

Financial Security Committee

**ITALY'S NATIONAL ASSESSMENT OF
MONEY-LAUNDERING
AND TERRORIST FINANCING RISKS**

2014

Synthesis

LIST OF CONTENTS

GLOSSARY	1
INTRODUCTION	2
1. ANALYSIS MODEL – DESCRIPTION	3
1.1 Money laundering: analysis of threats	4
1.2 Analysis of vulnerabilities within Italy’s socio-economic system	5
1.3 Inherent risk assessment – Matrix	6
2. SYNTHESIS OF ITALY’S NATIONAL ASSESSMENT OF MONEY-LAUNDERING AND TERRORIST FINANCING RISKS – MAIN OUTCOMES	7
2.1 Threats and weaknesses within Italy’s socio-economic system	7
2.1.1 Weaknesses within Italy’s socio-economic system	7
2.1.2 Intensive use of cash – Risk indicators	8
2.2 Money laundering: Criminal activities carried out within the national territory	10
2.2.1 Analysis of conducts that generate proceeds to be laundered	11
2.2.2 Conclusions: synthesis assessment of Italy’s system inherent risk of money laundering	13
2.3 Terrorist Financing	14
2.3.1 Context analysis: terrorist financing threat evolution	15
2.3.2 Origin, transfer and use of funds	17
2.3.3 Conclusion: synthesis assessment of Italy’s system inherent risk of terrorist financing	19
3. ANALYSES OF VULNERABILITIES	21
3.1 Preventive safeguards	21
3.1.1 Safeguards implemented by obliged entities	21
3.1.2 Legal persons and trusts’ transparency	26
3.1.3 Cross-border controls	27
3.1.4 Analysis of Suspicious Transaction Reports (STRs)	27
3.2 Investigative safeguards	28
3.3 Repressive safeguards	28
3.4 <i>Ad-hoc</i> CFT safeguards	29
4. CONCLUSIONS AND ACTION LINES	31
4.1 Preventive safeguards	31
4.2 Investigative safeguards	35
4.3 Repressive safeguards	35
4.4 <i>Ad-hoc</i> CFT measures in place	36

GLOSSARY

<i>ABI</i>	<i>Associazione Bancaria Italiana</i> (Italian Banking Association)
<i>AML</i>	Anti-Money Laundering
<i>AQAP</i>	Al-Qaida in the Arabian Peninsula
<i>AQI</i>	Al-Qaida in Iraq
<i>AQIM</i>	Al-Qaida in Islamic Maghreb
<i>AUI</i>	<i>Archivio Unico Informatico</i> (Unified Computerised System)
<i>CDD</i>	Customer Due Diligence
<i>CDDPP</i>	<i>Cassa Depositi e Prestiti</i>
<i>CSF</i>	<i>Comitato di Sicurezza Finanziaria</i> (Italy's Financial Security Committee)
<i>DIA</i>	<i>Direzione Investigativa Antimafia</i> (Anti-Mafia Investigation Directorate)
<i>DNFBPs</i>	Designated Non-Financial Businesses and Professions
<i>EC</i>	European Commission
<i>EMIs</i>	Electronic Money Institutions
<i>ETA</i>	<i>Basque Euskadi ta Askatasuna</i>
<i>EU</i>	European Union
<i>ISIL</i>	Islamic State of Iraq and the Levant
<i>IVTS</i>	Informal Value Transfer Systems
<i>FAI</i>	<i>Federazione Anarchica Informale</i> (Informal Anarchist Federation)
<i>FATF-GAFI</i>	Financial Action Task Force – <i>Groupe d'Action Financière</i>
<i>JITs</i>	Joint Investigation Teams
<i>LTTE</i>	Sri Lankan Liberation Tigers of Tamil Eelam
<i>ML</i>	Money Laundering
<i>NRA</i>	National Risk Assessment
<i>PIs</i>	Payment Institutions
<i>PIEs</i>	Public Interest Entities
<i>PKK/KCK</i>	Kurdish Partiya Karkerên Kurdistan
<i>RBA</i>	Risk-Based Approach
<i>SICAV</i>	<i>Società d'Investimento a Capitale Variabile</i> (Investment company with variable capital)
<i>SIM</i>	<i>Società di Intermediazione Mobiliare</i> (Real estate brokerage company)
<i>SGR</i>	<i>Società di Gestione del Risparmio</i> (Asset management company)
<i>SMEs</i>	Small and Medium Enterprises
<i>STRs</i>	Suspicious Transaction Reports
<i>TUB</i>	<i>Testo Unico Bancario</i> (Italy's Consolidated Banking Law)
<i>TF</i>	Terrorist Financing
<i>UIF</i>	<i>Unità Informazione Finanziaria</i> (Italy's Financial Intelligence Unit – FIU)
<i>UN</i>	United Nations
<i>VLTs</i>	Video Lottery Terminals

INTRODUCTION

Within the powers established by Article 5 of Legislative Decree N. 231/2007, Italy's Financial Security Committee (*Comitato di Sicurezza Finanziaria – CSF*) performed an analysis of money-laundering and terrorist financing risks identified at national level. Such analysis – i.e. the *National Risk Assessment* – was accomplished, for the first time in a systematic way, in application of new¹ FATF Recommendation 1, with the objective to identify, analyse and assess money-laundering and terrorist financing threats, and thus detect major pressures and the methods of conducting such criminal activities, as well as the vulnerabilities of the national system of prevention, investigation and prosecution of such phenomena, hence the sectors most exposed to such risks. The exercise is aimed at defining action lines for mitigating the risks identified, consistently with an AML/CFT risk-based approach that requires that implementation of AML/CFT measures should be commensurate to the risks countered².

Developed on the basis of a specific methodology, the National Risk Assessment was conducted by an *ad-hoc* working group composed of the representatives from the authorities participating in the *CSF* (i.e. ministries, supervisors, Financial Intelligence Unit, law enforcement entities), as well as from other relevant administrations and Italy's Presidency of the Council of Ministers. Significant contributions resulted from the meetings with scholars and representatives from academia and private sector, which stimulated comparative analysis opportunities that enriched the study with valuable evidence and/or integrations. Several sector associations and private institutions shared their direct experiences and assessments on specific issues identified over the meetings jointly attended.

The conclusions drawn reflect a shared assessment of the phenomena – both as to threats and vulnerabilities – based upon information, data and evaluations retrieved from heterogeneous sources, and provide the grounds for strategic coordination of competent authorities' policies.

¹ The new FATF Standards were approved, under the Italian Presidency, in February 2012.

² FATF Recommendation 1.

1. ANALYSIS MODEL – DESCRIPTION

The first assessment is of an experimental nature and will be updated in three years' time, in order to take account of forthcoming developments within EU and national legal frameworks, and suggestions arising from the activities performed by supervisory authorities, police investigations and FIU analyses. Subsequently, the national analysis will be updated on a five-year basis, and could also be carried out in case of emerging threats or notably remarkable vulnerabilities.

The assessment exercise was conducted upon clear distinction between money-laundering risks and terrorist financing risks, although the methodology applied for the latter is derived from the one applied to money-laundering risks, amended, whereby necessary, so as to take account of sectoral regulations and relevant processes. In both cases, the exercise was developed at the national level.

The methodology applied requires identification, analysis and assessment of main domestic risks (through examination of the related causes or threats) and underlying vulnerabilities and resulting consequences.

Starting from such grounds, the analysis is broken down into the following phases:

- Assessing the ML/TF inherent risk(s) within the system;
- Assessing the effectiveness of preventive, investigative and repressive safeguards.

The inherent risk of Italy's socio-economic system is assessed based upon identified threats and challenges related to the informal economy and use of cash. The analysis of money laundering identifies threats associated to money-laundering predicate offences; conversely, the analysis of terrorist financing unveils a complex process including collection, transfer and use of funds and economic resources.

As far as money-laundering analysis is concerned, the aim is to identify the main threats – wherever possible also through quantification of criminal activities proceeds – and identification of major laundering methods and possible economic sectors in which the proceeds of crimes committed both in Italy and/or abroad are invested.

The subsequent stage lies in the effectiveness analysis of preventive, investigative and repressive safeguards in place in Italy in order to counter money-laundering crimes. This Section assesses the main vulnerabilities identified within Italy's preventive and repressive systems, which enable existing threats to result in money laundering and terrorist financing phenomena.

The effectiveness of preventive safeguards is analysed in reference to elements such as: safeguards put in place by obliged entities; adequacy of measures provided for cross-border

controls; transparency of legal entities and trusts; and adequacy of activities related to suspicious transactions analysis. In particular, obliged entities are broken down into macro-categories (i.e. financial intermediaries, non-financial professionals, and operators). Their ability to meet own obligations is assessed with respect to the anti-money laundering *specific* risk level, namely the level of risk associated to each category, depending on its structural characteristics and activities.

