



Ministero dell'Economia e delle Finanze
Financial Security Committee

**Analysis of Italy's national money-laundering
and terrorist financing risks**

METHODOLOGY

Contents

1. Introduction	3
2. Methodology	5
2.1 Data source	5
2.2 Overview - Threats, vulnerabilities, and consequences	6
2.3 Identification of Money-Laundering (ML) and Terrorist Financing (TF) risks	8
2.3.1 Analysis model: Money-Laundering (ML) risks	8
2.3.1.1 Assessing ML inherent risk in the system	10
2.3.1.2 Effectiveness of preventive, investigative and repressive safeguards. Vulnerability analysis	14
2.3.2 Terrorist Financing (TF) risk – Analysis model	29
3. Glossary	32

ANALYSIS OF ITALY'S NATIONAL MONEY-LAUNDERING

AND TERRORIST FINANCING RISKS

METHODOLOGY

Rome, 2014 July

1. Introduction

The 2014 National Risk Assessment is the first exercise carried out by Italy on the national assessment of the risks of money-laundering and terrorist financing. The assessment is made on the basis of this Methodology.

The exercise consists in identifying and analysing the risks of money-laundering and terrorist financing, aimed at the development of intervention guidelines for mitigation of the same and adoption of a risk-based approach to the activity of AML/CFT (anti-money laundering and countering the financing of terrorism). This approach requires that AML/CFT policies and measures be carried out in proportion to the risks they face¹.

The first assessment is of an experimental nature, and will be updated after three years, in order to take into account the forthcoming evolution of the Community and national regulatory frameworks, as well as indications arising from supervisory authorities, investigations carried out by police forces and analysis made by the FIU. Subsequently, the national analysis will be updated every five years.

The analysis could also be conducted in case of emerging threats or vulnerabilities of particular relevance.

It is a complex process that requires the preliminary definition of the pursued objectives and scope in which to conduct the analysis, as well as the definition of specific procedures agreed with the plurality of actors involved.

The purpose of the exercise is to attain national understanding of:

- 1) threats of money-laundering and terrorist financing, by identifying the most relevant ones;
- 2) methods mainly used for carrying out such criminal activities;
- 3) vulnerabilities in the national system of prevention, investigation and prosecution of such phenomena, and therefore the sectors most exposed to such risks;
- 4) the actions to be initiated and their priorities.

The analysis is conducted by differentiating the assessment on money-laundering from the assessment on terrorist financing; in both cases the assessment is carried out at the national level.

The National Risk Assessment is conducted by Italy's Financial Security Committee (*Comitato di Sicurezza Finanziaria - CSF*). The CSF involves within specific thematic meetings further administrations on issues falling within their direct competences. At its 28 February 2013 meeting, the CSF established an *ad-hoc* Working Group to develop an analysis method proposal and perform the assessment². The Working Group is composed of all the authorities present in CSF and representatives of Italy's Presidency of the Council of Ministers. Coordination by the CSF is indicative of the high degree of

¹ FATF Recommendation 1.

² These are the terms of reference of the Working Group. The Group identifies and collects data necessary to carry out the analysis. In general, the mapping of the risks of money-laundering and terrorist financing requires availability of data from different sources, such as police forces, intelligence, FIU, supervisory authorities within their competence fields, financial institutions and professionals, Ministry of Justice, ISITAJ and the private sector. The Group noted such limitations in data collection can affect the quality of the analysis to be performed, in order to suggest improvements. The Group also considers whether there are any limits to the exchange of relevant information between authorities. The Group aims to develop a methodology for conducting periodic National Risk Assessments. To such end, the Group identifies the actors who can contribute to risk analysis; model identification, analysis and risk assessment; forms and procedures for involvement of the private sector. The Group will also consider how to use the results from authorities, in order to direct policy decisions and resource allocation, and financial institutions and other obliged parties in support to their specific business risk analysis.

coordination of the Italian authorities involved in the assessment and the related objectives³.

The risk analysis will take into account additional risk analyses, whereby elaborated at the supranational level.

The private sector is involved in risk analysis development: in particular, trade associations and private institutions are invited to share their experiences on the field and their assessments on specific topics identified over time.

The assessment output consists of the preparation of a document for authorities and competent administrations in the field of AML/CFT.

The CSF determines which results of the Report are to be shared with the private sector (industry associations and professional associations), so that the *obliged parties* will have information relevant to conduct the respective risk assessment activities.

³ The Group met regularly and informed of developments within CSF activities at each CSF meeting. The CSF from time to time suggested analysis profiles on which necessary investigations were carried out, thus integrating the Methodology accordingly.

This document was then shared with experts and academics to assess its robustness. As a result of the comments made on the occasion of this meeting, and the assessment of its first application, the final version of the Methodology was prepared, approved by the CSF in its 18 July 2014 meeting.

2. Methodology

The analysis aims to identify, analyse and assess Italy's ML/FT main risks at national level, through the examination of their causes, as well as vulnerabilities that allow such risks to arise and their related consequences.

The money-laundering definition underlying the Methodology is that referred to in Italy's Legislative Decree n. 231/2007, which also includes self-laundering assumptions. As this definition does not coincide with the definition provided by the Penal Code, this gap shall be taken into account in the assessment of judicial data.

The definition of terrorist financing is that referred to in Article. 1(a) of Italy's Legislative Decree n. 109/2007.

The information available and utilised is accurate, both statistical and of other nature, and represents a necessary starting point for our analysis; yet, such information is not exhaustive, as data need to be contextualised and interpreted by the *ad-hoc* Group of Experts in order to adequately identify, analyse and assess both threats and vulnerabilities.

