



COUNTER-TERRORISM

POLICY

Version n.1 – 20 December 2017

Summary

| | |
|--------------------------------------|----------|
| BACKGROUND | 3 |
| POLICY STATEMENT | 3 |
| SCOPE | 3 |
| SOURCES OF AUTHORITY | 4 |
| PROCEDURES APPROACH | 5 |
| ENFORCEMENT | 5 |
| REPORTING | 8 |
| ANNEX 1 | 9 |
| INTERNATIONAL | 9 |
| AUSTRALIA | 9 |
| CANADA | 9 |
| EUROPEAN UNION (EU) | 9 |
| DENMARK | 9 |
| FRANCE | 10 |
| GERMANY | 10 |
| JAPAN | 10 |
| NETHERLANDS | 10 |
| NEW ZEALAND | 10 |
| NORWAY | 10 |
| UNITED KINGDOM (UK) | 10 |
| UNITED STATES OF AMERICA (USA) | 11 |
| SWITZERLAND | 11 |
| INTERNATIONAL REGULATIONS | 12 |
| <i>United Nations</i> | 12 |
| <i>Community Regulations</i> | 12 |
| <i>GAFI Recommendations</i> | 13 |
| NATIONAL REGULATIONS | 13 |
| REGULATORY REFERENCES | 14 |

BACKGROUND

As an NGO operating in 23 countries, **Cesvi** recognizes that there may be a risk of its donor funds being diverted by staff, contractors, financial service providers and partners to finance or support terrorist activities.

Cesvi recognizes that, as other sectors (e.g. profit sector) are tightening their safeguards against terrorist abuse, there is a risk that terrorist organizations may focus more attention on non-profit sector.

Cesvi recognizes that different countries have different approaches and levels of regulation and safeguards and has therefore developed the present policy to ensure that **Cesvi** is consistent in its approach.

Cesvi believes that strong effective governance, financial and partner management are key to preventing abuse. This policy highlights the mechanisms in place. The issue of diversion of aid and contravention of counter-terrorism legislation is viewed as an internal control and risk management issue alongside fraud, bribery and corruption.

Cesvi has developed this policy to ensure that **Cesvi's** and donor funds and resources are not being used directly or indirectly to support terrorist activities and to provide a clear guide on what to do if terrorist activity is suspected. More broadly, this policy will enable **Cesvi** to support sustainable development and reputation in delivering sustainable overseas aid, as well as ensure continued community support for overseas aid projects.

Our donors have extensive legislation around anti-terrorism and national security. International and national bodies impose strict obligations on funding recipients to ensure that funds do not support terrorist activities. **Cesvi** will use its best practices and principles to ensure that our programs are conducted in the context of these laws and obligations.

Failure to comply with donor requirements could significantly impact the reputation of **Cesvi** as well as expose the organization to potential penalties. This policy therefore articulates **Cesvi's** commitment to avoid involvement in terrorist activities and terrorist financing and outlines processes and procedures aimed at preventing, stopping, and punishing terrorism financing that can potentially lead to the diversion of humanitarian aid or assistance.

POLICY STATEMENT

Cesvi renounces all forms of terrorism and will never knowingly support, tolerate or encourage terrorism or the activities of those who embrace terrorism. Consistent with numerous United Nations Security Council resolutions, including S/RES/1269 (1999), S/RES/1368 (2001), and S/RES/1373 (2001), **Cesvi** is firmly committed to the international fight against terrorism, and in particular, against the financing of terrorism. It is the policy of **Cesvi** to seek to ensure that none of its and its donor funds are used, directly or indirectly, to provide support to individuals or entities associated with terrorism. In accordance with this policy, **Cesvi** undertakes to use reasonable efforts to ensure that none of its or its donor funds are used to provide support to individuals or entities associated with terrorism.

SCOPE

This policy applies to all **Cesvi** board members, staff, volunteers, financial service providers and contractors (suppliers, service providers and consultants).

This policy also applies to all partner organisations, their board members, staff, volunteers, financial service providers, contractors and sub-grantees implementing projects with **Cesvi** funding.

SOURCES OF AUTHORITY

International and national regulations: Cesvi recognizes the regulations by which donor countries abide. Cesvi also recognizes relevant legislation related to data protection (refer to Annex 1).