The effectiveness of the investigative phase is assessed by differentiating between in-depth analysis of STRs and independent investigative activities, taking account, in both cases, of factors such as: adequacy of resources; investigative techniques; access to information; international cooperation; and the results attained by means of the activities performed.

Effectiveness of the repressive activities implemented is assessed based upon the adequacy of the disciplinary system as to correct identification of offences and possible perpetrators – also in terms of legal assistance provided by national authorities to foreign authorities – and upon the capacity to seize and confiscate the assets involved in such criminal phenomena.

Furthermore, the analysis is also aimed at assessing the specific measures implemented to counter the financing of terrorism. In synthesis, the effectiveness analysis on preventive, investigative and repressive safeguards aims at identifying up to what extent they can actually mitigate the inherent risk of money laundering and/or terrorist financing.

In particular, in light of the inherent risk identified, the lower vulnerabilities detected within the preventive, investigative and repressive actions undertaken, the more safeguards in place effectively mitigate the related inherent risk(s).

1.1 Money Laundering: analysis of threats

Threats are identified on the basis of money-laundering predicate offences as per the related FATF–GAFI classification³ and further criminal cases identified by relevant authorities.

At this stage, threats are ranked according to the seriousness of the resulting consequences (so-called *relevance indicator*). Consequences are estimated according to the following parameters:

³ The list includes: organised crime and mafia-type criminal organisations; terrorism and terrorist financing; trafficking in human beings and migrants; sexual exploitation (also of children); drug trafficking; illicit arms trafficking; receiving and smuggling of stolen goods and other assets; corruption and bribery; fraud; forgery of means of payment; counterfeiting and smuggling of products; environmental crimes; murder and bodily injury; kidnapping; robbery or theft; smuggling (also related to customs duties, excises and taxes); tax offences (direct and indirect taxes); extortion; counterfeiting; piracy; insider trading and market manipulation.

- Financial estimate – Measuring the financial relevance of threats and as such providing an essential reference for money-laundering threat assessment;
- Penalty prescribed by law – Measuring the negative social value attributed to the threat-event and, consequently, assessing political sensitivity to the issue. The value is assessed based upon relevant provisions within Italy’s Criminal Code or *ad-hoc* legislation;
- Reports – Measuring the actual threat incidence on the territory.

Whereby no significant data are acquired on one or more of the three above analytical elements taken as a reference, the risk indicator cannot be determined. Under such assumptions, the risk indicator is determined exclusively on the basis of assessments made by competent authorities. The classification is broken down into ranks according to the scores attained. The "**non-significant**" judgment **does not mean the risk is non-existent or insignificant**; rather, it indicates the threat relevance is **very low**.

Table 1 – Domestic threat relevance

Threat relevance	Relevance indicator – Values
Non Significant/very low	1
Lowly Significant	2
Rather Significant	3
Highly Significant	4

1.2 Analysis of vulnerabilities within Italy’s socio-economic system

For the purposes of assessing the system’s inherent risk, the analysis also takes account of Italy’s socio-economic system vulnerabilities – i.e. the informal economy and use of cash. Within the national context, such contextual factors are considered as most significant in terms of ability to influence the Country’s inherent risk level. Cash use, in particular, is utilised to shape two provincial risk indicators both for the private sector and public authorities.

Table 2 – Vulnerabilities within Italy’s socio-economic system: Relevance

Vulnerability relevance	Intensity indicator – Values
Non Significant/very low	1
Lowly Significant	2
Rather Significant	3
Highly Significant	4

1.3 Inherent risk assessment – Matrix

The inherent risk level is estimated based upon a combination of threats and challenges within the system.

Table 3 – Inherent risk

Threat	Highly Significant				Highly Significant
	Rather Significant			Rather Significant	
	Lowly Significant		Lowly Significant		
	Non-Significant	Non-Significant			
		Non-Significant	Lowly Significant	Rather Significant	Highly Significant
	System vulnerabilities				

2. SYNTHESIS OF ITALY'S NATIONAL ASSESSMENT OF MONEY-LAUNDERING AND TERRORIST FINANCING RISKS – MAIN OUTCOMES

The national evaluation of money-laundering and terrorist financing risks based upon the methodological lines briefly described led to the findings set out below.

2.1 Analysis of threats and weaknesses within Italy's socio-economic system

2.1.1 Vulnerabilities within Italy's socio-economic system

The features of socio-economic systems can either amplify or help curb the risk that the proceeds of illegal activities could be reintegrated into the formal economy. Two elements are taken into account within the analysis – namely: *i*) use of cash; and *ii*) the shadow economy. Both factors are critical elements with **very significant influence** on the Country's level of risk⁴. Cash is considered the privileged means of payment for transactions linked to the shadow (illegal) economy, as it ensures non-traceable and anonymous exchange⁵. Comparative analysis with other advanced economies reveals the use of cash is particularly strong in Italy: based upon a study carried out by the European Central Bank (ECB) in 2012, 85% of the total volume of transactions settled in Italy was performed in cash, against the EU 60% average⁶. Besides being affected by diverse development levels within the financial system, and spreading of alternative means of payment throughout the Country (notably electronic ones), the finding may reflect heterogeneous sizes of the shadow economy across European Union Countries. Italy's shadow economy is estimated⁷ to have reached a market share equal to 22% of GDP in 2012, versus the EU 19% average. The shadow economy constitutes a fertile ground for criminal activities⁸; over recent years, the use of cash has constantly decreased, due both to

⁴ The “shadow economy” is to be intended as the production of assets and services that, lawful in nature, escape direct observation, as they are often the object of tax/contribution evasions. Properly criminal activities are therefore not directly included (as production/sale is not carried out in violation of criminal rules – e.g. drug trafficking), likewise *per se* lawful activities that are illegal whereby exercised without adequate authorisation or competence (e.g. smuggling; arms trafficking, etc.).

⁵ See, for instance: Ardizzi, Petraglia, Piacenza & Turati, *Measuring the underground economy with the currency demand approach*, *Temi di discussione* n. 864, Banca d'Italia (April 2012).

⁶ See: European Central Bank, *The Social and Private Costs of Retail Payment Instruments. A European Perspective*, *Occasional Paper Series* n. 137 (September 2012).

⁷ *The Shadow Economy in Europe* (Visa, 2013) – *Using electronic payment systems to combat the shadow economy*. Different estimates are available with regard to the shadow economy. Istat (2010) – *La misura dell'economia sommersa*, for instance, estimated that in 2008 the added value produced within the shadow economy was equal to EUR 255-275 billion, namely 16.3% and 17.5% of GDP, respectively.

⁸ Schneider and F. Enste, D. H. (2000), ‘Shadow Economies: Size, Causes, and Consequences’, *Journal of Economic Literature*, Vol. XXXVIII, March.

increasing use of alternative instruments and restrictive policies impact on cash circulation. This finding, nevertheless, does not mitigate the assessment. The effects on the relationship between the informal illegal economy and the proxy represented by cash do appear potentially ambiguous: on the one hand, the increased use of payment instruments other than cash may also have involved the criminal economy; on the other hand, high traceability of new payment instruments and the constraints set on cash use – which mainly discourage “lawful” uses – suggest the overall scope of cash as a proxy of the shadow economy has been increased.

2.1.2 Intensive use of cash – Risk indicator

Cash use is uneven across Italy. Based on the assumption that *cash* is an indicator – at least partially – of money-laundering risks, a risk indicator developed at provincial level is hereby presented. *As follows some preliminary results of an ad-hoc study still ongoing*⁹.

This indicator is based on the incidence of “anomalous” volumes of money transfers, which indirectly indicate operations in cash recorded in a given province are likely to be linked to criminal activities. The “excessive” use of cash is estimated at municipal level based upon a statistical model that takes into account the “physiological” (socio-economic and financial) determinants of cash use.