In this regard, "Experts Opinion" is to be intended as the opinion issued by the Working Group, or by the CSF, whereby each participant issues the assessments of the authority to which they belong. The Group composition has been enhanced with additional representatives from participating authorities in relation to the specific subjects discussed.

The risk analysis is conducted at the national level. Nevertheless, a risk indicator is also provided so as to guide relevant authorities and operators in their respective choices for supervision and definition of anti-money laundering safeguards whereby they depend on local factors.

2.1 Data source

Information collection is a strategic component of analysis, which needs to be properly monitored and reinforced. Collection is organised by individual authorities. The analysis carried out is based on assessments based both on public information and confidential information. By way of example, it is possible to identify certain types of information provided by members of the group in charge of collecting it:

- Judiciary type information, both of a qualitative nature, relatively to significant investigation of money-laundering and financing of terrorism, or of offences deemed as notably indicative (so-called *alert offences*), as well as of a quantitative nature⁴;

⁴ 1 [...] "terrorist financing" means "any activity directed by any means, to the collection, provision, brokerage, deposit, custody of funds or economic resources, in whatever way made, intended to be, in whole or in part, used in order to accomplish one or more crimes of terrorism under the Criminal Code, regardless of the actual use of funds and economic resources for the purposes addressed".

⁵ For money-laundering, for instance:
• number of cases registered for the offences referred to in Articles 648-bis and 648-ter Penal Code;
• number of investigations concluded with the prosecution;

⁶ For terrorist financing (even if not definitive) for the offences referred to in Articles 648-bis and 648-ter Penal Code:

• the number of persons prosecuted and convicted (even on a non-definitive basis);

• approximate value of seized and confiscated proceedings of money-laundering.

For the financing of terrorism, for instance:

• number of proceedings initiated for the offence of financing of terrorism, distinguishing, where possible, between domestic terrorism and international terrorism;

• number of investigations concluded the prosecution;

• number of convictions (even if not definitive) for the offence of financing of terrorism;

- Financial estimates on proceeds from money-laundering predicate offences, as well as on money-laundering and terrorist financing;
 - Cases or typologies of criminal conducts identified by the police and the FIU;
 - Information on obliged parties;
 - Information, both of a qualitative and quantitative nature in relation to the type, frequency and seriousness of the irregularities identified, processed by the relevant Supervisory Authorities on the basis of anti-money laundering checks carried out;
 - Information on penalties imposed (sanctions);
 - Information on the number and quality of suspicious transaction reports;
 - Qualitative and quantitative information on cooperation between national authorities and between those authorities and foreign authorities.
- The analysis furthermore considers reports drawn up by international bodies, academic studies, and specialised press.

2.2 Overview - Threats, vulnerabilities, and consequences

In general, the risk of an event depends on the likelihood the event will occur and the consequences⁵; it will determine, as the higher the risk the greater the probability the event will occur and the more serious its consequences. The likelihood is in turn a function of the presence of threats⁶ that can produce a phenomenon of money-laundering or financing of terrorism and the vulnerabilities⁸ of a system.

The model adopted mainly manages information related to threats and vulnerabilities. Consequences are assessed in a timely context: an assessment of impacts attributable to the threats (i.e. financial consequences and negative social value associated with each predicate offences). This, by reason of a specific methodological choice: it is believed, in fact, that the lack of some analytical data does not always allow for accurate assessment of the impacts and that an estimate of their intensity would have the effect to make the ratings considerably arbitrary.

The logical structure of the model aggregates the analysis of threats and vulnerabilities through the assessment of inherent risk and AML/CFT effectiveness.

In particular, the model encompasses:

- a) assessment of the inherent risk of money-laundering and terrorist financing of the system, through identification of threats and vulnerabilities of the socio-economic system;
- b) assessment of the effectiveness of the AML/CFT regime as to the:

- a. Preventive phase;
- b. Investigative phase; and
- c. Repressive phase.

• the number of persons prosecuted and convicted (even on a non-definitive basis);

• number of seizures and confiscations;

• approximate value of seized and confiscated assets.

For predicate offences, for instance:

• number of reports and arrests;

• The consequences relate to the effects arising from the occurrence of risk events.

7 The threats are the causes that can lead to money-laundering and terrorist financing, and are related to the nature and quantity of illegally acquired proceeds that could be laundered.

8 Vulnerabilities are weaknesses whose exploitation allows threats to be translated into money-laundering and terrorist financing.

Within such phases, the model analyses their respective vulnerabilities. With regard to the vulnerability of the preventive phase, the model performs a sectoral analysis⁹ for each category of recipients of anti-money laundering regulations: financial intermediaries, professions and non-financial operators. These categories are further detailed. The analysis can also be extended to non-required application of money-laundering legislation whereby attention however is required.

In light of the inherent risk, the lower vulnerabilities identified in the preventive, investigative and repressive phases, the more effective safeguards in place are in mitigating such inherent risk.

The model differentiates the analysis on money-laundering from the analysis on the financing of terrorism. The latter derives from the former, as amended - whereby necessary - in order to take account of the related factual and regulatory peculiarities.