- DDLL 18 febbraio 2015 n.7, pubblicato in G.U. 20 aprile 2015, n.91, coordinato con la legge di conversione 17 aprile 2015, n.43 – *nuove Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale;*
- DDLL 21.11.2007 n.231 – *prevenzione dell'utilizzo del sistema finanziario a scopo riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo;*
- DDLL 22.06.2007 n.109 – *misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale;*
- LL 15.12.2001 n.438 – conversione in legge del DDLL 18.10.2001 n. 374 – *disposizioni urgenti per contrastare il terrorismo internazionale;*
- LL 14.12.2001 n.431 – conversione in legge DDLL 12.10.2001 n. 369 – *misure urgenti per reprimere e contrastare il finanziamento del terrorismo internazionale;*
- D.Lgs. 8 giugno 2001, n.231 – *disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n.300;*
- Decreto Legge 6 settembre 2011 n.159 – *codice delle leggi antimafia e delle misure di prevenzione – integrato da D.Lgs. 13 ottobre 2014, n.153;*
- Legge n.155 del 31 luglio 2005 (convertito in legge da Decreto Legge 27 luglio 2005, n.144) *recante misure urgenti in contrasto con il terrorismo internazionale (c.d. Pacchetto Antiterrorismo);*
- Legge 6 febbraio 1980, n.15 – (convertito in legge, con modificazioni, dal Decreto Legge 15 dicembre 1979, n.625), *concernente misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica;*
- D.Lgs 25 maggio 2017 n.90 (recepimento direttiva 2015/849) – *Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi.*

Cesvi has endorsed the Red Cross and Red Crescent codes of conduct (since 2003) and the CHS Alliance (since 2015);

Furthermore **Cesvi** has developed its own policies which include:

- Security Policy (2017)
- Audit charter (2006)
- Acquisitions procedures (updated edition 2014)
- Project management and reporting procedures
- Program document on security - privacy document DL 196/2003
- Management of relations with individual donors (2007)
- Evaluation of risk document - in compliance with decree DL 626/94 now TU81/2008 (2007- 2008)
- Guidelines on human resources management and staff codes (2008)

- Guidelines on Safety and Security
- Guidelines on the prevention of corruption and fraud
- Logistics Manual
- HQ Administrative Manual (2015) and Country operational guidelines
- Sharing cost policy (2014; 2nd edition 2016)
- Foreign Office Administrative Manual (currently being developed)

PROCEDURES APPROACH

Cesvi's procedures have a strong emphasis on “deter, detect, prevent, and respond”. To minimize the risk of aid diversion, and in particular terrorism financing, **Cesvi** employs the following approach:

1. Conducts regular risk analyses concerning anti-terrorism activities. The risk analysis typically includes a review of the relevant legal requirements of donor governments, transit governments (e.g., territories through which goods or services are transferred), and host state governments, as well as donor policies and industry standards (if any) from other sectors. It also includes security analyses, including stakeholder analyses (armed groups, state and non-state actors), to determine the risk of terrorism targeting or undermining **Cesvi's** operations.
2. Enforces a strict code of conduct among its staff and staff of partner organizations with a strong reference point to anti-diversion and a statement on financial transactions with armed groups.
3. Maintains comprehensive financial records which account for all expenditure and publishes annual financial statements with detailed breakdown of incomes and expenditures.
4. **Cesvi** produces an yearly audit performed by a major auditing company, certifying the transparency and consistency of accounting, organization and procedures in the course of the various financial years. Control monitoring by the auditing company has been extended to effectiveness of on-site activities. As partner of the European Commission **Cesvi** is subject every three years to a procedural and organizational review at headquarters and field level Countries. This review is carried out every three years by ECHO (European Commission's Humanitarian Aid and Civil Protection). It happens similarly with USAID, which monitors the Foundation's economic and financial situation on a yearly basis. Furthermore, there are routine inspections and final reviews conducted on the great majority of projects.
5. Regularly trains its staff and partners on anti-fraud and corruption, procedures and practices.
6. Conducts an in-depth due diligence of partners and sub-grantees, including Third Party Reference Check to ensure the partner/sub-grantee does not appear on the US Office of Foreign Asset Control (OFAC) list, UK Treasury lists, EU proscribed lists and UN sanctions lists. The check is performed manually comparing the references with the main international control lists.
7. Applies a “know your supplier” principle for procurements for all national, international and restricted tenders.