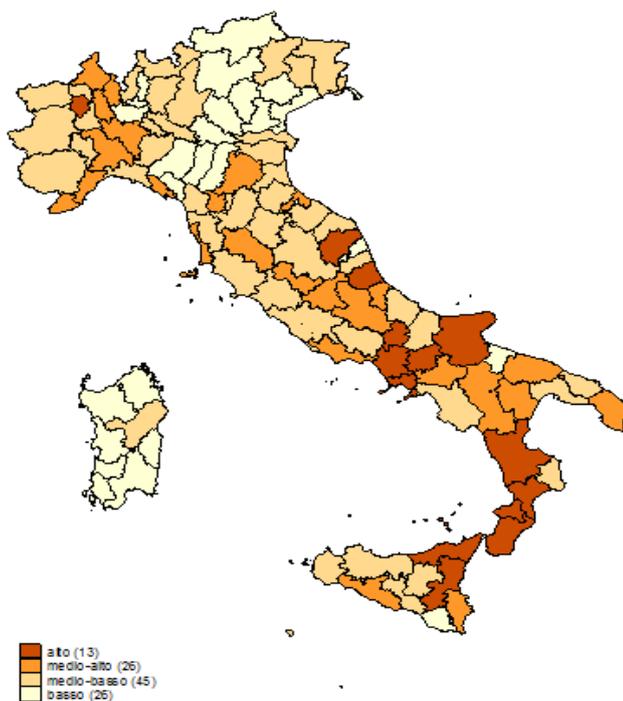
The indicator is constructed according to the provincial average of excessive use of cash at municipal level. The provincial mapping of such risk measure is displayed in Figure 1, which itemises four levels of risk – i.e. *i*) high; *ii*) medium-high; *iii*) medium; and *iv*) low. The complete lists of relevant provinces are itemised within Table 1. From a methodological point of view, it is worth underlining the broke-down of provinces in four ranks – likewise the high number of each rank – is not based upon thresholds, rather it is determined “endogenously” by standard stratification algorithms that gather findings into as-homogeneous-as-possible groups as per indicator values.

The provinces marked by higher risk level (“high”) are concentrated, with some exceptions, in southern Regions strongly affected by criminal infiltration. The subsequent risk class (“medium-high”) includes southern provinces and notably central and north-western areas. The findings are still preliminary, and the indicator is being fine-tuned. Developments include the

⁹ Indicators are devised by Italy’s Financial Intelligence Office (*Ufficio Informazione Finanziaria – UIF*) and adopted by the Financial Security Committee.

elaboration of specific risk measures for different categories of crimes, and comparative analysis of several methods of aggregation of findings at province level¹⁰.

Figure 1 – Geographical distribution of risk – Intensive use of cash



Source: UIF (preliminary findings)

¹⁰ The study is being carried out by Italy's Financial Intelligence Unit (*Unità di Informazione Finanziaria – UIF*), within its strategic analysis activity.

Table 1 – Provinces’ classes of risk. Intensive use of cash

Risk class	Provinces
High	<i>Benevento, Biella, Caserta, Catania, Catanzaro, Cosenza, Foggia, Isernia, Macerata, Messina, Napoli, Reggio Calabria, Vibo Valentia.</i>
Medium-High	<i>Agrigento, Alessandria, Avellino, Bari, Bologna, Imperia, La Spezia, L'Aquila, Latina, Lecce, Livorno, Matera, Novara, Pavia, Pescara, Pistoia, Potenza, Rieti, Rimini, Savona, Siena, Siracusa, Teramo, Terni, Varese, Verbano-Cusio-Ossola.</i>
Medium	<i>Ancona, Aosta, Arezzo, Ascoli Piceno, Asti, Belluno, Bergamo, Brescia, Brindisi, Caltanissetta, Campobasso, Chieti, Como, Cremona, Crotone, Cuneo, Enna, Ferrara, Firenze, Forli-Cesena, Frosinone, Genova, Gorizia, Grosseto, Lodi, Lucca, Nuoro, Palermo, Perugia, Pesaro e Urbino, Piacenza, Pisa, Pordenone, Prato, Ravenna, Roma, Rovigo, Salerno, Sondrio, Taranto, Torino, Trapani, Udine, Vercelli, Viterbo.</i>
Low	<i>Barletta-Andria-Trani, Bolzano, Cagliari, Carbonia-Iglesias, Fermo, Lecco, Mantova, Massa-Carrara, Medio Campidano, Milano, Modena, Monza e della Brianza, Ogliastro, Olbia-Tempio, Oristano, Padova, Parma, Ragusa, Reggio Emilia, Sassari, Trento, Treviso, Trieste, Venezia, Verona, Vicenza.</i>

Source: UIF (preliminary findings)

2.2 Money laundering: Criminal activities carried out within the national territory

The impact of illegal economic activities on the Country is undoubtedly remarkable. Although there is no single official estimate of the economic value of criminal activities, the assessments (ranging between 1.7 and 12% of GDP, depending on the underlying definition and methods)¹¹

¹¹ The shadow economy can be estimated based upon both direct and indirect methods. The former are based on household surveys and indicators related to crimes and criminality, while the latter deduct the extent of the phenomenon by comparing macroeconomic indicators. The first group includes estimates by *SOS Impresa*, according to which Mafia turnover is equal to EUR 138 billion, namely 8.7% of GDP (XIII Report 2012, referring to 2010 sales). Based upon the same method, within the “*Sicurezza 2007-2013*” National Operational Programme, *Transcrime* provides very different findings: the turnover of illegal activities reportedly amounted to average 1.7% of GDP in 2010, equal to EUR 17.7-33.7 billion turnover. A study conducted by Bank of Italy in collaboration with researchers from several universities (Ardizzi and others) applies a variant of the currency demand approach in order to separately estimate the component of the underground economy linked to activities classified as legal but actually exercised unlawfully (e.g. for evading taxes and contributions) and the illegal component in a strict sense (excluding violent crimes, theft, extortion, robbery, usury, and, as such, notably prostitution and illicit drug trafficking). Over 2005-2008 the shadow economy is estimated to amount to 16.5 percent of GDP and the inherently illegal economy to 10.9 percent of GDP, respectively. A further academic study (Argentiero and others, 2008) proposed a macroeconomic estimate of money laundering in Italy for the 1981-2001 period. The model adopted suggests that, over that period, money laundering accounted for approximately 12 percent of GDP. The study also shows that money laundering has natural anti-cyclical increases during crisis periods (See: Signorini address, Bank of Italy 2012). Istat has recently published new GDP estimates for 2011-2013, which, consistently with EU guidelines, introduced the production value related to three illegal activities (i.e. drug trafficking; prostitution; smuggling). The estimate published is consistent with the values used within the definition of this ratio and is equal to approximately 0.9% of the new GDP level.

utilised) concur to supporting an extremely significant opinion as to the threat that illicit proceeds are produced in the Country and then reintroduced into Italian and foreign economic and financial channels.

If the analysis of consequences is extended to the economic cost of criminality – i.e. the compression of the total income resulting from criminal activities, specifically if organised, because of costs imposed inefficiently allocated resources, discouraged investments or however hindered activities – the result is even more severe¹². Such opinion, expressed by the academic world, is shared both by the government authorities involved in combating these phenomena and by the private sector.

The current economic crisis has offered further opportunities for criminality to penetrate the economic fabric. For instance, financial difficulties (specifically in terms of liquidity) may induce usury increase, making companies and individuals more vulnerable to criminals' attempts to extend their control over the legal and formal economy.

The current threat that money-laundering phenomena may affect our economy is thus deemed as **very significant**.

2.2.1 Analysis of conducts that generate proceeds to launder

Starting from the analysis of predicate offences based upon relevant indicators – i.e. proxies of economic impacts, territorial dissemination and negative social value attributed – the relevance of threats posed by different criminal behaviours was then assessed. This estimate reflects the perception of the phenomenon's magnitude based both upon operational experience of authorities aimed at preventing and countering money laundering, and the private sector.

Corruption is a major criminal phenomenon, although the EUR 50-60 billion financial / year estimate reported by more institutional sources is deemed as not fully reliable. The perception of the phenomenon is still very strong, confirmed by the significant number of people reported to law enforcement authorities for corruption in Italy, while taking into account that such criminal offence is definitely under-reported. As revealed by a recent survey carried out by the

¹² A recent econometric analysis conducted by Bank of Italy (Pinotti, 2012) proposes an overall estimate of losses in terms of GDP which can be attributed to organised crime in Italy's Mezzogiorno Area. The work compares the economic development of two Regions (Apulia and Basilicata) more recently experiencing criminal infiltration, over the decades before and after Mafia's spreading, which took place in the late 1970s, with that of a group of Italy's central and northern Regions that previously experienced similar socio-economic conditions. If assumptions are valid, as a result of Mafia's spreading, the two Regions suffered a cut in GDP per capita growth of approx. 20 percentage points over thirty years. The main direct cause is lower private investment.

World Bank¹³, in terms of costs, each point of decrease within Transparency International corruption perception index results in a 16% decrease in foreign investments.

A recent study by Unimpresa¹⁴ indicates corruption in Italy does increase the overall cost of procurement contracts by 20%. Between 2001 and 2011, corruption *consumed* EUR 10 billion per year in terms of Gross Domestic Product (GDP) – i.e. EUR 100 billion over ten years. Businesses operating in a corrupt environment grow on an average by 25% less than competitors operating in a lawful environment. In particular, SME sale growth rate is over 40% lower than for large ones. Furthermore, social control systems prove to be ineffective.