2.3 Identification of Money-Laundering (ML) and Terrorist Financing (TF) risks

2.3.1 Analysis model: Money-Laundering (ML) risks

The ML analysis model is developed as follows:

- I. Determination of ML inherent risk in the system
 - a. Presence of the proceeds of criminal activities carried out on national territory
 - i. Analysis of offences
 - b. Presence of proceeds from criminal activities carried out outside the national territory
 - c. Criticalities within the socio-economic system
 - ii. Informal economy
 - iii. Use of cash
- II. Effectiveness of preventive, investigative and repressive safeguards
 - a. Preventive safeguards
 - a.1 Effectiveness of AML¹⁰ regime application by obliged parties
 - a.2 Effectiveness of processes
 - i. Cross-border controls
 - a.3 Effectiveness of the analysis of suspicious transactions
 - i. Dedicated resources
 - ii. Support activities for obliged parties and feed-back
 - iii. Access to databases
 1. Access to information held by obliged parties
 2. Access to information held by other authorities
 - iv. Analysis activities
 - v. Dissemination activities
 - vi. Cooperation with other authorities
 1. National authorities
 2. European FIUs
 3. Non-European FIUs
- b. Investigative safeguards
 - b.1 Presence of vulnerabilities within in-depth analysis of STRs
 - i. Dedicated resources
 - ii. Adequacy of investigative techniques
 - iii. Access to documents and information
 1. Access to information held by obliged parties
 2. Access to information held by other authorities
 - iv. Cooperation with other authorities

¹⁰ The reference is made to the following elements: ownership and control, CDD measures, information conservation, suspicious transaction reporting (STRs), internal controls and training, supervision and sanctions.

⁹ Vulnerabilities can be assessed with respect to various aspects, such as, sectors, products, or specific business relationships, distribution channels, customers and jurisdictions.

2.3.1.1 Assessing ML inherent risk in the system
Estimated proceeds of criminal activities committed in the national territory
Analysis of predicate offences
 The starting point of the analysis is the collection of data and information, and the sharing of "cases" or typologies of criminal conducts identified by the police, the Ministry of Justice and the FIU. The reference period is the last period for which data are available with regard to the different areas of analysis to ensure homogeneity in the ratings.

Threats are identified on the basis of the ML predicate offences included among the FATF predicate offences¹ and further criminal instances identified by the Expert Group. Following the description of threats, including a quantification of the proceeds of the related criminal activities, of any economic sector in which they are invested, and an outline of the main money-laundering techniques, the output is a graduation of the threats according to the seriousness of the consequences resulting therefrom (so-called "intensity indicators"). These consequences can be estimated by parameters such as:

1. **Financial estimate** – It measures the financial importance of the threat and is therefore an indispensable reference for the assessment of the threat as a precondition of money-laundering. For determination of the financial estimate it is necessary to refer to specifically to the sources identified. Whereby the financial estimate ranges between a minimum value and a maximum value, the average between the two values will be used. In the case of multiple sources with different estimates, we adopt the average of the sources (after any possible average between the minimum and maximum values of each source);
2. **Statutory penalty** – It measures the negative social value attributed to the threat event and, consequently, the political sensitivity of the issue. In order to determine the value, reference is made to Penal Code laws or special laws of medium criminalisation. The reference value is the average of the minimum statutory penalty and the maximum penalty prescribed by law for the specific offence (e.g., corruption), or, as frequently happens, for the class of offences (e.g. tax offences);

¹ The list includes:
 conspiracy and mafia-type association;
 terrorism, including the financing of terrorism;
 trafficking in human beings and trafficking of migrants;
 sexual exploitation, including sexual exploitation of minors;
 illicit trafficking of drugs and psychotropic substances;
 illicit arms trafficking;
 illicit trafficking in stolen and other goods;
 corruption and bribery;
 fraud;
 fake money;
 counterfeiting and piracy of products;
 environmental crimes;
 murder, grievous bodily injury,
 kidnapping, illegal restraint and hostage-taking;
 robbery or theft;
 contraband (including that relating to customs, duties, excise duties and taxes);
 tax crimes (direct and indirect taxes);
 extortion;
 falsification;
 piracy;
 insider trading and market abuse.

1. National authorities
 2. European authorities
 3. Non-EU authorities
 - v. Outcomes
- b.2 Presence of vulnerabilities within ML investigative activities**
- i. Dedicated resources
 - ii. Adequacy of investigative techniques
 - iii. Access to documents and information
 1. Access to information held by obliged parties
 2. Access to information held by other authorities
 - iv. Cooperation with other authorities
 1. National authorities
 2. European authorities
 3. Non-European authorities
 - v. Outcomes

- c. Repressive activity**
- c.1 Presence of vulnerabilities in the capacity to punish perpetrators of offences**
- i. Proper identification of offences and perpetrators
 - ii. Indictments
 - iii. Convictions
 - iv. Penalties
 - v. Mutual Legal Assistance
 1. European authorities
 2. Non-European authorities

- c.2 Presence of vulnerabilities within seizure and confiscation activities**
- i. Authorities powers
 - ii. Seized assets
 - iii. Confiscated assets
 - iv. Cooperation
 1. National authorities
 2. European authorities
 3. Non-European authorities

3. Reports – It measures the concrete occurrence of the threat on the territory. The data used originate from the evidence available on the subject of reports to the particular offence or class of offences, making reference, in order of preference and subject to availability, to the national aggregate data reported by the Ministry of the Interior, the data reported by single police forces or, failing that, to works published by ISTAT.

The parameters to be used shall be the most recent among all those available.

Whereby it is not possible to estimate the intensity indicator for some threats, as the research carried out does not allow acquiring meaningful data on one or more than one of the three analytical elements taken as a reference, the risk indicator will not be determined, since a possible estimate based on partial data is to be deemed as unreliable. In such cases, as well highlighted in the analysis, the risk indicator shall be determined exclusively on the basis of expert assessments.