ENFORCEMENT

The security measures in Italy and in the field are applied as per **Cesvi's** operating structure. While the CEO at headquarters is responsible for the application of security measures in Italy, security measures abroad are applied along the operational structure hierarchy, from the COO, to the Head of Project Department, to the Area Desk together with the Heads of Mission.

The **COO** is responsible for

- Ensuring that **Cesvi** and all staff members, volunteers and contractors comply with all relevant legislation,

Cesvi Code of Conduct and Cesvi policies;

- Ensuring that all partner organizations and their board members, staff members, volunteers and contractors implementing aid and development projects funded by or through Cesvi comply with all relevant legislation and policies.

The **Heads of Mission** are responsible for:

- Ensuring compliance with relevant legislation and Cesvi policies;
- Communicating this policy to all partner organizations and their board members, staff members, volunteers and contractors implementing projects funded by or through Cesvi and ensuring that they comply with all relevant legislation and policies;
- Approving activities after all conditions have been met;
- Providing the General Direction with all relevant information which relates to breaches of this policy

All **employees** and **volunteers** are responsible for:

- Complying with this policy and other relevant legislation.

Cesvi HR Unit is responsible for:

- Recruitment of employees and volunteers, and any additional Third party reference checks which may be employed in sensitive and/or high risk countries;
- Ensuring that each member of staff abides by Cesvi Code of Conduct and Ethical Code;
- Ensuring adherence to relevant data protection legislation;
- Providing support to managers and other staff during any complaint or dismissal process.

Cesvi Security Unit is responsible for:

- Ensuring that up to date risk assessments and context analyses are undertaken for each area of intervention to identify risks (of aid diversion).

Cesvi Administrative and Finance Unit:

- Receives from the field updated accountancy and the cash/bank reconciliation items (digital and pdf) that allow correct account keeping and continuously monitoring of all the transactions. **Cesvi** maintains a multi-currency accounting system that allows tracking of all transactions with a unique reference (voucher number) in the system at country level. Every transaction, and in particular every expense, is linked to a specific project with the accounting paperwork and other documents (contracts, procedures, invoices, receipts);
- Is responsible for monitoring the use of **Cesvi's** funds: through internal control mechanisms at area, capital and HQ levels. The HQ performs a daily check on the project financial flows. In the field the controls are carried out weekly in the cash reconciliation phase and monthly in the bank reconciliation phase. These tools and procedures are explained in detail in the Foreign Office Administrative Manual (currently being developed). The local office makes available the accountancy documents monthly to enable a timely monitoring of financial flows, expenses and incomes;

- Is responsible for the selection of banks/financial institutions: following a due diligence check, including third party reference check, evaluating together with the HQ the various banks present and available in the country;
- Is responsible for the bank management: authorized levels to carry out financial operations, segregation of duties, signatures (with mandate from HQ) and monthly bank reconciliations all contribute to giving a clear picture on the use of funds and to preventing misuse;
- Is responsible for cash management: cash keeping processes, segregation of duties, weekly cash monitoring and monthly reconciliations contribute to giving a clear picture on the use of funds and to preventing misuse;
- Is responsible for money transactions:
 - Checking is done before payment: as defined in **Cesvi's** Finance Manual, no commitment to purchase can be made without authorization from the responsible person. The purchase must be documented with both internal (prior approval of the expense, including purpose of the transaction and reference to the budget line of the donor's contract, procedure and contract) and external documentation (invoice, bill, receipt, delivery note or other proof that the goods or service have been provided). Then payment can be made and booked in the system.
 - Bank transfers are preferred. In case of payment to be done in cash, a specific procedure as to be followed with identity check of the person coming to collect the payment at the office.
 - Following any payment by **Cesvi**, a confirmation of the receipt of funds is systematically requested.
 - Donations can only be accepted - as any other source of funding going through **Cesvi** – upon HQ review and validation.
 - No donation can be done by **Cesvi** to an external entity without HQ review and validation, due diligence of the entity and signature of a contract.
- Is responsible for procurement and contractor/supplier management based on the “know your supplier” principle which includes Third Party Reference check to ensure that contractors does not appear on the US Office of Foreign Asset Control (OFAC) list, UK Treasury lists, EU proscribed lists and UN sanctions lists;
- Is responsible for administering Ethical Procurement Policy for suppliers.
- Is responsible for controlling the use of Cesvi assets and stocks through internal control mechanism at area, capital and HQ levels and performed on a daily basis and reported from field to HQ on a monthly basis as detailed in the Logistics Manual.