The current economic crisis has also increased criminal phenomena such as **bankruptcy and corporate crimes, and usury**. Usury linked to loans granted by unauthorised persons is submerged (disclosure only results from reporting made by usury victims) and is strongly place-based. The phenomenon is mostly prevalent in southern and central Europe, although difficult to be circumscribed. As a result of the economic recession,¹⁵ the *usurer* has now turned into a "white collar" or professional figure (sometimes even organised) – which can result in criminal forms of unauthorised credit activity. Eventually, bankruptcy and corporate crimes result in conducts that are instrumental to the perpetration of other crimes including, of course, money laundering.

Tax evasion and tax related crimes are assessed as very significant, also in light of the close connection between tax evasion and money laundering within the operating methods used to conceal, transfer or re-utilise illicit assets within the legal economy¹⁶.

Italian and foreign **organised crime** operating on the national territory remains the prevailing and most worrying form of criminal behaviour. With the exception of tax evasion, almost all criminal behaviours are largely, and in some cases exclusively, ascribable to organised crime (e.g. drug trafficking, extortion, gambling, illegal traffic of waste, smuggling and counterfeiting). Also with regard to corruption, criminal infiltration within politics plays a key role (i.e. 110 municipal councils subject to dissolution over 2001-2009¹⁷ as they were infiltrated

¹³ See: Garofoli 2013.

¹⁴ See: UNIMPRESA, “Expo. Unimpresa, con corruzione in 10 anni - 100 miliardi di PIL in Italia”, 12 May 2014, <http://www.unimpresa.it/expo-unimpresa-con-corruzione-in-10-anni-100-miliardi-di-pil-in-italia/9241>.

¹⁵ In 2013, the reports related to usury (over 2,000) nearly doubled compared to 2012, mainly connected to the severe economic and financial crisis of recent years, which made the social fabric more permeable by criminal activities.

¹⁶ Identified ML-related crimes are mostly related to: false invoicing; use of shell companies; interposition of nominees or corporate schemes; transfer of assets abroad; bank or triangular trade; real estate investments; use of cash; use of banking channels.

¹⁷ See: Italy's Ministry of the Interior “Elaborazione statistica sui Consigli degli Enti locali sciolti in Italia dal 1 gennaio 2001 al 31 dicembre 2009”, Nov. 2010, <http://ssai.interno.it/download/allegati/scioglimenti.pdf>.

and conditioned by mafias – i.e. within procurement contracts). Some reflections arise with respect to conducts specifically ascribable to organised crime.

Drug trafficking is still the main funding source available to organised crime. Local mafia-type criminal associations (*Ndrangheta* in the first place, followed by *Mafia* and *Camorra*) continue to play a crucial role within drug trafficking activities. By means of *ad-hoc* intermediaries, such criminal associations have developed progressive internationalisation of their respective criminal structures in perfect synergy with the components of main Colombian and South American cartels, which allows supplying goods for subsequent retail distribution of drugs.

The **gaming** segment, both legal and illegal, is of the highest interest to organised crime, as it has historically been an important source of proceeds. Currently, Mafia criminality invests in the gaming industry by acquiring gaming rooms under nominees, both to gain substantial returns quickly (especially if the rules are altered to clear players' winning chances or reduce government charges) and to illegally launder acquired capital. Furthermore, management of **illegal waste trafficking** is of particular interest to organised crime.

Sexual exploitation is estimated to mainly generate criminal proceeds reinvested outside the Italian economy. Such offence is in fact practiced essentially by foreign criminal organisations (mostly Romanian or however Eastern European, which generally reinvest profits from criminal activities into their respective Countries), except in specific cases (e.g. when the *Camorra* “managed” sidewalks), local criminal organisations have shown great interest in such illicit phenomenon.

Trafficking in human beings turns out to be almost exclusively run by foreign criminal organisations. It is no longer a matter of single organisations, rather they are all associated structures dependent on a leadership that remains abroad. Such criminal associations, known as “new mafias”, run the new market with a *modus operandi* that is typical of foreign mafias. As a result, only the last links of the chain can be hit in Italy and Europe.

2.2.2 Conclusions: synthesis assessment of Italy's system inherent risk of money laundering

Taking into account the predominant profiles of criminal proceeds that are generated within the national territory and are put back into the economic-financial domestic circuit to a substantial extent – although not specifically measured – the overall money-laundering threat is deemed as very significant. In consideration of very significant vulnerabilities identified within the social

and economic system, the inherent risk is associated to the maximum value attributable within the model (so-called **very significant** inherent risk).

Table 4 – Money-laundering inherent risk – Synthetic assessment

Threat	Highly Significant				
	Rather Significant				
	Lowly Significant				
	Non-Significant	Non-Significant			
		Non-Significant	Lowly Significant	Rather Significant	Highly Significant
System criticalities: use of cash and the shadow economy					

2.3 Terrorist Financing

The definitions of “*terrorism, terrorist, terrorist acts, for the purposes of terrorism and the related financing of terrorism*” are heavily debated within the related literature. At international level, it is preferred to opt for identification of a series of acts, activities and behaviours that need find a suitable response in terms of criminal penalties within national laws. Italy’s Legislative Decree N. 109/2007 defines *Terrorist Financing (TF)* as “... Any activity that aims, through any means, to collect, supply, mediate, deposit, hold or disburse funds or economic resources, in any way undertaken, wholly or in part, for the purpose of committing one or more criminal acts of terrorism or favour the commission of one or more criminal acts of terrorism covered by Italy’s Criminal Code, regardless of whether such funds or economic resources were actually used to commit said criminal acts”.

Terrorist organisations also fund their activities through legitimate sources and legitimate channels, which makes prevention particularly relevant. The scenario is extremely complex: if on the one hand the means to identify sophisticated forms of handling and re-use of criminal proceeds need be constantly fine-tuned, on the other hand, special attention shall be ensured as to less modern methods individual groups continue to adopt, as they more closely reflect the needs and socio-economic structures of the geographical areas concerned.

2.3.1 Context analysis – Terrorist threat evolution

Domestic terrorism. Italy's current socio-economic environment addresses, *inter alia*, other critical issues connected to job insecurity, illegal immigration and protests to major works realisation. Significant increase has been identified in terms of counter-information and initiatives of protest, often characterised by violence, with wide participation by anarchist groups. As far as Red Brigades terrorism is concerned, in a long-term perspective it is worth taking into due consideration propaganda activism by small-scale and minor circuits of Marxist-Leninist extremists committed to preserving the memory of past armed struggles.

More concrete and topical is the threat related to anarchic-insurrectionist groups inclined to promoting, rather than a top-down organisational structure, the creation of "informal groups", "affinity groups", which – as "self-managed stand-alone units" – carry out "direct action", namely "immediate and destructive" attacks against the State and capital.

The main threat is represented by Italy's Informal Anarchist Federation (*Federazione Anarchica Informale-FAI*) / International Revolutionary Front (*Fronte Rivoluzionario Internazionale – FRI*), which might newly manifest itself via violent operational modes. The recent anarchist trend aims at internationalising insurrectional conflicts to share the fight carried out by groups operating in Countries traditionally affected by libertarian radicalism. In recent years, several investigations have been carried out into *FAI* operational cells, which led to the arrest of several anarchic-insurrectionist individuals. We may not, therefore, exclude that anarchic-insurrectionist terrorism will persist in Italy in the near future. Over 2013, the trend relating to acts of violence based on such threat, as well as the signals of trans-national coordination of area groups, confirmed levels almost comparable to previous years. On the other hand, evidence of collaboration between anarchists and organised crime groups was not identified. The extreme right-wing scenario is very fragmented and currently does not reveal specific terrorist. In summary, the following findings are identified:

- **Domestic terrorism: Red Brigades matrix** – No elements worth signalling, no relevant information evidence, no judiciary findings. Hence the related terrorist financing risk is assessed as non-significant;
- **Anarchic-insurrectionist area** – It is estimated to express a lowly significant terrorist threat. In this regard, the low operational profile actions suggests reduced need to raise funds and, consequently, a non-significant risk of funding;
- **Right-wing extremist groups** – At present, experts assess such terrorist threat as non-significant.

Religious terrorism – The evolution of the Al-Qaida terrorist threat reveals significant evidence at national level, based upon investigations conducted between end-1990s and 2007 which highlighted, *inter alia*, structured Jihadist networks linked to Al-Qaida also actively recruiting militants addressed to Jihad contexts and training camps.

The gradual military decline of *Al-Qaida Core*, namely the historical core of the organisation founded by Bin Laden, has over the years coincided with dynamism of regional affiliate organisations (*Al-Qaida in Islamic Maghreb/AQIM*, *Al-Qaida in the Arabian Peninsula/AQAP*, *Al-Qaida in Iraq/AQI*) or ideologically contiguous affiliate organisations (*Islamic State of Iraq and the Levant /ISIL*, *Al-Shabaab*, *Boko Haram*).