After acquiring analytical data on the offences or classes of offences taken into consideration, a score shall be assigned following a decreasing order depending on the relevance of the single indicator index. The three scores assigned to each offence are summed on the basis of analytical elements pertaining to it.

A proper ranking can thus be drawn, subject to validation by experts. Experts may jointly agree to modify the intensity indicator assigned to each threat and thus the ranking. Each change is justified.

In conclusion, the ranking is divided into bands according to the reported scores, so as to ensure balanced distribution. "Non-significant" does not mean "non-existing" or "irrelevant", but simply that the threat intensity is very low.

Table 1 – Internal threat relevance

Threat relevance	Intensity indicator values
Non-significant	1
Lowly significant	2
Rather significant	3
Very significant	4

Presence of proceeds of criminal activities carried outside the national territory

The starting point of the analysis is the collection of data and information, and sharing of "cases" or typologies of criminal conducts identified by Police, the Ministry of Justice and the FIU. The reference period is the last period for which data are available with regard to the different areas of analysis to ensure homogeneity in the ratings.

The experts, on the basis of the information collected, assess the threat relevance.

Table 2 – External threat relevance

Threat relevance	Intensity indicator values
Non-significant	1
Lowly significant	2
Rather significant	3
Very significant	4

Estimate of the total amount of ML in Italy and assessment of the overall threat relevance

Table 3 – Overall ML threat relevance

Threat relevance	Intensity indicator values
Non-significant	1
Lowly significant	2
Rather significant	3
Very significant	4

Analysis of critical issues relating to the socio-economic system

For the assessment of the system inherent risk, the analysis also takes into account the weaknesses in the socio-economic system, and in particular the importance of:

- Informal economy;

- Use of cash.

In the national reality, these contextual factors are considered as the most relevant in terms of ability to affect the level of Country inherent risk. Cash, in particular, is used to construct two risk indicators for the private sector and authorities.

As to corruption, while not ignoring the systemic character, the methodological choice to assess its effects in the context of threats and contextual factors was selected.

Table 4 - Intensity of vulnerabilities related to the socio-economic system

Vulnerability relevance	Intensity indicator values
Non-significant ¹²	1
Lowly significant	2
Rather significant	3
Very significant	4

¹² The "non-significant" assessment is not to be intended as "non-existing" or "irrelevant", but simply that the level of weakness is very low.

Matrix for inherent risk identification

The level of inherent risk is assessed through the combined assessment of threats and weaknesses.

Table 5 – Inherent Risk

Threat	Highly significant	Lowly significant	Medium significant
	Lowly significant	Non significant	Highly significant
System vulnerabilities	Lowly significant	Non significant	Highly significant
	Highly significant	Lowly significant	Medium significant

2.3.1.2 Effectiveness of preventive, investigative and repressive safeguards.

Vulnerability analysis

The inherent risk of money-laundering – as defined above – is mitigated by safeguards in place. In particular, the more effective safeguards in place, the lower vulnerabilities.

In order to carry out an exhaustive analysis of such safeguards, the items are broken down as follows:

- Preventive safeguards
 - o Preventive safeguards applied by obliged parties
 - Financial Intermediaries
 - Professionals
 - Non-financial operators
 - o Specific safeguards
 - Cross-border controls
 - Transparency of legal entities and trusts
 - o Analysis of suspicious transactions reports
- Investigative safeguards
 - o In-depth analysis of suspicious transaction reports
 - o Investigative activities
- Repressive safeguards
 - o Imposition of sanctions for perpetrators
 - o Seizure and confiscation of proceeds of crime

Preventive safeguards applied by obliged parties

The vulnerability analysis is performed for the areas required to implement the anti-money laundering legislation, based on their ability to fulfill the obligations provided for therein.

The analysis starts from data and information¹³. Final assessment is nevertheless left to the experts.

The risk analysis of individual categories of obliged parties is characterised by application of difficult quantitative measurement, which makes it necessary to use qualitative analysis. The assessment of anti-money laundering vulnerabilities of the system as a whole is based, according to a bottom-up approach, on the data collected and analysed by relevant supervisory authorities, the FIU and *Guardia di Finanza* within audits of individual subjects. Therefore, as qualitative analyses are carried out at micro level, qualitative criteria are to be followed in order to identify and measure vulnerabilities to the risk of the money-laundering system as a whole.

For each category of obliged parties, the so-called specific risk and effectiveness of anti-money-laundering safeguards in place are assessed.

The specific risk is an estimate of the general level of risk associated with each category of obliged parties, and depends on the related structural characteristics and the

¹³ *Information sources.* Assessments on anti-money laundering vulnerabilities of the various categories of obliged parties are therefore based primarily on an analysis of the results of inspections, which represent the most robust tool of knowledge and assessment of adequacy. The analysis, however, also takes into account the elements of information acquired by the Authority within off-site controls – whereby required – resulting, for instance, from information transmitted by other authorities, reports of irregularities made by supervisory bodies of intermediaries, reports made by the Compliance and Audit reports, meetings with obliged parties, information retrievable from the media.

activity in place. Consequently, values are to be considered as standard values. The specific risk of each operator within the analysed categories may be higher or lower depending on the activities carried out in practice. For each category, the criteria for determining the level of specific risk associated are identified.

The score scale for the specific risk is based on a range from 1 (negligible risk) to 4 (high risk). The score assigned is to be motivated.