Cesvi Project Unit is responsible for:

- Due diligence and selection of partner organizations;
- Training and oversight of partner organizations (with support of above departments);
- Project cycle management, incl. monitoring and evaluation to improve the relevance, quality and accountability of **Cesvi's** programs;
- Ensuring beneficiaries are identified on the basis of the needs only and not vetted/screened in fulfillment of principles of humanity and impartiality;
- Management of the beneficiary complaints and response mechanism.

Cesvi Legal Department is responsible for:

- Compliance with **Cesvi** procedures including Anti-Fraud and Corruption Policy.

Cesvi Audit Department is responsible for:

- Monitoring of this policy and adherence by staff, volunteers, partner organizations and contractors to this policy;
- Providing an independent assurance perspective with regard to all **Cesvi** operations.

REPORTING

In case of suspected terrorism related activity any **Cesvi** staff member is encouraged to report to: whistleblowing@cesvi.org or to the Supervisory Body that will:

- Investigates according to **Cesvi's** Anti-Fraud and Whistleblowing Policy and takes action accordingly;
- Notifies the donor immediately if any link is discovered between funds, an assisted organization and terrorist related organization.

This policy was endorsed by the **Cesvi Executive Board** on 20 December 2017

ANNEX 1

International

UN Security Council Resolution (UNSCR) 1373 obliges Member States to prevent terrorist financing (freezing assets, criminalizing fund-raising and economic support to terrorist activities) and improve judicial cooperation and border controls. The Resolution also created the new Counter-Terrorism Committee (CTC) to monitor its implementation.

- UNSCR 1267 (sanctions list covering Al Qaeda, Taliban and associates)
http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml
- International Convention for the Suppression of the Financing of Terrorism (the “Terrorism Financing Convention”)
- Financial Action Task Force (Special Recommendation 8 in International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation: The FATF Recommendations, February 2012)

Australia

Note: UN terrorist lists apply for sanctions. National list maintained by Foreign Minister.

- Australian Criminal Code (102.6, 102.7, 102.8 Terrorism financing and association)
- UN Charter Act (empowers Foreign Minister to list individuals and entities in implementation of UNSCR 1373. Designations under UNSCR 1267 are automatically incorporated into Australian law)
- Autonomous Sanctions Act 2011

Canada

Note: UN terrorist lists apply for sanctions. Canada also maintains a national list established by the Governor General in Council.

- Canadian Criminal (Code 83 as amended by Anti-Terrorist Act)
- Charities Registration (Security Information Act)
- United Nations Act (for counter-terrorism sanctions)

European Union (EU)

Note: UN/EU terrorist lists apply for sanctions although some judicial rulings have led EU to revise its implementation of the UNSC lists.

- Framework Decision on combating terrorism 2008/919/JHA
- EU Council Regulation 2580/2001: EU sanctions list pursuant to UNSCR 1373
- Regulation (EC) No 881/2002 implementing UN sanctions lists of UNSCR 1267

Denmark

Note: EU terrorist lists apply for sanctions. No separate lists maintained.

Penal Code 2002 explicit terrorist offences contained in it.

France

Note: EU terrorist lists apply for sanctions. French Finance Minister empowered to create national list of entities connected with terrorism.

Code Penal penalizes financing of terrorist organizations along same lines as the Terrorism Financing Convention

Germany

Note: EU terrorist lists apply for sanctions. No separate list maintained.

- Criminal Code
- Money Laundering Act (1993) amended 2002 (criminalizes financing of terrorism)

Japan

Note: UN terrorist lists apply for sanctions. It also maintains an independent list.

- Criminal Code
- Act on Punishment of Financing of Offences of Public Intimidation (2002)
- Prevention of Transfer of Criminal Proceeds (2007 amended 2011)

Netherlands

Note: EU terrorist lists apply for sanctions. Foreign Minister, Ministers for Security and Justice and Finance may jointly agree sanctions against additional individuals/entities.

