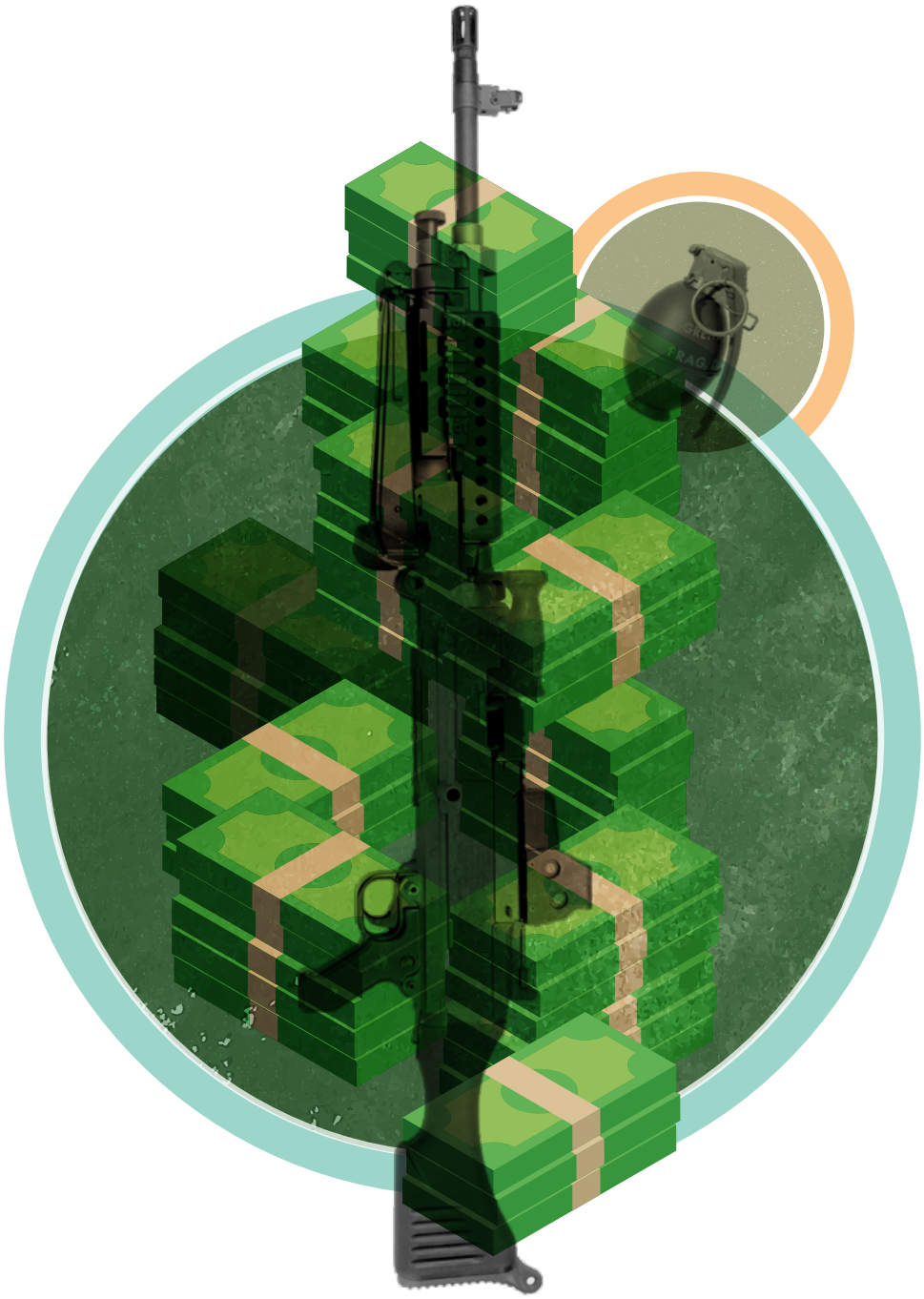
UNODC
United Nations Office on Drugs and Crime

Guidance manual for Member States on terrorist financing risk assessments



UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

Guidance manual for Member States on terrorist financing risk assessments

UNITED NATIONS
Vienna, 2018

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitations of its frontiers or boundaries.

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Contents

Acknowledgements

The present guidance manual has been made possible by the cooperative efforts and invaluable contributions of numerous individuals and Governments.

The United Nations Office on Drugs and Crime (UNODC) wishes to extend its gratitude to the Member States and international and regional organizations that contributed to the consultation process.

UNODC is grateful to the participants of the expert group meeting on the identification of good practices in assessing terrorist financing risk assessments, held in Vienna on 4 and 5 of April 2017, who have provided valuable input and contributions for this manual. The following experts attended the meeting: Alistair Sands, Philippe de Koster, Marc Penna, Mario Janeček, Dominic Steinrode, Giuseppina Pellicanò, Giovanna Perri, Thomas Muli Kathuli, Tarek Zahran, Ennasr El Hassane, Anne Mette Wadman, Kirill Korelin, Revza Erdogan Aydoyan, Moza Mohamed Alzamar, Abdulaziz Alnuaim, Emmanuel Saliot, Giancarlo Vucchi, Delphine Schantz, Shana Krishnan, Kevin Stephenson, Muazu Umari, Paul Riordan, Tom Keatinge, Iris Pilika, Irina Donciu and Kuntay Celik.

The following staff members of UNODC contributed to the project: Mauro Miedico, Loide Lungameni, Elena Rigacci Hay, Oliver Gadney, David Alamos, Antonio Giovanni Luzzi, Rima Al-Kaissi, Melissa Tullis, Yevheniy Umanets, Oleksiy Feshchenko, Hannah Baumgaertner.