At the same time, Al-Qaida propaganda in the Web has continued to be a primary source of inspiration and incitement to Jihadist terrorism, aiming to proselytism both in contexts affected by Arab-Israeli tensions and conflicts and among Muslims in the West – the latter incited (in the name of individual Jihad) to join battle sets or perform direct attacks in terrorists' Countries of residence. Since 2007, also in Italy, CFT has steered towards individual terrorists and micro-groups, lacking specific links with structured organisations, often self-radicalised in the Internet. At this stage, the threat of Jihadist terrorism in the Country as in the rest of Europe is mainly related to: events in Northern Africa (widespread activism of Salafi-Jihadist movements) and the Middle East; the evolution of the Syrian crisis; and the growing phenomenon of so-called *homegrown* extremism – i.e. Muslims born or raised in the West, including converted Muslims. That said, **religious terrorism threats are considered lowly significant in Italy**¹⁸.

Non-religious terrorism – Currently the activity of non-religious terrorist organisations, most of which have nationalist or separatist agendas (Basque Euskadi ta Askatasuna/ETA; Sri Lankan Liberation Tigers of Tamil Eelam/LTTE; Kurdish Partiya Karkerên Kurdistan – PKK/KCK), represent a non significant threat in Italy. The following table illustrates the above described elements.

¹⁸ The assessment was made ahead of recent Islamic terrorist events.

Table 5 – Terrorist threat relevance

Threat	Appreciated / Perceived relevance of terrorist threat
Domestic Terrorism	
a. Left-wing eversion	
a1. Red brigades area	Non Significant
a2. Anarchic-insurrectionist area	Lowly Significant
b. Right-wing eversion	Non Significant
International terrorism	
c. Religious terrorism	Lowly Significant
d. Non-religious terrorism	Non Significant

2.3.2 Origin, transfer and use of funds

Origin of funds. With regard to identified financing terrorism methods, the data and specimens so far emerged from in-depth analysis carried out in Italy by relevant police forces reveal different ways of supporting terrorist activities that, although converging towards the same goal, are attained through both lawful and unlawful activities.

As far as **lawful activities** are concerned:

- a) Profits and gains derived from activities carried out by Small and Medium Enterprises (SMEs) constituted and operating in various economic sectors, used as sources of legitimate income declared, in whole or in part, to relevant tax authorities.
- b) Donations by members of the Islamic community to charities, which – as detected – occasionally make a distorted use of parts of the sums received.
- c) Remittances from migrants, who have always needed to reach out a share of their earnings to their home countries in order to support their own families.

Remittances are predominantly based upon the use of the money transfer circuit, which enables transferring large amounts of money everywhere at low costs.

Furthermore, besides regular financial and banking intermediaries, there are also pseudo banking systems offering an alternative to official channels for transferring money, also of illicit origin – i.e., the so-called Informal Value Transfer Systems (IVTS), namely service companies and/or individuals without the required specific authorisations, which:

- are favoured by migrant workers, especially those without a residence permit, by reason of non-compliance with obligations in force for identification of the customer requesting the operation; and

- provide essentially trust-based services consistent with the needs of immigrants and traders settled in other Countries.

Unlawful activities range from drug trafficking to aiding and abetting illegal immigration, counterfeiting of trademarks, exploitation of illegal labour, unlawful betting collection, and illegal exercise of financial activity.

The conducts emerged as to terrorist financing primarily highlight the use of illegal economy circuits (e.g., drug trafficking) to raise the resources necessary to fulfill terrorist organisations' operational needs. It is also worth noting the circumvention of provisions relating to illegal immigrants in order to provide, upon payment, false permits to work in Italy. Among other less frequently identified modes: acquisition and receiving of stolen motor vehicles justified by way of lease financing to export/sell them in exchange of large amounts of money, receiving of forged documents and stolen goods, and trademark counterfeiting.

Transfer of funds: Patterns – The need to identify the originator of each transfer of funds remains a priority, and measures' effectiveness mainly depends on active collaboration between the financial and the banking sectors within the phenomenon prevention phase, mainly through CDD, record-keeping and reporting of suspicious transactions obligations. Following and assembling seemingly unconnected information that proves related to complex financial transactions may be crucial to understand how terrorists obtain and transfer the funds necessary for their activities and identify the leaders and members of groups linked to terrorist activities.

Funds collected within the national territory may either

- a) **remain in the national territory** – In this case, the flows generated in Italy fuel terrorist activities taking place in the Country – i.e. typically anarchic-insurrectionalist groups, such as *FAI*;
- or
- b) **be transferred abroad** – In this case, the flows generated in Italy fuel terrorist activities developed outside national borders. In line with typologies identified and highlighted at international level, investigations revealed such flows are transferred abroad through money transfer, payment remittance and cash courier circuits. This threat is assessed as “lowly significant”.

Funds raised abroad and transferred to Italy – Flows generated abroad do fuel organisations (more rarely, individual terrorists) that are active nationwide. This form of financing is less

frequent in Italy as, on the one hand, tracing flows is more effective and, on the other, it is generally easier to find resources within the Country rather than import them from less developed economies. Eventually, findings also reveal **funding from sources located abroad and addressed to terrorist organisations and/or individual terrorists working abroad** which, however, threaten western countries' interests. This is the case of cash flows feeding Al-Qaida related organisations/networks actively operating within Jihadist areas (e.g., Iraq or Afghanistan), where military forces are deployed or national interests are threatened by possible terrorist attacks. Amongst the mentioned categories of fund transfers (national/foreign origin; retention within national borders/transfer abroad), the first three may be subject to national authorities intervention, as *ad-hoc* preventive and repressive activities may be implemented to mitigate the associated financing risks. Conversely, the fourth category may require synergistic actions at supranational level.

Use of funds – Cash flows tracing by Italian authorities reflects the difficulty of ascertaining the actual causal links between transfers of funds and the financial support provided to criminal/terrorist organisations, notably when operating within foreign Countries – i.e. difficulty connecting cash to specific uses by individual terrorists and/or terrorist groups. Those using money to finance terrorism do not always hide and transform the resources intended to be allocated for the given purpose, they rather seek to hide and conceal the ultimate aim they pursue through those resources.

2.3.3 Conclusions: Synthesis assessment of Italy's inherent risk of terrorist financing

It is worth differentiating between the *terrorist threat* and the **terrorist financing threat**.

Only the latter, assessed in 2014 as lowly significant, is analysed within this document. Furthermore, in light of the very significant vulnerabilities affecting Italy's socio-economic system, the final assessment ascribed to the **inherent risk** is however “**rather significant**”.

Table 6 – Synthetic evaluation of TF inherent risk

Threat	Highly Significant				
	Rather Significant				
	Lowly Significant				
	Non-Significant				
		Non-Significant	Lowly Significant	Rather Significant	Highly Significant
Socio-economic system vulnerabilities: use of cash and the shadow economy					

3. ANALYSES OF VULNERABILITIES

The analysis of vulnerabilities was conducted by breaking down the overall system into the following phases: prevention, investigation, and repression. The analysis is common both to money laundering and terrorist financing, except for safeguards specifically designed to counter the latter phenomenon. As a whole, the **preventive and countering system appears as adequately responding** to the threat that the proceeds of criminal activities can be reinserted into the financial and economic system.

3.1 Preventive safeguards

Within Italy's preventive system, the analysis includes safeguards applied by relevant obliged entities, analysis of legal persons and trusts' transparency, cross-border checks, and suspicious transaction reporting. As to obliged entities, the vulnerability analysis is performed for the sectors obliged to implement anti-money laundering legislation according to their respective ability to fulfill the obligations set out therein and the risks specific to their operation. As to oversight, the methodology provides that, in the absence of implemented supervision, the maximum ranking shall be automatically assigned to vulnerabilities.

With respect to the overall anti-money laundering preventive system, the analysis primarily focuses on three pillars:

- Customer Due Diligence (CDD);
- Registration of significant relationships and transactions. In the case of Financial Intermediaries (FIs), such registration is carried out within the Unified Computerised System (*Archivio Unico Informatico – AUI*);
- Suspicious Transactions Reports (STRs).

Whereby possible, also profiles related to organisational structure and internal controls are here analysed. For some subjects¹⁹, current legislation only imposes the obligations of suspicious transactions reporting, but not CDD and registration obligations.

3.1.1 Safeguards enforced by obliged entities

¹⁹E.g., Public Administration offices; gold import/export and sale; antiques trade; auction houses and art galleries, etc.

Safeguards enforced by obliged parties – Anti-Money Laundering (AML) safeguards are unequally applied by the private sector. Such heterogeneity, revealed by uneven active collaboration, determines different impacts on the system depending on the scope of activity of each category.