In light of the specific risk, for each category of obliged parties the effectiveness of anti-money laundering¹⁴ safeguards in place is assessed, hence the intensity of the underlying vulnerabilities. The assessment of such vulnerabilities firstly takes into account the frequency and extent of violations of anti-money laundering provisions emerged in the inspection visits.

Among the circumstances indicating increased vulnerability to the risk of money-laundering:

- The frequency of inspections conducted annually by the competent authorities in each category of obliged parties in relation to the total number of the same (in this sense, a small number of inspections can be considered an indicator of vulnerability of the category to money-laundering risk);
- The number and typologies of anti-money laundering deficiencies found during the inspections conducted within the category of obliged persons analysed in the context of the overall supervisory activities, including off site;
- The greater or lesser frequency of application of sanctions and – whereby provided – extraordinary management procedures or compulsory liquidation or restrictive measures by the competent authorities, in relation to widespread weaknesses within the safeguards aimed at combating money-laundering;
- The greater or lesser frequency of involvement, even inadvertently, of the parties responsible in money-laundering operations that led to interventions of the Judiciary Authority.

The vulnerability assessment is broken down into a scale of 1 to 4 based on all the information available, appreciated in a comprehensive manner and in response to feedback of a discretionary nature. Considering the importance of the qualitative component, the marking is properly motivated. As follows, the related values:

Non-significant vulnerability (Value 1)
Category obliged parties, on an average, highlight a positive organisational framework.
Lowly significant vulnerability (Value 2)
Category obliged parties, on an average, highlight an organisational framework characterised by some weaknesses.
Rather significant vulnerability (Value 3)
Category obliged parties, on an average, highlight an organisational framework characterised by rather significant weaknesses.
Very significant vulnerability (Value 4)
Category obliged parties, on an average, highlight an organisational framework characterised by significant weaknesses – i.e. poor information on intermediaries is available due to lack of controls on them.

¹⁴ Anti-money laundering safeguards are divided into the following processes: ownership and control, or access to the professional category; customer due diligence; preservation and recording of information; reporting of suspicious transactions; internal controls and training; surveillance activities; sanctions.

For each category of obliged parties a synthetic indicator of relative vulnerability is therefore identified, namely estimated vulnerability compared to the level of specific risk¹⁵. This is achieved by combining the ratings of specific risk with the adequacy of the AML/CFT system.

As follows, the vulnerability indicator values:

Non-significant relative vulnerability (Value 1)
Category obliged parties, on an average, show a positive organisational framework and a negligible/average exposure to the risk of money-laundering, namely lowly significant weaknesses insignificant and negligible exposure to the risk of money-laundering.
Lowly significant relative vulnerability (Value 2)
The parties responsible for the category, on an average, show a positive organisational framework and significant exposure to the risks of money-laundering, or an organisational framework characterised by lowly significant weaknesses and average/relevant exposure to the risk of money-laundering, or an organisational framework characterised by rather significant weaknesses and average/highly exposed exposure to the risks of money-laundering or an organisational framework characterised by very significant weaknesses and negligible exposure to the risks of money-laundering.
Rather significant relative vulnerability (Value 3)
Category obliged parties show, on an average, an organisational framework characterised by positive or insignificant weaknesses and exposure to a high risk of money-laundering or an organisational framework characterised by rather significant weaknesses and a significant exposure to the risks of money-laundering or an organisational framework characterised by very significant weaknesses and average exposure to the risks of money-laundering.
Very significant relative vulnerability (Value 4)
Category obliged parties show, on an average, an organisational framework characterised by rather significant weaknesses associated with high exposure to the risk of money-laundering or an organisational framework characterised by very significant weaknesses associated with a significant or high exposure to risks of money-laundering.

The following table summarises the "grid" for assessment of vulnerability to money-laundering risks within each category of obliged parties:

¹⁵ Relative vulnerability is, in other words, the residual sectoral risk, i.e. the residual risk for each category of obliged parties, once AML/CFT safeguards have mitigated the scope.

Table 6 - Relative vulnerabilities

Specific Risk	Preventive safeguards vulnerabilities			
	1	2	3	4
4				
3				
2	Average risk	Poorly significant relative vulnerability		
1	Low risk	Non-significant relative vulnerability	Lowly significant	

Preventive safeguards applied to Financial Intermediaries (FIs)
Financial sector operators are disaggregated based on the following table.

Table 7 - Financial operators

Financial entities	Other	Italy's Legislative Decree n 231/2007
Paris and Poste Italiana SPA Financial entities (ART.107 TUB) Financial entities (ART.106 TUB) Insurance companies and institutions Electronic Money Institutions (EMIs) & Payment Institutions (SPI) - SGR - SIC IV	Large Major Medium Minor Small Insurance companies Insurance brokers Casa Doposm e Prestiti (Money changers) Companies performing tax collection services Trade as per Article 109 of Legislative Decree n 58 of 24 February 1998 ¹⁵ Trusts as per Law n. 1986 of 23 November 1939, except those under Article 199 of Legislative Decree n 58 of 24 February 1998 Subjects disciplined by Articles 111 (Microcredit) and 112 of TUB (Confiat) Money changers Financial promoters Credit intermediaries Financial agents Agents as per Article 128-quater(6) of Italy's TUB Agents as per Article 128-quinquies(7) of Italy's TUB Centralised management companies for financial institutions Management companies of financial instruments regulated markets Company management services - Settlement of transactions in financial instruments Management company of clearing and settlement of transactions in financial instruments	Art. 11 Italy's Legislative Decree n 231/2007 Art. 10(2)(a), (b), (9), (d) Italy's Legislative Decree n 231/2007

¹⁵ Individuals who do not carry out the risk analysis as a category no longer exist.
¹⁷ Individuals who do not carry out the risk analysis as a category is not operational.

