ANNEX 1 – METHODOLOGY FOR CONDUCTING THE NATIONAL ASSESSMENT OF THE RISK OF MONEY LAUNDERING AND FINANCING OF TERRORISM

Introduction

Pursuant to Recommendation 1 issued by the Financial Action Task Force (FATF): "Countries should identify, assess, and understand the money laundering and terrorism financing 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 terrorism financing are commensurate with the risks identified".[1]

The essential purposes of such analysis are to identify the possible changes to the national anti-money laundering and counter-terrorism financing (AML/CFT) system, including, including changes in the law, as well as to specify the appropriate allocation of resources and set out the priorities in using these resources. The analysis should be reviewed on a periodic basis. The analysis results should be made available to the obligated institutions to facilitate their own money laundering and terrorism financing risk assessments.

The first national assessment of the risk of money laundering and financing of terrorism was published in 2019. It was a comprehensive document consisting in the body and 5 annexes, which presented – on the basis of the available information – the results of threats, vulnerability and risk analysis related to money laundering and financing of terrorism.

The Act of 1 March 2018 on counteracting money laundering and financing of terrorism provides for the regulations specifying the basic principles for preparing and updating the national assessment of the risk of money laundering and financing of terrorism (hereinafter: the national risk assessment) and the assessment-based strategy. According to these regulations, the General Inspector of Financial Information (GIFI) verifies whether the national risk assessment remains up-to-date and draws up the national risk assessment if needed however in any case at least once in 2 years.

Risk identification method

The FATF publication entitled "National Money Laundering and Terrorism Financing Risk Assessment" states that there is no single or universal methodology for conducting a money laundering and terrorism financing risk assessment. It depends mostly on the purposes and scope of the assessment[2].

The standard methods of money laundering (ML) and terrorism financing (FT) risk assessment are based on the identification of three components serving as a foundation of risk assessment: threat, vulnerability and consequences (additional component is probability understood as the function of threat and vulnerability). The essential difference between them lies in the method of their identification, especially of threat.

---

[1]International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, updated in October 2018, p. 9, available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.
[2]National Money Laundering and Terrorist Financing Risk Assessment, FATF, February 2013, p. 9.

In the methodologies elaborated by the World Bank or the International Monetary Fund, the threat is identified on the basis of the list of predicate offences for money laundering (and additionally the estimated amount of the proceeds of crime), flow directions of the illegal proceeds, ML techniques and their development trends. When conducting the FT risk assessment, the risk is identified by referring to the threat assessment on terrorism as well as information on the identified sources of funds allocated to financing of terrorism (both illegitimate and legitimate) and their transferring methods.

The European Commission, in its works on the supranational ML/FT risk assessment, focused primarily on the list of *modi operandi* used to commit these crimes. The scenarios of criminal activities identified in this list are then used to estimate the threat understood as the assessment of the intents and capabilities of the criminals' to exploit them as well as vulnerability understood as the assessment of countermeasures. The European Commission stated in its methodology[3] that the ML/FT consequences shall not be subject to a detailed risk assessment. The Commission assumed that ML/FT activities generate constant significant negative effects on the transparency, good governance and the accountability of public and private EU institutions, cause significant damage to EU countries national security and to the EU economy.

For the purposes of the national ML/FT risk assessment, the following indirect method was adopted, involving:

- the "inherent risk" assessment separately for ML and FT, based essentially on the assessment of threats related to the predicate offences for money laundering, financial flow directions, estimated amounts of laundered assets or assets used for the purposes of terrorism financing, information on the potential vulnerabilities related to products and services offered on the market, operation of the authorities included in the national anti-money laundering and countering financing of terrorism (AML/CFT) system, as well as legal regulations and their application in practice;
- the "residual risk" assessment, based on the assessment of sectoral risk and risk related to the list of *modi operandi* (also separately for ML and FT), compiled on the basis of both national and foreign experiences (similarly to the methodology elaborated by the European Commission);
- estimation of overall risk separately for ML and FT, based on the two assessments referred to above.

ML risk estimation – assumptions

ML "inherent risk"

The level of ML threat for the purposes of the "inherent risk" assessment will be assessed following the scheme presented in Table 1. Each itemised component identified in the table below is assessed separately. The level of threat will be estimated on the basis of arithmetic mean from their assessments.

Table 1 – The levels of ML threats for the purposes of "inherent risk" assessment

[3] 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 terrorist financing 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 terrorist financing risks affecting the internal market and related to cross-border activities), available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272.

Level of threat	Characteristics of the level of threat *(in order to assign a specific risk level, the conditions set out in at least 2 of 4 assigned items should be met)*[4]
Low threat (1 point)	1. The level of estimated illegal assets (conducted in Poland or transferred to Poland and derived from the offences committed abroad) in annual scale: x <0.05%*GDP. 2. The proceeds-generating crime (i.e. predicate offences) risk assessment for Poland at low level (among others on the basis of analysis related to economic crime, corruption, illegal trade and trafficking in narcotic drugs, arms, human beings, etc.). 3. ML risk in the EU determined at low level. 4. Poland is not indicated in known risk assessment of the other countries as one of the countries, from which the illegal assets derive, or to which such assets are transferred.
Medium threat (2 points)	1. The level of estimated illegal assets (conducted in Poland or transferred to Poland and derived from the offences committed abroad) in annual scale: 0.05%*GDP< x < 0.5%*GDP. 2. The illegal proceeds-generating crime (i.e. predicate offences) risk assessment for Poland at moderate/medium level (among others on the basis of analysis related to economic crime, corruption, illegal trade and trafficking in narcotic drugs, arms, human beings, etc.). 3. ML risk in the EU determined at moderate/medium level. 4. Poland is indicated in known risk assessment of the other countries as one of the countries, from which the illegal assets derive, or to which such assets are transferred.
High threat (3 points)	1. The level of estimated illegal assets (conducted in Poland or transferred to Poland and derived from the offences committed abroad) in annual scale: 0.5%*GDP < x <1%*GDP. 2. The illegal proceeds-generating crime (i.e. predicate offences) risk assessment for Poland at high level (among others on the basis of analysis related to economic crime, corruption, illegal trade and trafficking in narcotic drugs, arms, human beings, etc.). 3. ML risk in the EU determined at high level. 4. Poland is indicated in known risk assessment of the other countries as one of the main countries, from which the illegal assets derive, or to which such assets are transferred.
Very high threat (4 points)	1. The level of estimated illegal assets (conducted in Poland or transferred to Poland and derived from the offences committed abroad) in annual scale: x >1%*GDP. 2. The illegal proceeds-generating crime (i.e. predicate offences) risk assessment for Poland at very high level (among others on the basis of analysis related to economic crime, corruption, illegal trade and trafficking in narcotic drugs, arms, human beings, etc.). 3. ML risk in the EU determined at very high level. 4. Poland is indicated in known risk assessment of the other countries as the main country, from which the illegal assets derive, or to which such assets are transferred.

The level of ML vulnerability for the purposes of the "inherent risk" assessment will be assessed following the scheme presented in Table 2. Each itemised component identified in the table below is assessed separately. The level of vulnerability will be estimated on the basis of arithmetic mean from their assessments.