The private sector has been analysed on the basis of two dimensions: the operational dimension, related to structural characteristics and activities performed (so-called “specific risk”), and the dimension related to vulnerability within the application of anti-money laundering measures. Joint evaluation of the two areas enables appreciating vulnerabilities within the risks identified (i.e. relative vulnerability).

With regard to **financial intermediaries**, it is worth underlining that:

- a) Delays in the implementation of measures aimed at fulfilling **CDD** obligations are more frequently identified within banks, as well as intermediaries in the securities market (*SIMs* and, mainly, *SGRs*). In particular, brokers should on the one hand solve residual problems of identification and verification of the so-called beneficial owner and, on the other hand, fully internalise the so-called Risk-Based Approach (RBA) in order to modulate both the extent and depth of obligations related to the concrete money-laundering risk linked to the customer;
- b) Failure to comply with requirements on **record-keeping and registration** of transactions within the *AUI*, such as: omitted or belated registrations; duplication or incorrect attribution of motives and/or ownership of operations; failure or misrepresentation of personal data. In most cases, dysfunctions are connected to technical-procedural problems; in some cases, conversely, violations are related to the obligation to retain the information collected to fulfill the CDD requirements.
- c) Infrequent anomalies (and related only to banks and finance companies) concerning restrictions on the use of **cash** and bearer bonds.
- d) **Weaknesses** have been identified **within proceedings aimed at evaluation and reporting of suspicious transactions** also within banks and on the occasion of inspections on *SGRs* and *EMIs/Payment Institutions*.

As follows some remarks on the vulnerabilities identified within different categories of obliged entities.

Banks and Poste Italiane are characterised by high operational risks: sector size, wide array of activities carried out, use of cash, and interconnection with foreign financial systems make them very exposed to the risk of being used as a tool for money-laundering and/or terrorist financing. Sector safeguards, which also benefit from pervasive prudential supervision mechanisms, help reduce such risks: incisive oversight and level of awareness of the phenomena addressed (i.e. active collaboration is an indicator) positively affect the ability to apply averagely appropriate measures provided for by sector legislation. Hence, a rather significant vulnerability level is identified.

Adequate safeguards are also present for **real estate brokerage companies** (*Società di Intermediazione Mobiliare – SIM*), **asset management companies** (*Società di Gestione del Risparmio – SGR*), and **investment companies with variable capital** (*Società d’Investimento a Capitale Variabile – SICAV*) and non-bank financial intermediaries as per Articles 106-107 of Italy’s Consolidated Banking Law (*TUB*), with respect to a relevant, though not maximum, operational risk.

The analysis of activities performed by *Cassa Depositi e Prestiti (CDDPP)* and by entities laid down in Article 10(c.2)(a), (b), (c) and(d) of Legislative Decree N. 231/2007, and the nature of the subjects to which they provide their services do not reveal specific areas exposed to money-laundering and/or terrorist financing risks. The safeguards in place indeed appear to be adequate. As far as the **insurance sector** is concerned, it is appropriate to differentiate insurance companies from insurance intermediaries, identifying their respective specific risk profiles (higher for enterprises) and vulnerabilities (higher for intermediaries), as intermediaries are currently overseen via group policy scrutiny rather than via direct supervision. Albeit with the mentioned differences, in both cases the assessment on relative vulnerabilities is: **lowly significant**. The life insurance sector is rich in products with substantial medium-term investment purposes, with low prevalence of social security products.

In light of their operational activity related to “shielding” property and ownership rights, **so-called static trusts** are associated to high risks. The sector is watched over by authorities, yet further strengthening is required in terms of implementation of existing safeguards. As such, the **overall assessment of relative vulnerability is: very significant**.

Very significant relative vulnerability is also identified for **Electronic Money Institutions (EMIs) and Payment Institutions (PIs)**, essentially due to the relevant EU regulatory framework that enable agents, through free provision of services and relocation processes, to operate in our territory without adequate regulatory and control frameworks. As a matter of

fact, investigations confirmed this distribution network fails to provide adequate barriers against illicit financial flows.

BOX n. 1 – Money transfer circuit and money-laundering risks

Money transfer business is closely linked to the large presence of migrant workers who send part of their earnings to own families living in their respective Countries of origin. While acknowledging the high financial inclusion benefits provided by money transfer activities, it is worth taking account, as identified at financial system supervisory level, of the evidently high money-laundering and terrorist financing risks connected with money transfer activities. Such risks stem from intensive/predominant use of cash and are linked to the service being deployed across the Country almost exclusively through “sale points”. Safeguarding money transfer networks from money-laundering risks proves notably difficult, due to the distribution network composition (i.e. operators mainly active within the non-financial sector – e.g. travel agencies, bars, tobacco shops, service centres, and Internet cafes, call centres, and exchange offices²⁰) and the nature of operations carried out (e.g. occasional transactions, transfer of low amounts apparently not deserving high attention, transfers of funds to Countries that lack robust anti-money laundering safeguards).

BOX n. 2 – Electronic money and money-laundering risk

The use of electronic money instruments has increased very markedly over recent years, also due to the policy aimed at combating use of cash.

The very features that make e-money instruments efficient and competitive versus traditional means of payments will also enhance their attractiveness in terms of illicit applications²¹. In the face of such risks, supervisory authorities have taken appropriate mitigation measures, pending a more restrictive revision of EU legislation.

Main market operators introduced thresholds both on the amount of balance available on each card, and

²⁰ This can help, e.g., pay attention to consistent transfers of fractional availability carried out via nominees.

²¹ As follows, such characteristics:

- Their management typically involves operators and intermediaries of various kinds, not all of them subject to controls or endowed with consolidated anti-money laundering “culture”. In addition, information gathered on customers is fragmented amongst operators;
- Due to the nature of prepaid funds, issuers may have less incentive to take complete and accurate information both on customers and the business relationship nature. As such, checks may be too costly, both in economic and procedural terms, not only for operators but also for customers;
- Transactions are executed and funds are withdrawn or converted into cash much faster than through traditional channels. This can hinder adequate monitoring of flows;
- Currently, cards are rechargeable and can be used indefinitely without geographical restrictions (thanks to international dimension payment circuits). Besides unlimited spending ceilings, they also enable moving funds anywhere and very easily.

the overall number of recharges performable on cards in the name of the same subject.

With regard to **financial agents** (Article 128-*quarter*(1) of Italy's Consolidated Banking Law – *TUB*) and **credit intermediaries** (Article 128-*sexies*(1) of *TUB*), incisive forms of control both in terms of access to the profession and performance of activities – together with the responsibility held by principal intermediaries and several and joint liability intermediaries in relation to financial agents conduct – contribute to curbing the specific risk, thus assessed as *medium*. The vulnerability level is deemed as lowly significant, as inspections revealed poor evidence. Therefore, such vulnerability is assessed as non-significant.

As to money-changers, the specific risk is negligible, due to the nature of operations and the low value (unit terms) of money change transactions. Vulnerability is rated as very significant, in application of the methodological rule which establishes that, in the absence of controls, vulnerability is automatically considered as maximum. The relative vulnerability level identified is therefore lowly significant.

Professionals generally do not fulfill preventive requirements, due to non-adequate *ad-hoc* training. Conversely, as adequate knowledge is necessary to such professional categories (notably in relation to subjective and objective elements of clients' operativeness), such gap results in very significant relative vulnerability for **notaries, lawyers, chartered accountants and accounting experts**. Besides, it is worth acknowledging the progress made by notaries both as to CDD obligations and active collaboration, which reveals a more satisfactory capacity to fulfill AML rules.

Auditors of Public Interest Entities (PIEs) are subject to pervasive oversight and reveal adequate safeguards and negligible specific risks. With reference to **other legal auditors** (enrolled within the Register introduced by Legislative Decree N. 39 of 27 January 2010), the recently established control system, although related to a high number of professionals, is characterised by wide-ranging and in-depth information collected to monitor adequate application of AML provisions. As such, relative vulnerabilities are assessed as non-significant. Apart from possible links with other professions associated to given levels of risk (i.e. chartered accountants), the activities performed by **labour consultants** do not reveal vulnerabilities specifically related to money laundering (rather to possible "irregular" labour). Within a **negligible risk context**, relative vulnerabilities are lowly significant.

This risk analysis includes only some figures of non-financial operators, selected as per their related vulnerability to possible infiltration by organised crime, as identified upon investigation

evidence: betting and gaming operators, cash-for-gold shops (“*compro oro*”), and real estate agents.

Mafia’s presence in the **betting and gaming** sector does not only concern illegal gambling; it also significantly encompasses some related legal activities. Hence, gaming typologies (not all falling within the scope of AML provisions) differ as to their specific risks and vulnerabilities. Among online gambling/gaming circuits, the platforms related to other EU Countries operating under free provision of services regime entail very significant vulnerabilities, as the related cash flows fully escape monitoring by authorities. Among gambling forms, it is worth recalling that so-called VLTs and fixed odds betting are easily usable within money-laundering operations.