The assessment of the specific risk for financial intermediaries¹⁸ is carried on the basis of the following elements (so-called **specific risk elementary factors**):

- relevance within the structure of the Italian financial system;
- nature, scale and complexity of the activity;
- profile of customers, products and activities, including the distribution chains used. In particular, some of these factors can be further detailed as follows:

- **Operational complexity**, notably significant whereby associated with large volumes and in contexts characterised by high competition and intense pressure on profit margins;
- **Increased or decreased activity** of category intermediaries in products and services that can increase the risk of money-laundering and/or terrorist financing (e.g., favoring anonymity);
- **Procedures for establishment and conduct of business relationship or transaction**; in this context, without limitation, focus is, as an increased risk perspective factor, on higher or lower use, among category intermediaries, a mode of establishment and development of the relationship that do not require the physical presence of the customer or do not allow its direct identification of the recipient. Particular attention should be paid to relationships established and managed exclusively via interposition of external collaborators;
- **The trend in terms of higher or lower use of cash** by customers of category intermediaries.

The relative vulnerability of the whole financial sector is determined as the geometric mean of the vulnerabilities of each professional category of intermediary considered individually.

¹⁸ Specific risk analysis is based on assessments of a qualitative nature, arising also from the results in the analysis of threats.

Preventive safeguards applied by Professions
Professions are disaggregated consistently with the following table:

Table 8 - Professions

Professions		Art. 12 Leg. Decree n. 231/2007
Chartered accountants and accounting experts	Labour consultants	Art. 13 Leg. Decree n. 231/2007
	Notaries	
Audit companies and accounting auditors	Lawyers	Art. 12 Leg. Decree n. 231/2007
	Other	
Professions		
Auditing of EPFs Auditing of non EPFs Any other subject that supplies services provided by surveyors, consultants and other subjects performing accounting and tax collection services at professional level Providers of services related to companies and trusts		

The specific risk for each category of professionals is determined on the basis of the following elements (so-called **specific risk elementary factors**):

- number of professional categories;
- nature of the activity and role of the professional;
- customer profile;
- value and nature of operations;
- trend in terms of higher or lower use of cash by customers of category professionals.

The relative vulnerability of the entire sector of professions is determined as the geometric mean of the vulnerabilities of each professional category considered individually.

Preventive safeguards applied to non-financial operators
Non-financial operators are broken down as follows:

Table 9 - Non-financial operators

Managers of gaming and betting activities	Casinos	Art. 14 Leg. Decree n. 231/2007
	On-line games and betting Games and gambling/betting Recovery of loans to third parties Custody and transport of cash and securities or valuables by means of special security guards Transport of cash, securities or other assets without the use of security guards Real estate brokerage agency Trade of gold for industrial purposes or investment Manufacturing, mediation and trade, including export and import of precious objects Manufacturing of valuables by handcraft businesses Dealing in antiques Operating of auction houses or art gallery Mediation/Brokerage Italian branches of persons mentioned above with their registered office in a foreign state Public Administration	
Non-financial operators	Other non-financial operators	Art. 10 Leg. Decree n. 231/2007

The specific risk of non-financial operators is determined on the basis of the following elements (so-called specific risk elementary factors):

- number of professional categories;
- nature and scale of the activity;
- customer profile;
- value of transactions;
- trend, in terms of higher or lower use of cash by customers of the category operators.

For operators as per Article 10 of Legislative Decree n. 231/2007, vulnerability assessment is carried out only with respect to the activity of reporting suspicious transactions. The analysis can however appreciate the possible effects arising from non-application of additional AML/CFT requirements.
Relative vulnerability of the entire scope of non-financial agents is determined as the geometric mean of vulnerabilities of each professional category considered individually.

Preventive safeguards – Relative analysis
Cross-border controls
Effectiveness of such safeguards is assessed on the basis of the following grid for identification and analysis of possible vulnerabilities.

Table 10 - Cross-border control effectiveness

	Effectiveness			
	Non-significant vulnerabilities	Lowly significant vulnerabilities	Rather significant vulnerabilities	Very significant vulnerabilities
Information sharing with FIU	-1-	-2-	-3-	-4-
Coordination with other AML authorities	The process does not reveal significant vulnerabilities.	The process reveals some vulnerabilities, however, not such as to compromise its effectiveness significantly	The process reveals vulnerabilities such as to compromise its effectiveness significantly	The process reveals vulnerabilities such as to compromise its effectiveness seriously
International cooperation				
Seizure/Confiscation				
Proportionate, dissuasive sanctions				

Although based on information provided, the assessment of vulnerabilities and their components is entrusted to assessment by experts.

Transparency of legal persons and trusts
Private legal persons

The analysis focuses on private legal persons and, thanks to the system of registration to which such entities are subject, enjoys a good base of information assets.

Specific risk is preliminarily assessed for legal persons. The specific risk is determined on the basis of the following elements (so-called elementary factors of specific risk):

- number of entities belonging to each category;
- decision-making system within the entity;
- typologies deduced from the analysis of treaties;
- activity nature and scale;
- spatial distribution.

Following specific risk assessment, its transparency will be assessed, or the ease with which the competent authorities have access to information on the beneficial owner, i.e. the physical/natural person(s) that ultimately own(s) or control(s) the concerned legal person. The greater transparency, the lower vulnerabilities.