- Dutch Criminal Code (also contains liability for violation of Terrorism Financing Convention under Article 4 Dutch Criminal Code)

New Zealand

Note: UN terrorist lists apply for sanctions. It also maintains an independent list maintained by the Prime Minister.

- Terrorism Suppression Act (2002) (fulfils obligations under UNSCRs 1373 and 1267)
- Anti-Money Laundering and Countering Financing of Terrorism Act 2009

Norway

Note: Norway implements the UNSC 1267 lists. It does not maintain its own list. It stopped following EU list in 2006 on the grounds that continued alignment may affect its role as a neutral facilitator in certain peace processes.

- Criminal Code 1902 amended 2002
- 1968 Statute on Implementation of Mandatory Decisions of the UNSC

United Kingdom (UK)

Note: EU terrorist lists apply for sanctions. It also maintains a national list of designated persons, not groups).

- The Terrorism Act (2000) and Anti-Terrorism Crime and Security Act (2001).
- The Terrorism Act (2006).

- The Terrorist Asset-Freezing etc. Act (2010). Incorporates UK obligations under Security Council Resolution 1373, EU Council Regulation 2580/2001, UNSCR 1267 and EU Regulation 881/2002.
- The Terrorism Prevention and Investigation Measures (TPIMs) Act (2011).
- Charities Act 2011 (see also Charity Commission Compliance toolkit)

United States of America (USA)

Note: UN terrorist lists apply for sanctions. National list of Foreign Terrorist Organizations (FTOs) maintained.

Individuals and organizations subject to two specific Executive Order sanctions regimes: Executive Order 13224 and Executive Order 12947. Sanctions administered by OFAC (Office of Foreign Assets Control)

<http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>

- USA Patriot Act
- The USA (Uniting and Strengthening America) Act 2001 is an expansion of the Foreign Intelligence Surveillance Act (FISA) 1978.
- Executive Order 13224 Blocking Property and prohibiting transactions with persons who commit, threaten to Commit or Support Terrorism 2001. Anti-Terrorism Certification (ATC) confirming that they do not provide material support or resources to any terrorist individual or entity. (The ATC derive from Executive Order 13224)
- Executive Order 12947 Prohibiting Transactions with Terrorists who Threaten to Disrupt the Middle East Peace process

Switzerland

Note: UN terrorist lists apply for sanctions. Finance and Economy ministries also maintain their own lists.

- Code Penal 21 December 1937 updated 01 January Articles 306 (criminal organization), 305 (money laundering) and 305 (lack of vigilance in financial operations and the right of communication). The Code Penal sanctions any offence committed within the context of organized crime (money laundering, corruption, fraud, drug trafficking, etc.)
- Federal Act of 12 December 2014 on the Prohibition of the 'Al-Qaida', 'Islamic State' groups and related organizations (updated)
- Federal Act of 22 March 2002 on the Implementation of International Sanctions (Embargo Act, EmbA) (updated 27 July 2004), SR 946.231
- Federal Act of 10 October 1997 on Combating Money Laundering and the Financing of Terrorism in the Financial Sector (Anti-Money Laundering Act, AMLA) (updated 1 Jan. 2015), SR 955.0

Source: <http://uif.bancaditalia.it/normativa/norm-contr-terr/>

International Regulations

United Nations

The strategic lines of the fight against financing international terrorism, in the guiding principles, have been defined by the UN in 1999 in the New York Convention, with which for the first time the distinctive importance of the subject was recognised; in drawing up the Convention, the bases were established for the penal repression of the phenomenon, and for the extension to the same of the preexisting system of units for overseeing and contrasting of money laundering.

In the same year the UN Security Council **Resolution n. 1267/1999** introduced as an added measure, specific to the fight against terrorism, a procedure for “freezing” the funds and economic resources held by people linked to the Al-Qaeda terrorist network, according to a black-list managed by a specific committee (Sanctions Committee); later the 1373/2001 Resolution widened the scope of the freezing lists system, extending it to further lists, managed directly by the member States, of people suspected of belonging to or supporting terrorist organisations.

