences (2 p.)	Emergence of short-term (up to one year) socio-economic consequences: – increase of terrorist activity in the country, – increase of criminal activity, financing terrorist activity, – increase of the overall amount of resources from illegal sources legitimised domestically and/ or transferred abroad, – increase of the costs of operation of public and private sector entities that are related to the assurance of security of their activity and of society, – reduction of public sector revenue.
Significant consequences (3 p.)	1. Emergence of short-term (up to one year) socio-economic consequences: – increase of terrorist activity in the country, – increase of criminal activity, financing terrorist activity, – increase of the overall amount of resources from illegal sources legitimised domestically and/ or transferred abroad, – increase of the costs of operation of public and private sector entities that are related to the assurance of security of their activity and of society, – reduction of public sector revenue. 2. Emergence of short-term (up to one year) political consequences: – increase of the popularity of the country as a criminal 'haven', – drop of the country's reliability in the international fora, – coverage of the country with political and economic sanctions.
Strong consequences (4 p.)	1. Emergence of long-term (over one year) socio-economic consequences: – increase of terrorist activity in the country, – increase of criminal activity, financing terrorist activity, – increase of the overall amount of resources from illegal sources legitimised domestically and/ or transferred abroad, – increase of the costs of operation of public and private sector entities that are related to the assurance of security of their activity and of society, – reduction of public sector revenue. 2. Emergence of long-term (over one year) political consequences:

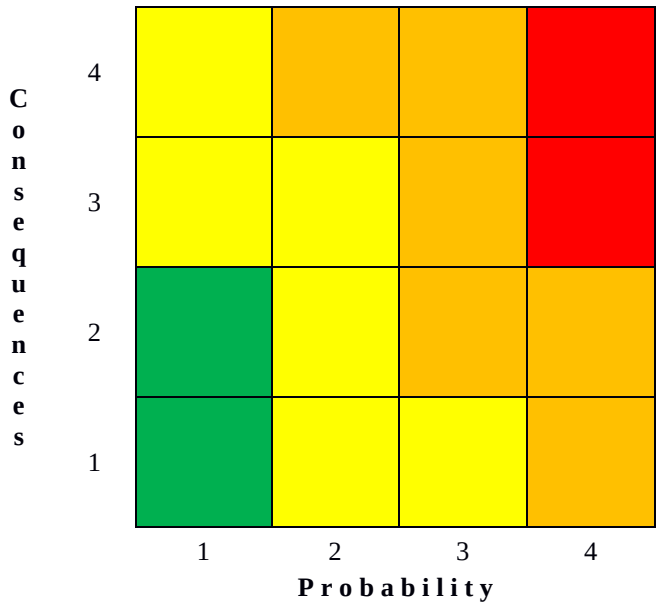
[14] A higher weight was assumed for the vulnerability level due to the fact that even if a high threat exists of financing of terrorism, the probability of its implementation depends more strongly on the vulnerability of the AML/CFT system, which should counter the execution of these threats.

[15] In order to assign the weak or significant levels or the strong level of consequences, at least four conditions should prevail from among those listed in the bullet points (including – in case of conditions from the significant and strong levels – at least one from among those under item no. 2).

	– increase of the popularity of the country as a criminal 'haven', – drop of the country's reliability in the international fora, – coverage of the country with political and economic sanctions.

The last stage shall evaluate the level of „basic risk" according to the rules presented below.

Table no. 13 – Mode of calculation of the level of „basic risk" of TF



Level of basic risk	
very high risk	3.6-4
high risk	2.6-3.5
medium risk	1.6-2.5
low risk	1-1.5

Using the formula: $R_{rp\_ft}=60\%*P_{rp\_ft}+40\%*K_{rp\_ft}$

Where: R_{rp_ft} – Level of „basic risk", P_{rp_ft} – Probability level of TF for the evaluation of „basic risk", K_{rp_ft} – level of consequences of TF for the evaluation of „basic risk".[16]

„Residual risk" of TF

The evaluation of „residual risk" will primarily be based on the assessment of the level of threat and vulnerability for each scenario.

The threat level for each risk scenario will be assessed on a scale ranging from one point – minimum, to four points – maximum. The assessment of the threat level will take into account two constituent components: the intentions of the perpetrators and their capabilities, as well as capacities to successfully transfer illegal or legal funds for the purpose of TF. It will be based on the scheme set out in table no. 6.