As follows, the factors that affect transparency:

- presence of direct holdings of foreign legal entities;
- presence of direct holdings of trustees;
- presence of direct holdings of trusts;
- belonging to groups whose control chain includes foreign entities, trusts or trusts.

Table 11 - Private legal persons

Private legal persons	Recognised associations	
	Foundations	Listed SpA ¹⁹ Non-listed SpAs
	Società di capitale	Venture capital corporations (Società per Azioni - SpA) Limited liability companies (Società a responsabilità limitata - Srl) Company limited by shares (Società in accomandita per azioni)
	Cooperatives	

¹⁹ Subject to a specific regime on transparency

Also in the case of legal persons, the analysis allows assessment of vulnerabilities, according to the table below.

Table 12 - Relative vulnerabilities - Private legal persons transparency

Specific risk	4				
	3				
	2	Average risk	Lowly significant relative vulnerability		
	1	Negligible risk	Non-significant relative vulnerability	1	2
				3	4
Transparency vulnerabilities					

Transparency vulnerabilities

This basic analysis can be enriched by insights that take into account the related activity sector, geographical area and economic performance of the company.

Trusts

Trusts are not provided for and governed by the Italian law. However, through the ratification of the Hague Convention of 1 July 1985, effectiveness of foreign trusts is recognised as well as the possibility to establish in Italy a trust governed by the provisions of a foreign State.

Unfortunately, at present it is not easy to estimate the number of trusts established or operating in Italy. Risk assessment is mainly based on specific typologies deduced from the analysis of threats, the analysis of suspicious transactions, and investigation activities.

As for the analysis of vulnerabilities in relation to transparency, FATF Recommendation 25 requires that the competent authorities have access to information relating to the trust(s) by making reference to Customer Due Diligence (CDD) implemented by intermediaries and professionals with which/whom the trustee comes into contact. CDD adequacy should be strengthened by the provision of a general nature which requires termination of the business relationship if the beneficial owner is not identified.

Assessment of relative vulnerabilities is notably appreciated by experts' assessment as to the capacity of competent authorities to have access to information on the subject.

Assessment of the specific risk is essentially based on typologies deduced from the analysis of threats, analysis of suspicious transactions and investigative activities.

Table 13 - Relative vulnerability - Trust transparency

4	Highly significant relative vulnerability	Highly significant	4
3	Significant relative vulnerability	Significant	3
2	Average risk	Lowly significant relative vulnerability	2
1	Negligible risk	Non-significant relative vulnerability	1
		Non-significant	
Vulnerabilities relative to trusts transparency			

Processes: Vulnerability assessment

Analysis relative to Suspicious Transaction Reports

Effectiveness of activities related to reporting of suspicious transactions is assessed based on the following criteria for identification and analysis of possible vulnerabilities.

- ✓ Dedicated resources
- ✓ Support to obliged parties, including feedback to STRs
- ✓ Access to documents and information
 - Access to information held by obliged parties
 - Access to information held by other authorities
- ✓ Analysis activity
- ✓ Dissemination activity
- ✓ Cooperation with other authorities
 - National authorities
 - European FIUs
 - Non-European FIUs

The following scale of vulnerability values is replicated on all the analyses described as follows.

Table 14

Non-significant vulnerabilities	-1-	Lowly significant vulnerabilities	-2-	Rather significant vulnerabilities	-3-	Non-significant vulnerabilities	-4-
The process does not reveal significant vulnerabilities		The process reveals some vulnerabilities, however, not such as to compromise its effectiveness significantly		The process reveals vulnerabilities such as to compromise its effectiveness significantly		The process reveals vulnerabilities such as to compromise its effectiveness	

Based on information provided, the assessment of relative vulnerabilities and their components is entrusted to experts.

Investigative activity analysis

Analysis related to in-depth examination of STRs

Effectiveness of in-depth analysis of STRs is assessed on the basis of the following criteria for identification and analysis of possible vulnerabilities.

- ✓ Dedicated resources
- ✓ Investigative techniques adequacy
- ✓ Access to documents and information
 - Access to information held by obliged parties
 - Access to information held by other authorities
- ✓ Cooperation with other authorities
 - National authorities
 - European FIUs
 - Non-European FIUs
- ✓ Outcomes

Analysis of ML investigative activities

The analysis of anti-money laundering investigative activities is assessed on the basis of the following criteria for identification and analysis of possible vulnerabilities.

- ✓ Dedicated resources
- ✓ Investigative techniques adequacy
- ✓ Access to documents and information
 - Access to information held by obliged parties
 - Access to information held by other authorities
- ✓ Cooperation with other authorities
 - National authorities
 - European FIUs
 - Non-European FIUs
- ✓ Outcomes

Analysis of repressive activities

Analysis related to capacity to sanction perpetrators of offences

The effectiveness analysis relative to the capacity to sanction perpetrators of offences is assessed on the basis of the following criteria for identification and analysis of possible vulnerabilities.

- ✓ Adequate identification of offences and related perpetrators
- ✓ Indictments
- ✓ Sentences
- ✓ Penalties
- ✓ Judicial assistance
 - European counterparts
 - Non-European counterparts

Analysis related to seizure and confiscation capacity

Effectiveness of analysis related to the capacity to seize and confiscate the proceeds from offences is assessed on the basis of the following criteria for identification and analysis of possible vulnerabilities.