Table 2 – The levels of ML vulnerability for the purposes of "inherent risk" assessment

Level of vulnerability	Characteristics of the level of vulnerability *(in order to assign a specific risk level, the conditions set out in at least 4 of 6 assigned items should be met)*[5]
Low vulnerability (1 point)	1. Vulnerability of the economy is at a low level. a) for products and services: – none or relatively low number of products and services facilitating fast and anonymous transactions, – secured and monitored movements of funds, – relatively low number of financial transactions, including cash transactions and other transactions that could enhance anonymity of their originators and beneficiaries, – relatively low number of international transactions; b) for the entities offering these products and services: – all categories of entities which should be the obligated institutions (OI) are subject to the anti-money laundering and countering financing of terrorism (AML/CFT) regulations and to the supervision of the public administration authorities in this area,

[4] If the conditions assigned to the lower and higher level are identified, they can be averaged (for example, from the level of low threat and the level of high threat – to the level of medium threat).

[5] If the conditions assigned to the lower and higher level are identified, they can be averaged (for example, from the level of low vulnerability and the level of high vulnerability – to the level of medium vulnerability).

	– OIs demonstrate the appropriate level of awareness of the obligations imposed on them in the area of AML/CFT. None or relatively low amount of information on the potential non-compliance of these OIs with the regulations, – according to the supervisory authorities, the OIs effectively analyse the transactions and apply customer due diligence (CDD) as well as report information on their suspicions to the Polish Financial Intelligence Unit (Polish FIU) – none or very few cases of imposing the financial penalties due to non-compliance of OIs with the AML/CFT regulations. 2. The activities of the supervisory authorities over the OIs are at a high level. a) the supervisory authorities have adequate financial, human and technical resources to control the OIs; b) the results of the performed controls form the basis to impose administrative penalties and apply other supervisory instruments to the OIs failing to implement with the AML/CFT regulations; c) all supervisory authorities provide information on the performed controls to the Polish FIU; d) cooperation with the other national and foreign supervisory authorities remains at a good level. 3. The Polish FIU activities are at a high level. a) Polish FIU demonstrates very good awareness of the ML/FT risk; b) relatively high Polish FIU capability to collect and analyse information on the suspicious operations/transactions (assessed on the basis of the existing powers, human, financial and technical resources): – Polish FIU has direct access to all databases of public administration authorities, necessary to analyse information on the suspicious operations/transactions, – Polish FIU has powers to receive additional information from the OIs and cooperating units (CUs) on request, – the analysts are trained in conducting the analyses, – Polish FIU has adequate human resources to perform the CFT tasks, – Polish FIU has the information system enabling the effective acquisition, collecting and analysing information on the suspicious operations/transactions, – the activities of Polish FIU are financed adequately to its needs; c) international cooperation of Polish FIU with its foreign counterparts is at a good level: – responses provided by Polish FIU are not limited in terms of scope and type of data, – average Polish FIU response time does not exceed 3 days from the day of the inquiry, – information obtained from vast majority of the foreign FIUs are not limited in terms of scope and type and data and the average response time does not exceed 3 days from the date of inquiry, – Polish FIU holds and uses the electronic communication channels for fast and secured information exchange with all FIUs, with which it exchanges information, – Polish FIU exchanges information with all FIUs operating under the Egmont Group; d) national cooperation of Polish FIU is at good level: – responses provided by Polish FIU are not limited in terms of scope and type of data and the type of law enforcement or judicial authority, – average Polish FIU response time does not exceed 3 days from the day of receiving the inquiry, – information obtained from the authorities are not limited in terms of scope and type and data, all authorities provide information within the time-limit set by the General Inspector of Financial Information (GIFI), – Polish FIU holds and uses the electronic communication channels for fast and secured information exchange with all types of law enforcement authorities. 4. The activities of the law enforcement authorities are at a high level. a) the law enforcement authorities demonstrate very good awareness of the ML/FT risk; b) the law enforcement authorities demonstrate a relatively high capability to counter the ML/FT risk (assessed on the basis of the existing powers, human, financial and technical resources): – have powers to acquire any and all necessary information during the performed activities, – have adequate human resources to perform the CFT tasks, – have adequate high-quality equipment to perform the activities, – their activities is financed adequately to their needs; c) national cooperation between law enforcement authorities is at a good level: – responses provided by the authorities are not limited in terms of scope and type of data or the type of law enforcement authority, – the authorities have and use the electronic communication channels for fast and secured information exchange between each other; d) international cooperation of law enforcement authorities with their foreign counterparts is at a good level: – responses provided by law enforcement authorities are not limited in terms of scope and type of data, – the authorities hold and use the electronic communication channels for fast and secured information exchange with all foreign counterparts. 5. The activities of law enforcement authorities are at a good level.

	a) the authorities demonstrate very good awareness of the ML/FT risk; b) the judicial proceedings are conducted in a relatively short time (up to 1 year from submitting the indictment to announcing the first instance decision in average). 6. Legal system – the scope of the existing legal regulations corresponds to the scope of the analysed risk and the EU requirements/standards and FATF recommendations.
Medium vulnerability (2 points)	1. Vulnerability of the economy is at a medium level. a) for products and services: – limited number of products and services facilitating fast and anonymous transactions, – movements of funds are in most cases secured and monitored, – relatively large number of financial transactions, including cash transactions and other transactions that could enhance anonymity of their originators and beneficiaries, – limited number of international transactions; b) for the entities offering these products and services: – most categories of entities that should be OIs are subject to the anti-money laundering and countering financing of terrorism (AML/CFT) regulations and to the supervision of the public administration authorities in this area, – OIs are aware of the obligations imposed on them in the area of AML/CFT. Few information on the potential non-compliance of these OIs with the regulations, – according to the supervisory authorities, the OIs analyse the transactions and apply customer due diligence (CDD) as well as report information on their suspicions to the Polish FIU there are however some cases of imposing the financial penalties due to non-compliance of OIs with the AML/CFT regulations. 2. The activities of the supervisory authorities over the OIs are at a good level. a) the supervisory authorities have rather adequate financial, human and technical resources to control the OIs, with occasional certain deficiencies in this area; b) the results of the performed controls form the basis to impose administrative penalties and apply other supervisory instruments to the OIs failing to implement with the AML/CFT regulations; c) most of the supervisory authorities provide information on the performed controls to the Polish FIU; d) cooperation with the other national and foreign supervisory authorities remains at a good level. 3. The Polish FIU activities are at a good level. a) Polish FIU demonstrates good awareness of the ML/FT risk; b) relatively good Polish FIU capability to collect and analyse information on the suspicious operations/transactions (assessed on the basis of the existing powers, human, financial and technical resources): – Polish FIU has direct or indirect access to all databases of public administration authorities, necessary to analyse information on the suspicious operations/transactions, – Polish FIU has powers to receive additional information from the OIs and CUs on request, – most of the analysts are trained in conducting the analyses, – Polish FIU has adequate human resources to perform the CFT tasks, with occasional certain deficiencies in this area, – Polish FIU has the information system enabling acquisition, collecting and analysing information on the suspicious operations/transactions, – the activities of Polish FIU are financed adequately to its needs, with occasional certain deficiencies in this area; c) international cooperation of Polish FIU with its foreign counterparts is at an adequate level: – responses provided by Polish FIU are not limited in terms of scope and type of data, – average Polish FIU response time exceeds 3 days however does not exceed 7 days from the day of receiving the inquiry, – information obtained from vast majority of the FIUs are not limited in terms of scope and type and data and the average response time exceeds 3 days however does not exceed 7 days from the date of inquiry, – Polish FIU holds and uses the electronic communication channels for fast and secured information exchange with most of the FIUs, with which it exchanges information, – Polish FIU exchanges information with most of the FIUs operating under the Egmont Group; d) national cooperation of Polish FIU is at a good level: – responses provided by Polish FIU are not limited in terms of scope and type of data and the type of law enforcement or judicial authority, – average Polish FIU response time exceeds 3 days however does not exceed 7 days from the day of the inquiry, – information obtained from the authorities are not limited in terms of scope and type and data, most of the authorities provide information within the time-limit set by the General Inspector of Financial Information (GIFI), – Polish FIU holds and uses the electronic communication channels for fast and secured information exchange with most types of law enforcement authorities. 4. The activities of the law enforcement authorities are at a good level.