The UN adopted two new resolutions against Al-Qaeda (**1989/2011 Resolution**) and the Talibans (**1988/2011 Resolution**), formerly governed by a single Security Council Resolution (1267/1999). Procedural guarantees protecting people listed were reinforced, increasing the transparency of the procedures of listing and delisting, and the role of the Ombudsperson was reinforced whose remit includes the evaluation of requests for delisting.

The UN Resolution 2178/2014 of the 24th September, S/RES/2178 (2014), Threats to peace and international security caused by terrorist acts, resolution against Daesh, obliges the States to adopt a series of measures to face up to foreign terrorist fighters and requires the signatories to “prevent and suppress the recruitment, organisation, transport and equipping” of foreign fighters, in order to dismantle the organisation of Daesh.

Community Regulations

The UN Security Council Resolutions have been adopted by the European Union with two distinct Council measures: the [CE n.337/2000 Regulation](#) (later abrogated by the [CE n.467/2001 Regulation](#), in turn substituted by the [CE n.881/2002 Regulation](#)) issued to enact the 1267/1999 Resolution, for the names designated by the UN Sanctions Committee; the [CE n.2580/2001 Regulation](#), issued to enact the 1373/2001 Resolution, for further designated names within the jurisdiction of the European Union, proposed by the relevant authorities of the various countries.

In the following years, freezing measures analogous to those envisaged for terrorists have been applied by the European Union, following input from the UN, to sanction the governments of countries accused of serious violation of Human rights, or of threatening international peace and security; this latter case includes countries involved in proliferation of weapons of mass destruction, at the heart of a wider packet of restrictive measures (see the section dedicated to opposing proliferation programmes).

- EU Regulation n.2015/847 concerning informational data included in fund transfers, to the end of guaranteeing uniform application of the international regulations in the fight against money laundering and financing terrorism (in abrogation of (CE) n. 1781/2006).
- EU directive N° 2015/849, dated 20 May 2015, by the European Parliament and Council, establishes common regulations to prevent the use of the Union’s financial system for money laundering or financing terrorism. Besides this preventive measure, financing terrorism should be punishable in the member States. Not only financing of terrorist acts should be classified as crime, but also financing terrorist groups as well as other crimes connected to terrorist activities, such as recruitment and training, or travel for terrorist purposes. Such measures could contribute to the dismantling of support structures that facilitate commission of terrorist crimes.
- EU Directive 5 July 2016, COM(2016)/450 Final – which modifies the (EU) directive 2015/849 concerning the prevention of use of the Union’s financial system for money laundering or financing terrorism. The aim of the directive is to reinforce the fight against money laundering and financing terrorism.

- EU Directive 15 March 2017 n. 2017/541/UE - GUUE 31 March 2017, n. L 88, on the prevention and repression of international terrorism. The objectives are drawn up on the subject of the fight against terrorism for the member states. Member States must commit to introducing specific crimes in the fight against terrorism.

GAFI Recommendations

In the course of the plenary session held a few days after the 11 September attacks on New York (29 and 30 October), GAFI widened its mandate on contrasting the financing of terrorism, developing the regulations and guiding principles to fulfil the UN resolutions. On that occasion it released 8 [Special Recommendations](#) (9 from 2004) specifically concerning financing of terrorism.

The Special Recommendations, as well as supplying guidelines for implementing the UN Resolutions, have defined a few regulatory standards to better safeguard on a regulatory level those sectors considered to be most exposed to the risk of financing terrorism (money transfer services, cross border credit transfers, cash transfers, non profit Organisations operations).

The Special Recommendations were merged in February 2012 in the new [40 Recommendations](#) which include in their field of application the prevention and opposition to money laundering, to financing terrorism and to financing proliferation programmes of mass destruction weapons.

National Regulations

The strategies for opposing terrorism, defined in the competent international seats (UNO, European Union, GAFI) have been incorporated in our legal system with the laws n. 438/2001 and 431/2001, which have respectively introduced the particular penal case of association to the ends of international terrorism (clause 270 bis of the penal code), and given regulatory instructions for enacting the freezing measures. On that occasion the [Financial Security Committee](#) was established in our judicial system within the Ministry for the Economy and Finance. The Committee's remit used to consist in the coordination between the authorities and the police forces designated with acting against terrorism, and in overseeing the activities relating to the application of international sanctions, including the management of the designation proposals to the relevant international organisations. At a later stage the duties of the Committee have been widened to include money laundering.