- ✓ Authorities powers
- ✓ Seized assets
- ✓ Confiscated assets
- ✓ Cooperation
 - National counterparts
 - European counterparts
 - Non-European counterparts

Aggregation of vulnerabilities of processes and additional aggregations

Vulnerability of processes is determined as the geometric mean of the vulnerabilities of each process individually considered.

It is also possible to carry out additional aggregations, by calculating average vulnerability for all the various levels of AML/CFT. A reference value is thus obtained, which provides synthesis information of the overall vulnerability of the system.

It is however advisable to point out that the real added value of the model is represented by the analysis and assessment contribution provided by individual components related to threats and vulnerabilities.

2.3.2 Terrorist Financing (TF) risk – Analysis model

The Methodology described to assess the risk of money-laundering is used and adapted so as to assess the risk of terrorist financing. Consequently, whereby common AML/CFT criticalities and safeguards are to be assessed, the analysis results are the same both for money-laundering and terrorist financing.

Within the assessment of threats, the Methodology considers the financing of terrorism as a process developing in three distinct phases: collection, transfer and use of funds and economic resources. In analysing safeguards' effectiveness, the Methodology also relies on assessment of specific measures to combat terrorist financing (in particular freezing measures).

TF analysis model is broken down as follows.

I. Identification of FT inherent risk within the system

- a. Context analysis
 - i. Evolution of terrorist and terrorist financing threat
 - ii. Socio-economic system vulnerabilities
 - 1. Informal economy
 - 2. Use of cash
- b. Funds origin
 - i. Proceeds of illegal activities
 - ii. Proceeds of crimes committed on national territory
- b. Funds transfer
 - i. Funds collected on national territory:
 - 1. Stay on national territory
 - 2. Transferred abroad
 - ii. Funds collected abroad and transferred domestically
- c. Funds use
 - i. For terrorist acts by:
 - 1. Individual terrorists
 - 2. Terrorist organisations.
 - ii. For support to individual terrorists as well as terrorist groups/organisations

II. Identification of FT residual risk within the system, as to

- a. *Preventive measures*
 - a.1 Effectiveness of application of specific FT measures
 - i. Procedures for listing proposals
 - ii. Application of freezing measures
 - 1. Timeliness
 - 2. Exhaustiveness
 - 3. Notification/Reporting obligations
 - iii. Opposability to third parties
 - iv. Management of frozen funds and economic resources
 - 1. Exceptions
 - 2. Management/Administration
 - v. Procedures for de-listing proposals
 - vi. Non-profit sector structure
 - a.2 Effectiveness of AML/CFT regime by obliged parties
 - a.3 Effectiveness of processes
 - i. Cross-border controls
 - ii. Transparency of legal persons and trusts
 - iii. Non-profit sector structure and characteristics
 - a.4 Effectiveness of the analysis of STRs
 - i. Dedicated resources
 - ii. Support to obliged parties
 - iii. Access to databases
 - 1. Access to information held by obliged parties
 - 2. Access to information held by other authorities
 - iv. Analysis activities
 - v. Dissemination activities
 - vi. Cooperation with other authorities
 - 1. National authorities
 - 2. European FIUs
 - 3. Non-European FIUs
- b. *Investigative activities*
 - b.1 Presence of vulnerabilities within in-depth analysis of STRs
 - i. Dedicated resources
 - ii. Investigative resources
 - iii. Access to documents and information
 - 1. Access to information held by obliged parties
 - 2. Access to information held by other authorities
 - 1. Cooperation with other authorities
 - 1. National authorities
 - 2. European authorities
 - 3. Non-European authorities
 - 2. Outcomes

- 3. Glossary**
- AML – Anti-Money Laundering
 - BCC – *Banche di Credito Cooperativo* (credit unions)
 - CDD – Customer Due Diligence
 - CFT – Countering the Financing of Terrorism
 - CSF – *Comitato di Sicurezza Finanziaria* (Italy's Financial Security Committee)
 - Leg. Decree – Legislative Decree
 - FT – Financing of Terrorism
 - GAFI-FAFT – Financial Action Task Force
 - ISTAT – *Istituto Nazionale di Statistica* (Italy's National Institute of Statistics)
 - ML – Money-Laundering
 - SGR – *Società di Gestione del Risparmio* (asset management companies)
 - SICAV – *Società di Investimento a Capitale Variabile* (investment companies with variable capital)
 - SIM – *Società di Intermediazione Mobiliare* (real estate brokerage companies)
 - STR – Suspicious Transaction Report
 - TUB – *Testo Unico Bancario* (Italy's Consolidated Law on Banking)
 - EU – European Union
 - UIF – *Unità di Informazione Finanziaria* FIU – Financial Intelligence Unit

b.2 Presence of vulnerabilities within investigative activities

- i. Dedicated resources
- ii. Investigative activities
- iii. Access to documents and information
 - 1. Access to information held by obliged parties
 - 2. Access to information held by other authorities
- iv. Cooperation with other authorities
 - 1. National authorities
 - 2. European authorities
 - 3. Non-European authorities
- v. Outcomes

c. Repressive activities

c.1 Presence of vulnerabilities in the capacity to sanction perpetrators of crimes

- i. Adequate identification of crimes and perpetrators
- ii. Indictments
- iii. Sentences
- iv. Penalties
- v. Judicial assistance
 - 1. European authorities
 - 2. Non-European authorities

c.2 Presence of vulnerabilities in seizure and confiscation activities

- i. Authorities' powers
- ii. Seized assets
- iii. Confiscated assets
- iv. Cooperation
 - 1. National authorities
 - 2. European authorities
 - 3. Non-European authorities