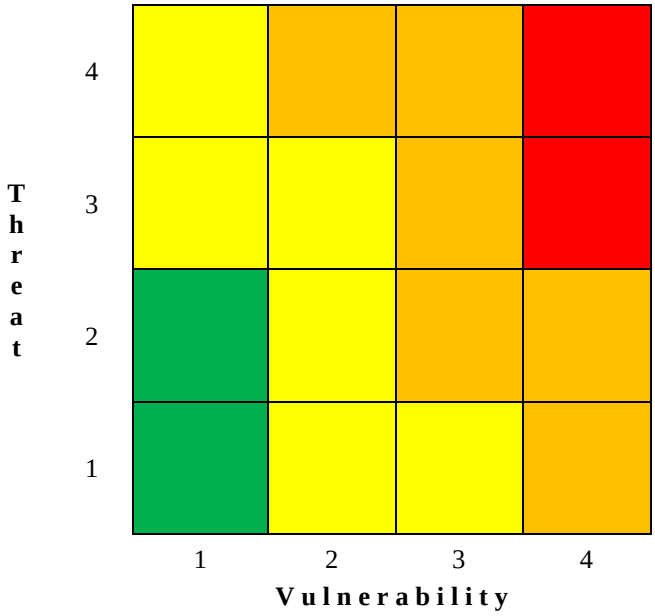
	a) the law enforcement authorities demonstrate good awareness of the ML/FT risk, b) the law enforcement authorities demonstrate good capability to counter the ML/FT risk (assessed on the basis of the existing powers, human, financial and technical resources): – have powers to acquire most of the necessary information during the performed activities. – have adequate human resources to perform the CFT tasks, with occasional certain deficiencies in this area. – have adequate equipment to perform the activities, – their activities is financed adequately to their needs, with occasional certain deficiencies in this area; c) national cooperation between law enforcement authorities is at an adequate level: – responses provided by the authorities are not limited in terms of scope and type of data or the type of law enforcement authority, – the authorities hold and use the electronic communication channels for fast and secured exchange of most information between each other; d) international cooperation of law enforcement authorities with their foreign counterparts is at a good level: – responses provided by law enforcement authorities are not limited in terms of scope and type of data. – most of the authorities hold and use the electronic communication channels for fast and secured information exchange with their foreign counterparts. 5. The activities of law enforcement authorities are at a good level: a) the authorities demonstrate good awareness of the ML/FT risk. b) the judicial proceedings are conducted in a moderate time (between 1 and 2 years from submitting the indictment to announcing the first instance decision in average). 6. Legal system – the scope of the existing legal regulations mostly corresponds to the scope of the analysed risk and the EU requirements/standards and FATF recommendations.
High vulnerability (3 points)	1. Vulnerability of the economy is at a high level. a) for products and services: – relatively large number of products and services facilitating fast and anonymous transactions, – movements of funds are not secured and monitored in a major part, – relatively large number of financial transactions, including cash transactions and other transactions that could enhance anonymity of their originators and beneficiaries, – relatively large number of international transactions; b) for the entities offering these products and services: – most categories of entities that should be IOs are not subject to the anti-money laundering and countering financing of terrorism (AML/CFT) regulations and to the supervision of the public administration authorities in this area, – OIs are inadequately aware of the obligations imposed on them in the area of AML/CFT. Large amount of information on the potential non-compliance of these OIs with the regulations, – according to the supervisory authorities, the OIs analyse the transactions and apply customer due diligence (CDD) as well as report information on their suspicions to the Polish FIU in an inadequate manner – numerous cases of imposing the financial penalties due to non-compliance of OIs with the AML/CFT regulations. 2. The activities of the supervisory authorities over the OIs are at an inadequate level. a) the supervisory authorities have inadequate financial, human and technical resources to control the OIs; b) the results of the performed controls form the basis to impose administrative penalties and apply other supervisory instruments to the OIs failing to implement with the AML/CFT regulations; c) most of the supervisory authorities provide no information on the performed controls to the Polish FIU; d) cooperation with the other national and foreign supervisory authorities remains at an inadequate level. 3. The Polish FIU activities are at an inadequate level. a) Polish FIU demonstrates inadequate awareness of the ML/FT risk; b) inadequate Polish FIU capability to collect and analyse information on the suspicious operations/transactions (assessed on the basis of the existing powers, human, financial and technical resources): – Polish FIU has direct or indirect access to a part of databases of public administration authorities, necessary to analyse information on the suspicious operations/transactions, – Polish FIU has inadequate powers to receive additional information from the OIs and CUs on request, – only a small part of the analysts are trained in conducting the analyses, – Polish FIU has inadequate human resources to perform the CFT tasks, – Polish FIU has the information system enabling acquisition, collecting and analysing information on the suspicious operations/transactions,