The level of system vulnerability for each scenario will also be estimated on a scale ranging from one point – minimum, to four points – maximum. The evaluation of weak sides will be based on the analysis of the prevalence and effectiveness of existing security measures, taking into account the legal situation (in particular in terms of regulations of the financial market, rights of the bodies within the domestic system of countering money laundering and financing of terrorism), information about the practical functioning of the financial market and the domestic Polish AML/CFT system. The assessment of the vulnerability level for each scenario will be performed on the basis of the scheme set out in table no. 7.

[16] A higher weight was assumed for the probability level due to the fact that it is a function both of the threat and vulnerability levels, and hence it should more strongly influence the determination of the basic risk level than the level of consequences does.

When evaluating the „residual risk", the assumption shall be made that consequences of TF (analysed as the third component of assessment of risk beside the threat and vulnerability) will not be calculated separately due to the difficulty to distinguish between them for the individual scenarios. Their assessment will be assumed to be the same as for the basic level of risk of financing of terrorism.

The estimate of „residual risk" will be made in three stages. In the first stage, estimated shall be the probability level of usage of each scenario on the basis of the threat level and vulnerability level (according to the scheme set out in table no. 8).

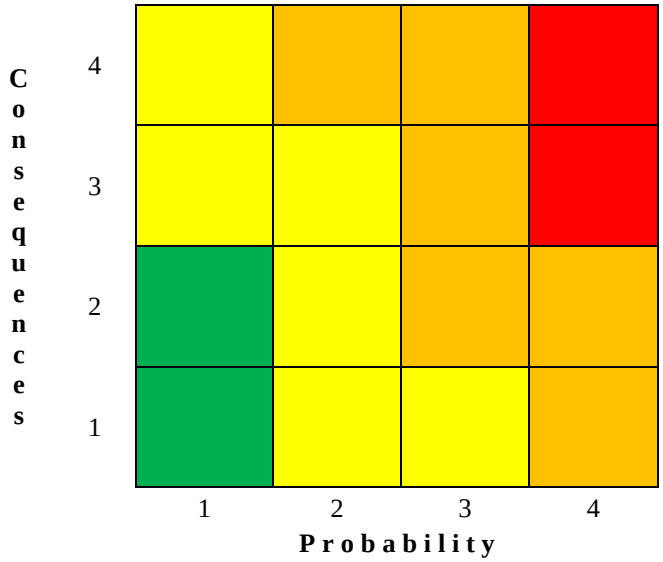
In the next stage, assessed shall be the general level of probability for scenarios on the basis of estimates of the probability levels for each scenario. This will take place based on the formula:

$$P_{p\_ft} = \sum (P_{ps\_ft})/n$$

Where: P_{p_ft} – Overall probability level for scenarios, n – scenario count

In the last stage, assessed shall be the level of „residual risk" as set out below.

Table no. 14 – Mode of calculation of the „residual risk" of TF



Residual risk level	
very high risk	3.6-4
high risk	2.6-3.5
medium risk	1.6-2.5
low risk	1-1.5

According to the formula: $R_{s\_ft}=60\%*P_{p\_ft}+40\%*K_{rp\_ft}$

Where: R_{s_ft} – Level of „residual risk", P_{p_ft} – Overall level of probability for scenarios, K_{rp_ft} – level of consequences of TF for the evaluation of „basic risk" (calculated for the basic level of risk of TF).[17]

„Overall risk" of TF

The assessment of „overall risk" of TF would entail the correlation of the assessment of „residual risk" with the assessment of „basic risk", as follows:

$$R_{O\_ft}=33.3\%*R_{P\_ft}+66.7\%*R_{S\_ft}$$

Where: R_{O_ft} – level of „overall risk", R_{P_ft} – level of „basic risk", R_{S_ft} – level of „residual risk".

The assessment of the „residual risk" level shall be assigned double the weight due to the fact that it is based on information about specific methods that are or may be used for the purpose

[17] A higher weight is used for the probability level due to the fact that it is a function both of the threat level as well as the vulnerability level, and hence it should influence the determination of the basic risk level more strongly than the level of consequences does.

of TF. This information can also be more easily confronted with data on the functioning of entities operating within the domestic Polish AML/CFT system, as well as the legal provisions, in order to assess the level of vulnerability to their execution. Hence, the level of „residual risk" is probably better assessed than the level of „basic risk", basing mostly on general information.

The final value of „overall risk" will be assigned to a specific level of risk using the following ranges:

- very high risk – <3.6;4.0>,
- high risk – <2.6;3.5>,
- medium risk – <1.6;2.5>,
- low risk – <1.0;1.5>.