The economic crisis led, among other things, to increased spreading of **cash-for-gold** shops (“*compro oro*”) – i.e. heterogeneous category of operators currently subject to the sole obligation to report suspicious transactions. Several investigations confirm **cash-for-gold** shops’ high operational risks and vulnerabilities, and recommends intensified safeguards.

Real estate is among ideal sectors for re-use of illegal proceeds from organised mafia crime and foreign illicit capitals. In terms of application of safeguards, although purchase/sale activities are detected by more mature categories, **real estate agencies** are not yet aware of their anti-money laundering role within such a high-risk context. Relative vulnerability is therefore highly significant.

Although subject to the obligation of reporting suspicious transactions, Italy’s **Public Administration** is not here analysed; yet, some remarks are advisable. To date, the overall sector is not aware of its possible role in such area; such vulnerability is not insignificant if we consider the relevant role played by corruption and/or by areas highly attractive to crime (e.g. EU funding or public procurement).

3.1.2 Legal persons and trusts – Analysis transparency

Both the analysis of property seized from criminality and investigative experiences show that criminal infiltration in businesses – although not generalisable across the national territory and all economic sectors – appears to be a relevant component of Italy’s shadow economy. Mafias do not favour sophisticated corporate structures; conversely, they prefer limited liability companies in which they can conceal their own presence by means of nominees. Likewise, the system does not show significant intrinsic vulnerabilities in terms of transparency: stringent civil legislation on governance and comprehensive information retrievable (via notaries and chartered accountants) from the Register of Businesses shall ensure that problem of access to

information on beneficial ownership concerns approximately 1% of the 6 million registered businesses.

Possible residual opacity indeed is identified amongst **legal persons** with connections or tools that may conceal property (e.g. "national" trusts and fiduciary service companies) or foreign corporate entities, especially within jurisdictions that either allow for corporate anonymity or have no adequate information gathering forms, or are poorly/non collaborative toward information exchange requests.

The system's most significant vulnerability can thus be associated to deficiencies within CDD safeguards in place, along with specific significant risks, resulting in rather significant vulnerabilities.

Trusts are increasingly widespread in Italy, generating several transparency problems, due to lack of adequate regulation by Italian legislation, and progressive dissemination, across the Country, of subjects acting as trustees (not surveyed at all), as well as professionals – i.e., obliged entities. Again, trustees do not appear to be well aware that their role also includes complying with anti-money laundering obligations. Furthermore, investigations and suspicious transaction reporting analyses reveal frequent use of trusts for illegal purposes, in particular for committing tax offences, money-laundering, bankruptcy, market abuse, and concealing illegal assets generated by organised crime. All such elements lead to assessing that trusts are associated to maximum vulnerability (i.e. "very significant relative vulnerability").

3.1.3 Cross-border controls

Cross-border controls have considerable strategic relevance, in light of cash use in Italy and illegal incoming/outgoing capital flows, usually of Italian origin. Safeguards in place thus appear adequate.

3.1.4 Analysis of Suspicious Transaction Reports (STRs)

The process of STRs analysis is generally effective: significant increase in reports from obliged entities, albeit unevenly distributed among all categories, and improving quality of reporting provide Italy's FIU with fundamental information. Such asset is effectively managed through integrated IT systems and risk-allocation procedures. The rising importance of STRs within judicial proceedings can be a good indicator of such assessment.

3.2 Investigative safeguards

In-depth analyses of STRs – STRs are also Italy's *Guardia di Finanza* and *Direzione Investigativa Antimafia – DIA* (Anti-Mafia Investigative Directorate) major information sources and assets, as highlighted by the significant number of reports related to criminal proceedings or considered of investigative interest. In-depth analysis of STRs is deemed as effective.

AML investigative activities – In general, judiciary institutions and tools contribute strong effectiveness to investigative actions (i.e. wiretapping, searches, undercover operations, cautionary measures, etc.). More pervasive investigative tools can then be utilised whereby money-laundering and/or re-use of illicit capital are connected to organised criminality. In light of the high number of investigations successfully completed – despite the persisting vulnerabilities – AML investigative activities can be assessed as generally effective.

CFT investigative activities – The investigation experience did not identify particular weaknesses having negative impacts on the effectiveness of CFT investigative activities, which therefore is assessed as effective. All investigative activities performed identified the absence of adequate cooperation from Countries experiencing socio-political or institutional instability – which practically resulted in restricting the scope of evidence gathering or falling back upon verification of other types of offences possibly related to terrorist financing.

Cooperation between Italian authorities is generally positive in both sectors and represents an asset, notably among those authorities traditionally engaged in combating these phenomena – i.e., Italy's Financial Intelligence Unit, *Guardia di Finanza*, relevant supervisory authorities, and the judiciary have effective cooperation channels also able to mitigate some regulatory shortcomings.

3.3 Repressive safeguards

AML: capacity to sanction the authors of ML crimes – Current Criminal Code provisions for money-laundering criminalisation – excluding punishability for those individuals participating in the related predicate offence(s) – do not suit today's scenarios, as they were introduced back in the 1980s and subsequently amended. Within the current environment, the proceeds of illegal activities are laundered in new ways.

Within the repressive experience on organised criminality, money-laundering often starts from participation by the author of the related predicate offence(s). Main difficulties arise in terms of assessment of money-laundering offences committed by third parties. From such point of view, the introduction of self-laundering instances would favour money-laundering punishability. Repressive safeguards are therefore affected by vulnerabilities assessed as rather significant.

CFT: capacity to sanction the authors of TF crimes – With reference to TF-related offences, the shortage of available statistical data does not allow for adequate assessment of the effectiveness of the sanctioning system set up by law. However, the experience of law enforcement bodies and, in particular, the impact deriving from difficult international cooperation lead us to assess the presence of rather significant vulnerabilities, although exogenous to our system.

AML: Seizure and confiscation – Preventive measures and specific regulations for the fight against organised crime provide massive capacity of aggressing criminal assets. The process is therefore considered effective.

3.4 Ad-hoc CFT safeguards

Freezing measures – Italy's CFT system relies upon typical AML preventive, investigative and repressive activities, as well as application of specific measures arising from UN Security Council Resolutions 1267 (1999) and 1373 (2001) and relevant Community framework for implementation, with national integrations. At organisational level, the cornerstone for implementation of such measures is Italy's Financial Security Committee (FSC).

Over 2010-2012, all communications relating to the freezing of funds were made by financial intermediaries. In most cases, the freezing related to the failure to perform wire transfers or transfers of funds to/from listed subjects, or bank accounts frozen as a result of the listing. In some cases, international cooperation between FIUs enabled solving homonymy cases, thus avoiding freezing measures imposed on individuals actually not liable to punitive measures. The CFT system detects certain criticalities/vulnerabilities connected to professionals and non-financial operators' (DNFBPs) poor inclination to notify funds freezing measures.

Non-profit sector – In light of the sector heterogeneity, the TF preventive system does not operate through provisions directly addressed to non-profit entities, but indirectly through measures put in place by obliged entities – i.e., CDD and STRs. The evidence resulting both

from the analysis of STRs and investigative elements does not suggest Italian non-profit entities' involvement in TF activities currently poses a threat. However, the checks carried out by relevant public authorities are pervasive and provide an adequate level of transparency, although they cover different and multiple aspects. Consequently, the specific risk identified is negligible, and vulnerabilities are assessed as lowly significant. This results in **non-significant relative vulnerability**.

4. CONCLUSIONS AND ACTION LINES

Within the analysis of threats, the assessment may be translated into a single synthetic opinion on ML and TF related risks, which are assessed as **very significant** and **rather significant**, respectively. As far as the analysis of vulnerabilities is concerned, it is not always easy to summarise the system’s overall vulnerability in a synthetic judgment; yet, simple mathematical formulas may be applied to favour aggregation.

4.1 Preventive safeguards implemented by obliged entities

In relation to the relative vulnerability identified with respect to the specific risk profile of each operator, advisable interventions are characterised by different priority levels (Table 7).

Table 7 – Interventions’ priority levels, broken down by examined categories

	Analysis	Dialogue and Training	Operational and regulatory interventions	Supervision/Control enhancement
FINANCIAL INTERMEDIARIES				
Banks & Bancoposta				
EMIs and PIs (incl. distribution networks)				
Financial entities as per Articles 106-107 TUB				
SIMs & SGRs				
Cassa Depositi e Prestiti and others				
Insurance companies				
Insurance brokers				
Trust companies				
Agents, brokers and money-changers				
PROFESSIONALS				
Notaries				
Lawyers				
Chartered accountants and accounting experts				
Legal auditors of PIEs				
(So-called “ordinary” Auditors				
Labour consultants				
NON-FINANCIAL OPERATORS				

Gaming and betting operators			Medium-High Priority	Medium-High Priority
“Compro-oro” (Cash-for-gold shops)			High Priority	Medium-High Priority
Real estate agencies		Low-Medium Priority		Medium-High Priority

Legend – Priority levels

-  Low Priority
-  Low-Medium Priority
-  Medium-High Priority
-  High Priority

Financial Intermediaries

As for financial intermediaries, the supervisory and preventive system in place is sufficiently sound to cope with a remarkable volume of customers and operations both in terms of wide-ranging scope and territorial coverage. Internal controls required by law and supervision by Bank of Italy and CONSOB integrates the work accomplished by the FIU and relevant *GdF* units/departments that, within their institutional activity, detect and notify the administrative violations identified.