	– the activities of Polish FIU are financed inadequately to its needs; c) international cooperation of Polish FIU with its foreign counterparts is at an inadequate level: – responses provided by Polish FIU are limited in terms of scope and type of data, – average Polish FIU response time exceeds 7 days however does not exceed 30 days from the day of receiving the inquiry, – information obtained from vast majority of the FIUs are not limited in terms of scope and type and data and the average response time exceeds 7 days however does not exceed 30 days from the date of inquiry, – Polish FIU holds and uses the electronic communication channels for fast and secured information exchange with a part of the FIUs, with which it exchanges information, – Polish FIU exchanges information only with a part of the FIUs operating under the Egmont Group; d) national cooperation of Polish FIU is at an inadequate level: – responses provided by Polish FIU are limited in terms of scope and type of data and the type of law enforcement or judicial authority, – average Polish FIU response time exceeds 7 days however does not exceed 30 days from the day of the inquiry, – information obtained from the authorities are not limited in terms of scope and type and data, only a part of the authorities provide information within the time-limit set by the General Inspector of Financial Information (GIFI), – Polish FIU holds and uses the electronic communication channels for fast and secured information exchange with a part of law enforcement authorities. 4. The activities of the law enforcement authorities are at an inadequate level. a) the law enforcement authorities demonstrate limited awareness of the ML/FT risk; b) the law enforcement authorities demonstrate inadequate capability to counter the ML/FT risk (assessed on the basis of the existing powers, human, financial and technical resources): – have powers to acquire a part of the necessary information during the performed activities, – have inadequate human resources to perform the CFT tasks, – have inadequate equipment to perform the activities (deficiencies in quantity or quality), – their activities is financed inadequately to their needs; c) national cooperation between law enforcement authorities is at an inadequate level: – responses provided by the authorities are limited in terms of scope and type of data or the type of law enforcement authority, – the authorities have and use the electronic communication channels for fast and secured exchange of a part of information between each other. d) international cooperation of law enforcement authorities with their foreign counterparts is at an inadequate level: – responses provided by law enforcement authorities are limited in terms of scope and type of data, – a part of the authorities holds and uses the electronic communication channels for fast and secured information exchange with their foreign counterparts. 5. The activities of law enforcement authorities are at an inadequate level. a) the authorities demonstrate inadequate awareness of the ML/FT risk; b) the judicial proceedings are conducted in a long time (between 2 and 3 years from submitting the indictment to announcing the first instance decision in average). 6. Legal system – the scope of the existing legal regulations corresponds only partially to the scope of the analysed risk and the EU requirements/standards and FATF recommendations.
Very high vulnerability (4 points)	1. Vulnerability of the economy is at a very high level. a) for products and services: – definitely large number of products and services facilitating fast and anonymous transactions, – movements of funds are not secured and monitored, – definitely large number of financial transactions, including cash transactions and other transactions that could enhance anonymity of their originators and beneficiaries, – definitely large number of international transactions; b) for the entities offering these products and services: – only a small part of categories of entities that should be IOs are not subject to the anti-money laundering and countering financing of terrorism (AML/CFT) regulations and to the supervision of the public administration authorities in this area, – OIs are unaware of the obligations imposed on them in the area of AML/CFT. Large amount of information on the potential non-compliance of these OIs with the regulations, – according to the supervisory authorities, the OIs fail to analyse the transactions and apply customer due diligence (CDD) as well as report information on their suspicions to the Polish FIU – numerous cases of imposing the financial penalties due to non-compliance of OIs with the AML/CFT regulations. 2. The activities of the supervisory authorities over the OIs are at a definitely low level.

	a) the supervisory authorities have inadequate financial, human and technical resources to control the OIs; b) the results of the performed controls form no basis to impose administrative penalties and apply other supervisory instruments to the OIs failing to implement with the AML/CFT regulations; c) the supervisory authorities provide no information on the performed controls to the Polish FIU; d) cooperation with the other national and foreign supervisory authorities remains at a low level. 3. The Polish FIU activities are at a low level. a) Polish FIU demonstrates no awareness of the ML/FT risk; b) poor Polish FIU capability to collect and analyse information on the suspicious operations/transactions (assessed on the basis of the existing powers, human, financial and technical resources): – Polish FIU has no direct or indirect access to the most of databases of public administration authorities, necessary to analyse information on the suspicious operations/transactions, – Polish FIU has no powers to receive additional information from the OIs and CUs on request, – the analysts are not (or are poorly) trained in conducting the analyses, – Polish FIU has inadequate human resources to perform the CFT tasks. – Polish FIU has no information system enabling acquisition, collecting and analysing information on the suspicious operations/transactions, – the activities of Polish FIU are financed inadequately to its needs; c) international cooperation of Polish FIU with its foreign counterparts is at a low level: – responses provided by Polish FIU are limited in terms of scope and type of data, – average Polish FIU response time exceeds 30 days from the day of receiving the inquiry, – information obtained from vast majority of FIUs are limited in terms of scope and type and data and the average response time exceeds 30 days from the date of inquiry, – Polish FIU holds no electronic communication channels for fast and secured information exchange with the FIUs, or if it holds such channels, it does not use them, – Polish FIU exchanges information only with the FIUs of the EU Member States; d) national cooperation of Polish FIU is at a low level: – responses provided by Polish FIU are limited in terms of scope and type of data and the type of law enforcement or judicial authority, – average Polish FIU response time exceeds 30 days from the day of the inquiry. – information obtained from the authorities are not limited in terms of scope and type and data, most of the authorities fail to provide information within the time-limit set by the General Inspector of Financial Information (GIFI), – Polish FIU holds no electronic communication channels for fast and secured information exchange with the law enforcement authorities, or if it hold such channels, it does not use them. 4. The activities of the law enforcement authorities are at a low level. a) the law enforcement authorities demonstrate no awareness of the ML/FT risk; b) the law enforcement authorities demonstrate poor capability to counter the ML/FT risk (assessed on the basis of the existing powers, human, financial and technical resources): – have powers to acquire a small part of the necessary information during the performed activities, – have inadequate human resources to perform the CFT tasks, – have inadequate equipment to perform the activities (significant deficiencies in quantity or quality), – their activities is financed inadequately to their needs; c) national cooperation between law enforcement authorities is at a low level: – responses provided by the authorities are significantly limited in terms of scope and type of data and the type of law enforcement authority, – the authorities have no electronic communication channels for fast and secured exchange of a part of information between each other or if they hold such channels, they do not use them; d) international cooperation of law enforcement authorities with their foreign counterparts is at a low level: – responses provided by law enforcement authorities are significantly limited in terms of scope and type of data, – the authorities hold no electronic communication channels for fast and secured information exchange with their foreign counterparts, or if they hold such channels, they do not use them. 5. The activities of law enforcement authorities are at a low level. a) the authorities demonstrate no awareness of the ML/FT risk; b) the judicial proceedings are conducted in a very long time (above 3 years from submitting the indictment to announcing the first instance decision in average). 6. Legal system – the scope of the existing legal regulations corresponds only in a small part to the scope of the analysed risk and the EU requirements/standards and FATF recommendations.

The level of probability shall be assessed on the basis of the estimated levels of threat and vulnerability as presented below.

Table 3 – Level of ML probability calculation method for the purposes of "inherent risk" assessment



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

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

where: P_{prp} – Level of ML probability for the purposes of "inherent risk" assessment, Z_{rp} – level of ML threat for the purposes of "inherent risk" assessment", P_{rp} – level of ML vulnerability for the purposes of "inherent risk" assessment".[6]

The next step includes the determination of the level of ML consequences for the purposes of "inherent risk" assessment according to the scheme presented in Table 4. In order to determine the level of consequences, the first step is to check whether there have been any socio-economic and political consequences. The second step is to estimate the level of consequences on the basis of available information in these categories in the scope of descriptions in the individual rows of the table below.

Table 4 –The levels of ML consequences for the purposes of "inherent risk" assessment

Level of consequences	Characteristics of the level of consequences[7]
Minor consequences (1 point)	No visible social, economic and political consequences.
Moderate consequences (2 points)	1. Presence of short-term (up to 1 year) socio-economic consequences: – increased criminal activities, – increased overall amount of illegal proceeds legitimised in the country or/and transferred abroad, – increased costs of operation of the public and private sector entities linked to ensuring the security of their operation and of the society,

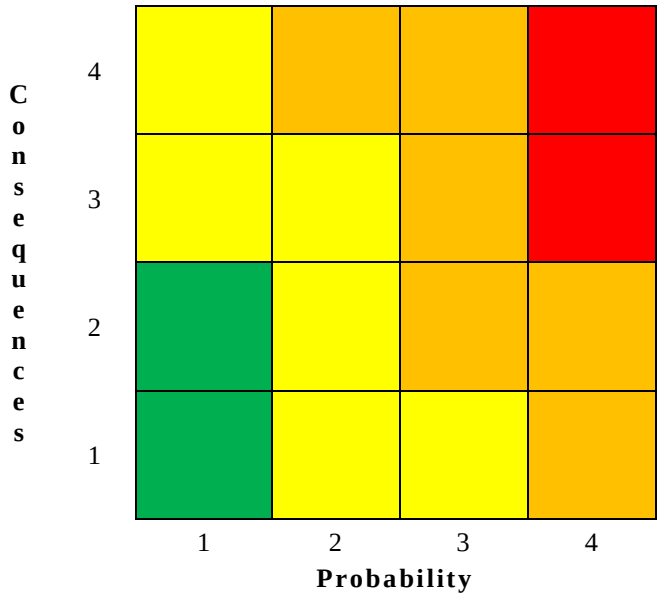
[6] The weight adopted for the level of vulnerability is higher due to the fact that even if there is a high threat of money laundering, the probability of money laundering depends to a greater extent from the vulnerability of the AML/CFT system, which should counteract the realisation of these threats. Based on expert knowledge, it could be assumed that the higher level of vulnerability, the greater "attractiveness" of the country, and therefore more probable benefiting from the money laundering opportunities, which ultimately affects the level of risk.