Within such a regulatory set up, the duties of the UIC, and later of the Financial Information Unit for Italy, have been extended to cover financing of terrorism; in particular the UIF deals with the collection of financial information and data of the designated persons, facilitates the circulation of the relative lists from its own internet site, receives and analyses the warnings of suspicious transactions.

The national regulations concerning the financing of terrorism have been brought together in the legislative decree n. 109 of 22 June 2007, with "measures to prevent, contrast and curb financing of terrorism and the activities of countries that threaten international peace and security", released to enact the directive 2005/60/CE.

The legislative decree 109/2007, charged to the recipients of the money laundering prevention regulations, in the light of the dual opposing activities provides for compliance of various nature, centred on freezing measures (communication obligation) and the flagging of suspicious transactions (flagging obligation).

In particular, related to the communication obligation, the legislative decree 109/2007 (art. 7 clause 1) requires the obliged subjects to communicate within 30 days to the UIF:

- the freezing measures imposed on the persons designated in the EU lists or in the ministerial decrees as per art. 4 of the legislative decree 109/2007, specifying the named persons, the sum- total and the nature of the funds or economic resources involved;
- the transactions, the connections and all other available information on the persons designated in the lists, as well as on the persons who are being designated on the basis of information supplied by the UIF, following indications from the Financial Security Committee.

These are two distinct types of communication in play for keeping the authorities informed, on the one hand about the freezing measures applied, on the other about the transactions, connections and all other financial information known about the persons designated in the lists of those being designated.

The flagging obligations in art. 8 clause 1 of the legislative decree 109/2007 have been brought under art. 41 clause 1 of the legislative decree 231/2007, following the extension of the prevention and opposition to money laundering to the phenomenon of financing terrorism in all areas of application (adequate verification of the clientele, signalling of suspicious transactions, conservation of documents, internal controls, evaluation and management of risk).

The requirements and the methods of transmitting the warnings are the same as those for money laundering; further information on the correct performance of the warning obligations are to be found in the section **Operators' Compliance**, in the paragraph **Flagging of suspicious transactions**.

The indicators of anomalies, issued by the Bank of Italy and other authorities proposed by UIF, play a fundamental role in identifying suspect transactions to be flagged; these also include certain specific indicators concerning the financing of terrorism. The specific indicators pay particular attention to the subjective profile (lists), the location of the beneficiaries, and non profit. More details on how to meet the warning obligations are available, for each type of compliance, in the relevant sections of the site.

The duties of the UIF in contrasting the financing of terrorism go beyond receiving communications of freezing, and receiving and analysing the warnings of suspicious transactions. Article 10 of the legislative decree 109/2007, while extending the responsibilities of the UIF for prevention of the use of the financial system for money laundering to opposition to the financing of terrorism, identifies the following additional UIF duties:

- favoring in the circulation of the lists of designated persons and subsequent modifications;
- seeing to monitoring of the carrying out of the financial sanctions adopted against the activity of countries that threaten international peace and security;
- dealing with the collection of financial information and data concerning the designated persons, and the funds and economic resources subjected to freezing;

Regulatory references

Decreto Legge 18 febbraio 2015 n.7 (Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale), <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1980-02-06;15!vig=>

Risoluzione ONU n. 2178/2014 del 24 settembre 2014,
[http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2178%20\(2014\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2178%20(2014))

Decreto Legge 27 luglio 2005 n.144 ('pacchetto antiterrorismo'),

<http://www.normattiva.it/urires/N2Ls?urn:nir:stato:decreto.legge:2005-07-27;144!vig=>

Decreto Legge 6 settembre 2011 n. 159 (Codice delle leggi antimafia e delle misure di prevenzione),
<http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2011-09-06;159!vig=>

Legge 15 dicembre 2001 n. 438, <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2001-12-15;438!vig=>

Decreto del Presidente della Repubblica 22 settembre 1988 n. 447,
<http://www.normattiva.it/urires/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447!vig=>

Legge 15 dicembre 1979 n. 625, <http://www.normattiva.it/urires/N2Ls?urn:nir:stato:decreto.legge:1979-12-15;625!vig=>