In future perspective, *it is necessary to preserve current control and enforcement instruments and dedicated human resources*, as most cash flows pass through financial intermediaries. It is furthermore necessary, in cooperation with relevant sector associations (e.g. *ABI*), to keep developing appropriate and pervasive training interventions and actions aimed at clarification of recent regulatory provisions, as well as continue to update and expand the use of anomaly indicators provided by Italy’s FIU as a result of analysis and study of concrete typologies.

For entities such as EMIs and *SGRs*, the existing safeguards should be maintained while paying special attention to riskiest operations, which require *ad-hoc* controls.

With regard to EMIs and PIs, the risk inherently associated to remittance activities (money transfers) should be pondered as per type of customer and operations (cash) and the need for financial inclusion of disadvantaged people, who risk being targeted by clandestine networks. The entry into force of the Fourth Directive will harmonise the EU framework in order to prevent softer controls and procedures implemented in other EU Countries from resulting in unequal treatment likely to distort competition and attract activities towards less safeguarded systems.

Trust companies are by nature exposed to high risks of opacity, already acknowledged by the preventive system, which shall continue to strongly oversee such category.

Agents, brokers and money changers, although subject to a regulated access system, shall be *subjected to more pervasive safeguards*.

The insurance sector, eventually, is assessed as rather safeguarded. As far as insurance intermediaries are concerned, additional effort should be ensured notably in a risk-based approach perspective. In this regard, the draft-law currently under discussion would, whereby approved, leave insurance agents and brokers uncovered by relevant authority supervision, thus creating a legal vacuum. In this regard, the FATF Recommendations establish that also such persons are obliged²² to implement AML/CFT legislation.

Non-Financial Operators

For non-financial operators, subject to potential and concrete infiltration by organised crime, further harmonisation of supervisory interventions should be pursued.

It is furthermore important to underline the strategic need for active collaboration within this sector. Reports from entities other than financial intermediaries can provide several suggestions in terms of better understanding and knowledge of a category of obliged entities requiring strengthened supervision and greater understanding of the sector characteristics.

In light of cross-border activity risks, the EU framework should be further harmonised by means of the Fourth Directive with regard to gaming operators; conversely, supervisory safeguards should be enhanced in the areas affected by main vulnerabilities.

With regard to cash-for-gold shops (*“compro oro”*), eventually, regulatory interventions are required, and awareness of their role should be raised within the market also through *ad-hoc* guidelines.

Professionals

Relevant authorities deem professionals do not have adequate awareness of the active role they are called for to play within AML and CFT safeguards. Dialogue with professionals is therefore required; furthermore CDD is of strategic importance and should be enhanced. Regular dialogue with such professional groups should be aimed at:

- In-depth analysis of relevant operation areas to better target their interventions;
- Developing CDD guidelines;
- Identifying *ad-hoc* mechanisms to ensure reporting confidentiality;
- Raising overall awareness of the reference role played by professional associations.

Furthermore, inspection activities should be intensified. With regard to labour consultants, the sector has not been subject to inspections for verification of AML legislation application and,

²² The definition of “financial intermediaries” in the FATF Glossary also encompasses *insurance agents* and *brokers*.

although the related specific risk is negligible, a proper control system should be ensured by relevant supervisory authorities.

With regard to statutory auditors, notably those supervised by Italy’s Ministry of Economy and Finance, their monitoring activities should be integrated with typical AML obligations ascribed to professionals. Regarding EIP auditors, in the face of adequate supervisory safeguards and a comprehensive regulatory framework, dialogue and *ad-hoc* training should be ensured in light of possible access to the category by individuals subject to different regulation, whereby they acquire EIP assignments.

Legal persons and trusts

In relation to the level of vulnerability identified with respect to the specific risk profile, interventions are distinguished as per different levels of priority (see Table 8).

Table 8 – Priority of interventions for legal persons and trusts

	Analysis	Dialogue and Training	Operational/Regulatory interventions	Supervision/Control enhancement
Legal Persons				
Trusts				

Legend – Priority levels

- Low Priority
- Low-Medium Priority
- Medium-High Priority
- High Priority

As to vulnerabilities identified in the category of legal persons and trusts, it is necessary to:

- Systematically identify the final beneficiary(ies) of businesses, and ensure necessary EU and international collaboration, so as to enable authorities to have timely access to such information. This objective is intimately tied to a desirable Community intervention, notably in order to harmonise and interconnect the Registers of Businesses of EU Member States;
- Ensure application of strict CDD safeguards by obliged entities (professionals), whereby they provide services to businesses.

Such considerations apply to both categories examined, with greater emphasis on trusts, more and more frequently used for illegal purposes, in particular tax offences, money laundering and

bankruptcy. In this regard, mitigating transparency-related vulnerabilities essentially implies retrieving information both on professionals who played a role in the establishment and/or management of domestic/foreign trusts, and on trustee(s) with residence, registered office or administrative centre(s) of activity in Italy and abroad. Correct CDD implementation is of key importance, as it allows collecting cross-cutting information on trusts established both in Italy and abroad. The entry into force of the Fourth Directive shall provide access to information on trusts at national level. Italy's national legislation shall then be consistently adapted and provide for a mechanism to ensure such access.

4.2 Investigative safeguards

International cooperation

Aiming to strategic integration of international information channels, strengthening internal collaboration procedures is recommended, for instance via an *ad-hoc* protocol aimed at defining procedures for exchange of information between Italy's *GdF*, *DIA* and *FIU*. At legal/judiciary level, Italy can provide wide cooperation and assistance to applicant Countries within the fight against international crime.

4.3 Repressive safeguards

A relevant statistical data and information system on legal/judiciary activities should be ensured, as *ad-hoc* statistical systems may enable better understanding of the national system's repressive capacity which, in the absence of adequate and updated relevant information, is likely to be distorted or underestimated.

Self-laundering criminalisation – The lack of "self-laundering" criminalisation seriously compromises the ability to punish perpetrators also in terms of ensuing effects on provisions and international cooperation. The process is affected by most significant vulnerabilities. However, over the years, the development of other mechanisms – e.g. preventive measures or application of confiscation per equivalent to a wider range of offences – in a context characterised by massive criminal conducts connected to organised crime and tax evasion has enhanced the effectiveness of the investigative phase, including seizure and confiscation activities.

Transposition of EU legislation on Joint Investigation Teams (JITs) – The transposition of EU legislation on Joint Investigation Teams will play a fundamental role: given the transnational

nature of several crimes, the opportunity to strengthen cooperation between investigative forces and, as such, the acquisition of evidence within the process is relevant.

Table 9 – Safeguards: action lines

	Analysis	Operational actions	Supervision / Control measures	Regulatory actions
Investigative safeguards				
In-depth analysis of STRs				
Investigative activity:				
AML				
CFT				
Repressive safeguards				
Capacity to sanction the authors of crimes				
AML				
CFT				
Seizure and confiscation				

Legend – Priority levels

- Low Priority
- Low-Medium Priority
- Medium-High Priority
- High Priority

4.4 Ad-hoc CFT measures in place – Listing, de-listing and freezing

With regard to identified vulnerabilities, it is required to:

- Define operational guidelines and procedures that, whereby deemed necessary, enable promptly complying with UN listings on a national basis.
- Promote the initiatives necessary within the EU on the review of Regulation (EC) N. 881/2002 for *freezing* to include the funds and resources owned/controlled in part by designated subjects and the funds and resources of persons/entities acting on behalf or under the direction of designated subjects.
- Encourage activities related to suspicious transaction reporting by most deficient professional groups, also via *ad-hoc* training activities.

Non-profit sector

With regard to the vulnerabilities identified, more coordination should be ensured between the competent authorities that oversee the sector in various capacities, in order to promote dissemination of information on the specific issue of terrorist financing and the risk of abuse in the related sector.

Table 10 – Action lines

	Analysis	Operational measures	Supervision/Control measures	Regulatory measures
Listing, de-listing and freezing				
Non-profit sector				

Legend – Priority levels

-  Low Priority
-  Low-Medium Priority
-  Medium-High Priority
-  High Priority