[7] In order to assign the level of moderate or significant or severe consequences, at least 4 conditions listed in the subpoints should be present (including – in the cases of the conditions listed at the significant and severe consequences levels – at least 1 condition present in point 2).

	– decreased public sector income.
Significant consequences (3 points)	1. Presence of short-term (up to 1 year) socio-economic consequences: – increased criminal activities, – increased overall amount of illegal proceeds legitimised in the country or/and transferred abroad, – increased costs of operation of the public and private sector entities linked to ensuring the security of their operation and of the society, – decreased public sector income. 2. Presence of short-term (up to 1 year) political consequences: – increased popularity of the country as a "haven" for criminal activity, – decreased credibility of the country on the international front, – imposing political and economic sanctions on the country.
Severe consequences (4 points)	1. Presence of long-term (above 1 year) socio-economic consequences: – increased criminal activities, – increased overall amount of illegal proceeds legitimised in the country or/and transferred abroad, – increased costs of operation of the public and private sector entities linked to ensuring the security of their operation and of the society, – decreased public sector income. 2. Presence of long-term (above 1 year) political consequences: – increased popularity of the country as a "haven" for criminal activity, – decreased credibility of the country on the international front, – imposing political and economic sanctions on the country.

The last step involves the estimation of the "inherent risk" level as presented below.

Table 5 –ML "inherent risk" level calculation method



Inherent 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: $R_{rp}=60\%*P_{prp}+40\%*K_{rp}$

Where: R_{rp}– "inherent risk" level, P_{prp} – Level of ML probability for the purposes of "inherent risk" assessment, K_{rp} – level of ML consequences for the purposes of "inherent risk" assessment".[8]

ML "residual risk"

Estimating the "residual risk" shall be based primarily on estimating the levels of threat and vulnerability for each product and service in the area concerned. These will form the basis to calculate the average level of threat and level of vulnerability for the area concerned.

The level of threat for each product/service shall be rated on a scale from 1 (minimum) to 4 (maximum). The threat level assessment shall include two components: intent of the perpetrators and their opportunities and capacities for successful transfer of illegitimate or legitimate funds for money laundering purposes.

Table 6 – Levels of threat

Level of threat	Characteristics of the level of threat
Low threat (1 point)	No information that the perpetrators are capable of (or intend to) using the analysed product/service and have relevant resources to do so. This method of operation is perceived by the perpetrators as unattractive and highly unsafe. It is very difficult to apply due to the necessary planning, specialist knowledge and skills. Using the other methods of operation (alternative to the analysed product/service) is less cost-consuming.
Medium threat (2 points)	There is few information that the perpetrators are capable of (or intend to) using the analysed product/service and have relevant resources to do so. The analysed product/service is perceived by the perpetrators as unattractive and unsafe. It is difficult to apply due to the necessary planning, specialist knowledge and skills. Using the other methods of operation (alternative to the analysed product/service) may be less cost-consuming.
High threat (3 points)	There is information that the perpetrators use the analysed product/service and have relevant resources to do so. The analysed product is perceived by the perpetrators as rather attractive (including in terms of finance) and relatively safe. Using this product/service requires medium capabilities in terms of planning, knowledge and skills.

[8] The weight adopted for the level of probability is higher due to the fact that it is a function of both the level of threat and of vulnerability and therefore should have a stronger impact on determining the level of inherent risk compared to the level of consequences.

Very high threat (4 points)	There is information that the perpetrators periodically use the analysed product/service. This method of operation is widely available and its use is relatively less cost-consuming compared to the other products/services. The analysed product/service is perceived by the perpetrators as attractive and safe. It requires minor planning, knowledge and skills.

The level of vulnerability of the system for each product/service shall be estimated also on the scale from 1 (minimum) to 4 (maximum). The weaknesses will be estimated on the basis of analysis of presence and effectiveness of the existing safeguards, with consideration to the legal status (in particular in the scope of the financial market regulations, powers of the units of the national AML/CFT system), information on the practical operation of the financial market and of the national AML/CFT system.

Table 7 – Levels of vulnerability

Level of vulnerability	**Characteristics of the level of vulnerability in order to assign a specific risk level, the conditions set out in at least 2 of 4 assigned items should be met[9]**
Low vulnerability (1 point)	1. Specific features of a product/service: a) the products and services concerned are hardly available, b) the products and services concerned provide no opportunities for hiding data of the entities using them, c) the products and services concerned provide no opportunity of making international transactions. 2. The activity of entities offering products and services: a) all entities offering the products and entities are OIs; b) OIs demonstrate the appropriate level of awareness of the obligations imposed on them in the area of AML/CFT. None or relatively limited amount of information on non-compliance of operation of these OIs with the AML/CFT regulations; c) according to the supervisory authorities, the OIs effectively analyse the transactions and apply customer due diligence (CDD) as well as report information on their suspicions to the Polish FIU. 3. The activity of the public administration authorities and units: a) the public administration authorities have sufficient risk assessment on money laundering and terrorism financing (ML/FT). The law enforcement authorities have relatively high capability to prevent the ML/FT risk linked to the product/service concerned (i.e. there is high probability of detecting the ML/FT case, followed by – in effect of an investigation/inquiry – a prosecution and conviction of the perpetrators); b) relatively high capability of Polish FIU to collect information on the suspicious operations/transactions from the OIs and CUs, detect and analyse the cases of suspected ML/FT in the scope of the analysed product/service (assessed on the basis of held powers, human, financial and technical resources). 4. Legal system – the existing regulations correspond to the scope of the analysed scenario.
Medium vulnerability (2 points)	1. Specific features of a product/service: a) access to the products and services concerned is impeded, b) the products and services concerned provide some opportunities for hiding data of the entities using them, c) the products and services concerned enable making international transactions. 2. The activity of entities offering products and services: a) most of the entities offering the products and entities used under the scenario are OIs; b) OIs covered by the scope of the analysed scenario, demonstrate the awareness of the obligations imposed on them in the area of AML/CFT. There is some information on non-compliance of operation of these OIs with the AML/CFT regulations; c) according to the supervisory authorities, the OIs analyse the transactions and apply customer due diligence (CDD), however there is information on deficiencies in the identification and verification of customers. The OIs report relatively few information on their suspicions to the Polish FIU. 3. The activity of the public administration authorities and units: a) the public administration authorities have risk assessment on ML/FT. The law enforcement authorities are capable of preventing the ML/FT risk linked to the scenario concerned (i.e. there is high probability of detecting the ML/FT case, followed by – in effect of an investigation/inquiry – a prosecution and conviction of the perpetrators);

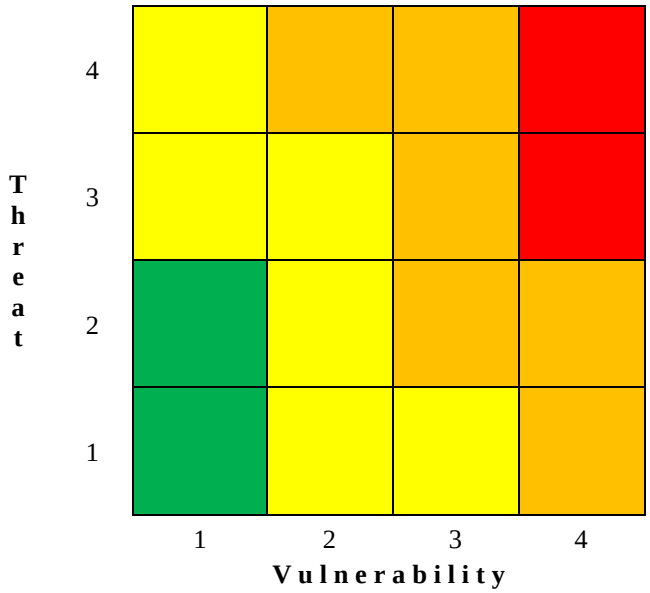
[9] If the conditions assigned to the lower and higher level are identified, they can be averaged (for example, from the level of low vulnerability and the level of high vulnerability – to the level of medium vulnerability

	b) Polish FIU is capable of collecting information on the suspicious operations/transactions from the OIs and CUs, detecting and analysing the cases of suspected ML/FT in the scope of the analysed scenario (assessed on the basis of held powers, human, financial and technical resources). 4. Legal system – the existing regulations largely correspond to the scope of the analysed scenario.
High vulnerability (3 points)	1. Products and services available for use under the *modus operandi*: a) access to the products and services concerned is relatively easy, b) the products and services concerned provide certain opportunities for hiding data of the entities using them, c) the products and services concerned enable making international transactions. 2. The activity of entities offering products and services available for use under the *modus operandi*: a) only a part of the entities offering the products and entities used under the scenario is OIs; b) OIs covered by the scope of the analysed scenario, demonstrate the relatively low awareness of the obligations imposed on them in the area of AML/CFT. There is relatively large amount of information on non-compliance of operation of these OIs with the AML/CFT regulations; c) according to the supervisory authorities, the OIs analyse the transactions and apply customer due diligence (CDD) to a relatively low extent. There is relatively large amount of information on deficiencies in the identification and verification of customers. The OIs report relatively few information on their suspicions to the Polish FIU. 3. The activity of the public administration authorities and units: a) the public administration authorities have a limited risk assessment on ML/FT. The law enforcement authorities have relatively low capability to prevent the ML/FT risk linked to the scenario concerned (i.e. there is probability of not detecting the ML/FT case or, if detected, that the investigation/inquiry will not lead to prosecution and conviction of the perpetrators); b) Polish FIU is capable of collecting information on the suspicious operations/transactions from the OIs and CUs, detecting and analysing the cases of suspected ML/FT in the scope of the analysed scenario only to a limited extent (capabilities assessed on the basis of held powers, human, financial and technical resources). 4. Legal system – the existing regulations fail to correspond to the scope of the analysed scenario to a great extent.
Very high vulnerability (4 points)	1. Products and services available for use under the *modus operandi*: a) access to the products and services concerned is common, b) the products and services concerned enable hiding data of the entities using them, c) the products and services concerned enable making international transactions. 2. The activity of entities offering products and services available for use under the *modus operandi* – these entities are not the OIs. 3. The activity of the public administration authorities and units: a) the public administration authorities have no risk assessment on ML/FT. The law enforcement authorities have definitely low capability to prevent the ML/FT risk linked to the scenario concerned (i.e. there is high probability of not detecting the ML/FT case or, if detected, that the investigation/inquiry will not lead to prosecution and conviction of the perpetrators); b) Polish FIU is not capable of collecting information on the suspicious operations/transactions from the OIs and CUs, detecting and analysing the cases of suspected ML/FT in the scope of the analysed risk only to a very limited extent (capabilities assessed on the basis of held powers, human, financial and technical resources). 4. Legal system – the existing regulations fail to correspond to the scope of the analysed scenario.

The "residual risk" shall be estimated under the assumption that the ML consequences (considered as a third risk estimation component accompanying threat and vulnerability) are not to be calculated separately due to difficulties in differentiating them for the individual products/services or areas. Their estimation shall the same as for the level inherent risk of money laundering.

The level of probability shall be estimated on the basis of the estimated levels of threat and vulnerability assigned to the areas (calculated as an arithmetic mean of the levels of threat and vulnerabilities estimated for the individual products/services in the area concerned).

Table 8 – Probability calculation method



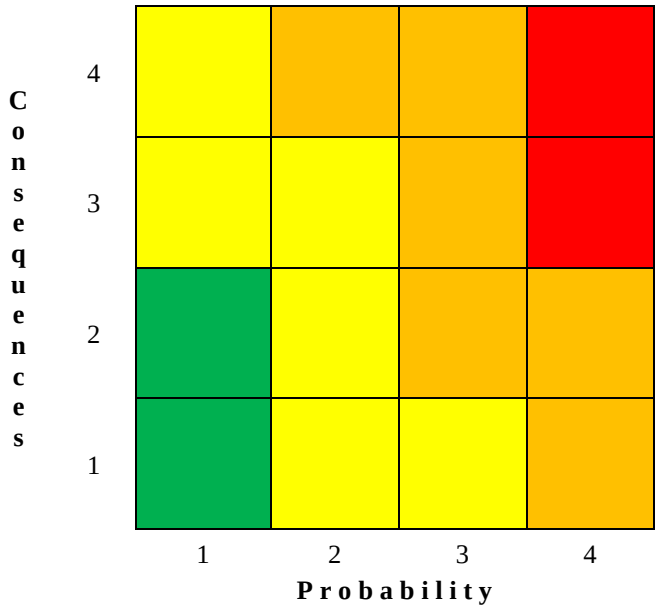
Level of probability	
very high probability	3.6-4
high probability	2.6-3.5
medium probability	1.6-2.5
low probability	1-1.5

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

Where: P_{prs} – Level of probability, Z_{ps} – level of threat, P_{ps} – level of vulnerability.[10]

The next stage involves the estimation of the risk level for the area concerned as presented below.

Table 9 – Method of risk level calculation for the area concerned



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

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

[10] The weight adopted for the level of vulnerability is higher due to the fact that even if there is a high threat of money laundering, the probability of money laundering depends to a greater extent from the vulnerability of the AML/CFT system, which should counteract the realisation of these threats. Based on expert knowledge, it could be assumed that the level of vulnerability most probably increases the attractiveness of the area concerned or products and services offered in the area, and therefore the intent of the perpetrators in this scope - which ultimately affects the level of risk

Where: R_{ps}– Level of risk, P_{prs} – Level of probability, K_{rp} – Level of ML consequences for the purposes of "inherent risk" assessment" (i.e. calculated for the ML inherent risk level).[11]

The last stage involves the estimation of "residual risk" of money laundering on the basis of arithmetic mean of the levels of risk assigned to the individual areas.

ML "overall risk"

Estimation of the ML "overall risk" would include correlation of the estimated "residual risk" with the estimated "inherent risk" as follows:

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

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

The estimated "residual risk" level shall have assigned a twice higher weight, due to the fact that it is based on information on the specific methods used or that could be used for ML. This information can be also easier confronted with data on the activities of the entities operating under the national AML/CFT system, as well as legal regulations to assess the level of vulnerability on their implementation. Therefore, the level of "residual risk" is probably better estimated compared to the level of "inherent risk", which is mostly based on general information.

FT risk estimation – assumptions

FT "inherent risk"

The level of FT threat for the purposes of the "inherent risk" assessment will be assessed following the scheme presented in Table 10. Each itemised component identified in the table below is assessed separately. The level of threat will be estimated on the basis of arithmetic mean from their assessments.

Table 1 – The levels of FT threats for the purposes of "inherent risk" assessment

Level of threat	**Characteristics of the level of threat** ***(in order to assign a specific risk level, the conditions set out in at least 3 of 4 assigned items should be met)***[12]
Low threat (1 point)	1. The level of estimated assets used for FT in annual scale: x < 0.000005%*GDP. 2. The risk of terrorism financing in the EU is determined at low level. 3. Information derived from a single source on the possible use of Poland for acquisition or transfer of assets for terrorist purposes. 4. Threat of occurrence of a terrorist event in Poland. 5. No alert state referred to in Article 15 of the *Act of 10 June 2016 on anti-terrorist activities* is implemented in Poland.
Medium threat (2 points)	1. The level of estimated assets used for FT in annual scale:0.000005%*GDP < x < 0.000025%*GDP 2. The risk of terrorism financing in the EU is determined at medium level. 3. Information derived from several sources on the possible use of Poland for acquisition or transfer of assets for terrorist purposes. 4. Threat of occurrence of a terrorist event in Poland. 5. One of the following alert states referred to in Article 15 of the *Act of 10 June 2016 on anti-terrorist activities* is implemented in Poland: ALFA, ALFA-CRP.
High threat (3 points)	1. The level of estimated assets used for FT in annual scale: 0.000025%*GDP < x < 0.00005%*GDP 2. The risk of terrorism financing in the EU is determined at high level.

[11] The weight adopted for the level of probability is higher due to the fact that it is a function of both the level of threat and of vulnerability and therefore should have a stronger impact on determining the level of inherent risk compared to the level of consequences.

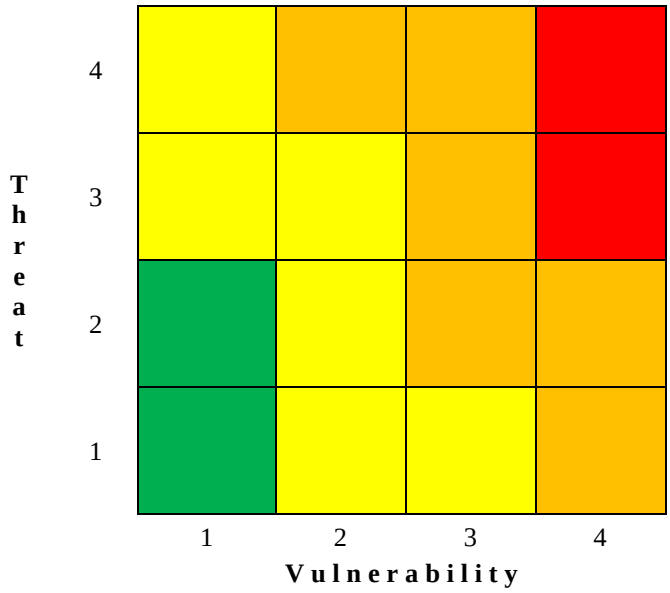
[12] If the conditions assigned to the lower and higher level are identified, they can be averaged (for example, from the level of low threat and the level of high threat – to the level of medium threat).

	3. Information derived from a single source on the possible use of Poland for acquisition or transfer of assets for terrorist purposes. 4. Threat of occurrence of a terrorist event in Poland. 5. One of the following alert states referred to in Article 15 of the *Act of 10 June 2016 on anti-terrorist activities* is implemented in Poland: BRAVO, BRAVO-CRP.
Very high threat (4 points)	1. The level of estimated assets used for FT in annual scale: x > 0.00005%*GDP 2. The risk of terrorism financing in the EU is determined at very high level. 3. Information derived from different sources on the possible use of Poland for acquisition or transfer of assets for terrorist purposes. 4. Threat of occurrence of a terrorist event in Poland. 5. One of the following alert states referred to in Article 15 of the *Act of 10 June 2016 on anti-terrorist activities* is implemented in Poland: CHARLIE, CHARLIE-CRP, DELTA, DELTA-CRP.

The level of FT vulnerability for the purposes of the "inherent risk" assessment will be assessed following the scheme presented in Table 2.

The level of probability shall be assessed on the basis of the estimated levels of threat and vulnerability as presented below.

Table 11 – Level of ML probability calculation method for the purposes of "inherent risk" assessment



Level of probability	
very high probability	3.6-4
high probability	2.6-3.5
medium 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} – Level of FT probability for the purposes of "inherent risk" assessment, Z_{rp_ft} – level of FT threat for the purposes of "inherent risk" assessment", P_{rp_ft} – Level of FT vulnerability for the purposes of "inherent risk" assessment".[13]

The next step includes the determination of the level of FT consequences for the purposes of "inherent risk" assessment according to the scheme presented in Table 12. In order to determine the level of consequences, the first step is to check whether there have been any socio-economic and political consequences. The second step is to estimate the level of consequences on the basis of available information in these categories in the scope of descriptions in the individual rows of the table below.

Table 12 – The levels of FT consequences for the purposes of "inherent risk" assessment

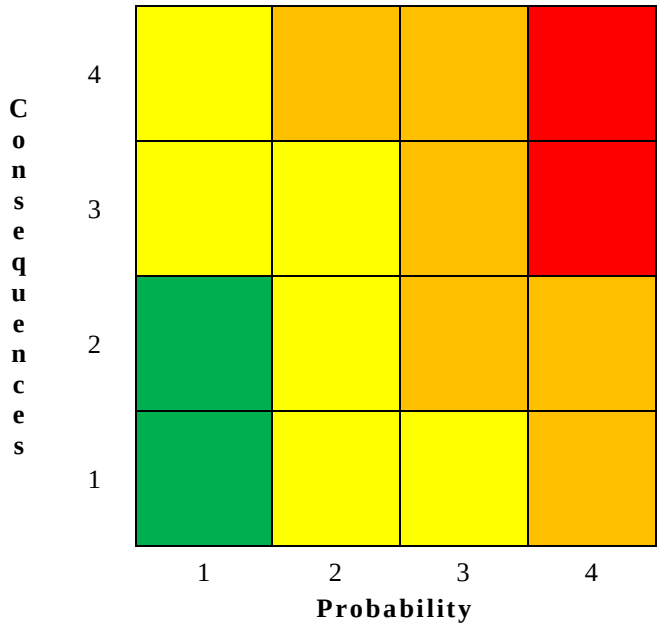
[13] The weight adopted for the level of vulnerability is higher due to the fact that even if there is a high threat of terrorism financing, the probability of terrorism financing depends to a greater extent from the vulnerability of the AML/CFT system, which should counteract the realisation of these threats. Based on expert knowledge, it could be assumed that the higher level of vulnerability, the greater "attractiveness" of the country, and therefore more probable benefiting from the terrorism financing opportunities, which ultimately affects the level of risk.

Level of consequences	Characteristics of the level of consequences[14]
Minor consequences (1 point)	No visible social, economic and political consequences.
Moderate consequences (2 points)	Presence of short-term (up to 1 year) socio-economic consequences: – increased terrorist activity in the country, – increased criminal activities financing the terrorist activity, – increased overall amount of illegal proceeds legitimised in the country or/and transferred abroad, – increased costs of operation of the public and private sector entities linked to ensuring the security of their operation and of the society, – decreased public sector income.
Significant consequences (3 points)	1. Presence of short-term (up to 1 year) socio-economic consequences: – increased terrorist activity in the country, – increased criminal activities financing the terrorist activity, – increased overall amount of illegal proceeds legitimised in the country or/and transferred abroad, – increased costs of operation of the public and private sector entities linked to ensuring the security of their operation and of the society, – decreased public sector income. 2. Presence of short-term (up to 1 year) political consequences: – increased popularity of the country as a "haven" for criminal activity, – decreased credibility of the country on the international front, – imposing political and economic sanctions on the country.
Severe consequences (4 points)	1. Presence of long-term (above 1 year) socio-economic consequences: – increased terrorist activity in the country, – increased criminal activities financing the terrorist activity, – increased overall amount of illegal proceeds legitimised in the country or/and transferred abroad, – increased costs of operation of the public and private sector entities linked to ensuring the security of their operation and of the society, – decreased public sector income. 2. Presence of long-term (above 1 year) political consequences: – increased popularity of the country as a "haven" for criminal activity, – decreased credibility of the country on the international front, – imposing political and economic sanctions on the country.

The last step involves the estimation of the "inherent risk" level as presented below.

[14] In order to assign the level of moderate or significant or severe consequences, at least 4 conditions listed in the subpoints should be present (including – in the cases of the conditions listed at the significant and severe consequences levels – at least 1 condition present in point 2).

Table 13 – FT "inherent risk" level calculation method



Inherent 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: $R_{rp\_ft}=60\%*P_{prp\_ft}+40\%*K_{rp\_ft}$

Whee: R_{rp_ft}– "inherent risk" level, P_{prp_ft} – Level of FT probability for the purposes of "inherent risk" assessment", K_{rp_ft} – level of FT consequences for the purposes of "inherent risk" assessment".[15]

FT "residual risk"

Estimating the "residual risk" shall be based primarily on estimating the levels of threat and vulnerability for each product and service in the area concerned. These will form the basis to calculate the average level of threat and level of vulnerability for the area concerned.

The level of threat for each product/service shall be rated on a scale from 1 (minimum) to 4 (maximum). The threat level assessment shall include two components: intent of the perpetrators and their opportunities and capacities for successful transfer of illegitimate or legitimate funds for FT purposes. The assessment shall be conducted on the basis of the scheme presented in Table 6.

The level of vulnerability of the system for each product/service shall be estimated also on the scale from 1 (minimum) to 4 (maximum). The weaknesses will be estimated on the basis of analysis of presence and effectiveness of the existing safeguards, with consideration to the legal status (in particular in the scope of the financial market regulations, powers of the units of the national anti-money laundering/counter-terrorism financing system), information on the practical operation of the financial market and of the national AML/CFT system. The level of vulnerability shall be estimated on the basis of the scheme presented in Table 7.

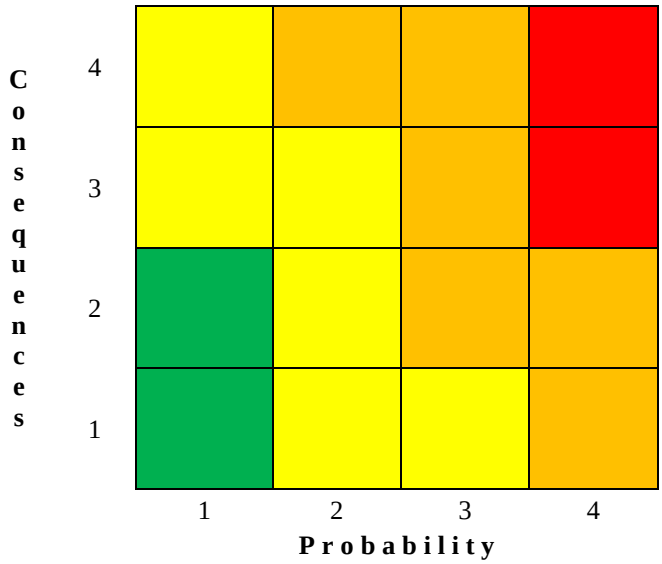
The "residual risk" shall be estimated under the assumption that the FT consequences (considered as a third risk estimation component accompanying threat and vulnerability) are not to be calculated separately due to difficulties in differentiating them for the individual products/services or areas. Their estimation shall the same as for the level inherent risk of terrorism financing.

[15] The weight adopted for the level of probability is higher due to the fact that it is a function of both the level of threat and of vulnerability and therefore should have a stronger impact on determining the level of inherent risk compared to the level of consequences.

The level of probability shall be estimated on the basis of the estimated levels of threat and vulnerability assigned to the areas (calculated as an arithmetic mean of the levels of threat and vulnerabilities estimated for the individual products/services in the area concerned).

The next stage involves the estimation of the risk level for the area concerned as presented below.

Table 14 – FT "residual risk" level calculation method



Level of residual risk	
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: $R_{s\_ft}=60\%*ML_{\_ft}+40\%*K_{rp\_ft}$

Where: R_{s_ft}– Level of risk, $ML_{\_ft}$ – Level of probability, K_{rp_ft} – Level of FT consequences for the purposes of "inherent risk" assessment (calculated for the FT inherent risk level).[16]

The last stage involves the estimation of FT "residual risk" on the basis of arithmetic mean of the levels of risk assigned to the individual areas.

FT "overall risk"

Estimation of the FT "overall risk" would include correlation of the estimated "residual risk" with the estimated "inherent 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 "inherent risk", R_{S_ft} – level of "residual risk".

The estimated "residual risk" level shall have assigned a twice higher weight, due to the fact that it is based on information on the specific methods used or that could be used for FT. This information can be also easier confronted with data on the activities of the entities operating under the national AML/CFT system, as well as legal regulations to assess the level of vulnerability on their implementation. Therefore, the level of "residual risk" is probably better estimated compared to the level of "inherent risk", which is mostly based on general information.

[16] The weight adopted for the level of probability is higher due to the fact that it is a function of both the level of threat and of vulnerability and therefore should have a stronger impact on determining the level of inherent risk compared to the level of consequences. Based on expert knowledge, it could be assumed that level of vulnerability most probably increases the attractiveness of a given area or the offered products or services, and therefore the intention of the offenders in this scope – thus ultimately affecting the level of risk.

The obtained value of “overall risk” shall be assigned to the specific level of risk using the following intervals:

- 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>.