The following staff members of UNODC assisted in the production of the present guidance manual: Mauro Miedico, Acting Chief of the Terrorism Prevention Branch, Division for Treaty Affairs; Elena Rigacci Hay, Chief A.I. of Implementation Support Section III, Terrorism Prevention Branch; Antonio Giovanni Luzzi, Programme Officer, Implementation Support Section III, Terrorism Prevention Branch; and Oliver Gadney, Programme Manager, Global Programme on Money-Laundering and the Financing of Terrorism.

UNODC would like to thank the following Member States and organizations for their comments and contributions to the drafting of the present guidance manual: the Counter-Terrorism Committee Executive Directorate; the European Commission; the Ministry of Economy and Finance of Italy; the Australian Transaction Reports and Analysis Centre, the financial intelligence unit of Australia; the Financial Intelligence and Enforcement Department of the Central Bank of Malaysia; the Financial Crimes Investigation Board, the financial intelligence unit of Turkey; Financial Intelligence Processing Unit, the financial intelligence unit of Morocco; the Ministry of Security of Bosnia and Herzegovina; the Special Investigation Commission of Lebanon; the Financial Intelligence Processing Unit of Belgium, the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015), concerning Islamic State in Iraq and the Levant (Da'esh), and the Financial Action Task Force.

List of abbreviations and acronyms

APG	Asia/Pacific Group on Money Laundering
Europol	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
IMF	International Monetary Fund
INTERPOL	International Criminal Police Organization
ISIL	Islamic State of Iraq and the Levant
NGO	non-governmental organization
UNODC	United Nations Office on Drugs and Crime

Introduction

To successfully prevent terrorism, terrorist financing needs to be countered in an efficient manner, as this is a key phenomenon that allows terrorist groups to thrive. Terrorists are continuously increasing and evolving their ability to diversify and renew not only the source of their funds, but also the channels and instruments they use to transfer those funds. It is therefore essential to have efficient coordination and cooperation among financial intelligence units, law enforcement entities and intelligence services, and to ensure strong political commitment on all levels.

Given its transnational nature, terrorist financing needs to be analysed and assessed not only from a national perspective but also from a sectoral, regional, supranational and even global perspective. Financial assets continue to adapt to the globalized nature of the economy and of financial systems, and regional, supranational and global risk assessments are needed.

Furthermore, as the terrorist threat directly impacts on security, an international approach to countering terrorism and terrorist financing has become increasingly important. The international community has placed the issue at the core of its agenda since the adoption of the International Convention for the Suppression of the Financing of Terrorism and Security Council resolution 1373 (2001). Of particular importance is the need to criminalize terrorism and introduce disruptive measures (such as the freezing of terrorist assets).

The United Nations Security Council has subsequently approved a series of key resolutions on the criminalization of the financial support to terrorist organizations, including Al-Qaida and ISIL): resolution 2178 (2014), on the financing of the travel of foreign terrorist fighters; resolution 2199 (2015), on the criminalization of any direct or indirect trade involving ISIL; and resolutions 2368 (2017) and 2396 (2017). The Security Council also established the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning ISIL (Da'esh), Al-Qaida, and associated individuals, groups, undertakings and entities.

The above-mentioned resolutions, approved under Chapter VII of the United Nations Charter, created an obligation for Member States to implement appropriate measures, but most of all highlighted their need to identify and assess the risks of terrorist financing within their economies.

It is essential that Member States apply a risk-based approach in order to ensure that the measures implemented to prevent or mitigate terrorist financing activities are commensurate with the risks identified and are effective in mitigating those risks.

To succeed, countries need to identify, assess and understand the risks and then take action, allocating adequate resources across their framework for countering the financing of terrorism and ensuring that the risks are mitigated effectively. The results of a risk assessment can also provide useful information to the financial sector, and designated non-financial businesses and professions, to support them in conducting their own risk assessments.

Risk assessments are very complex processes that require the preliminary definition of the pursued objectives and scope in which to conduct the analysis, as well as the definition of specific procedures, which must be agreed by all the relevant authorities involved. As a result, a unique model to assess terrorist financing risks does not suit all countries or territories. It is therefore important to take into account the specific features of a country, region or supranational territory when choosing a methodology. Furthermore, regardless of which methodology is chosen, a variety of sources should be used in the collection of information.

In view of this daunting task, competent authorities who work at the supranational and national levels often need guidance in preparing terrorist financing risk assessments, because they face several challenges in obtaining information that is adequate, accurate and up to date.

To support Member States in that endeavour, UNODC organized an expert group meeting on the identification of good practices in terrorist financing risk assessments, which was held in Vienna on 4 and 5 April 2017.

The initiative was led by the Terrorism Prevention Branch of UNODC and the Global Programme against Money-Laundering, Proceeds of Crime and the Financing of Terrorism, with the support of the Counter-Terrorism Committee Executive Directorate, and with the participation of representatives from law enforcement agencies, financial intelligence units and other relevant agencies from more than 20 Member States, as well as independent and international experts from international organizations and other designated entities. Member States and organizations with experience in the development and facilitation of such assessments provided a range of good practices; however, although many of those practices could be commonly followed, they needed to be adapted to the specific national, regional or supranational realities.

The participants in the expert group meeting decided to work together to develop a document containing good practice methodologies intended for Member States, regional entities and supranational territories for use in the development of terrorist financing risk assessments.

A questionnaire aimed at identifying good practices on terrorist financing risk assessments was distributed to all participants, and the responses provided were used to draft the present document. In addition, the present document is built upon important existing resources on terrorist financing risk assessments, including the following:

- FATF guidance document entitled "National Money-Laundering and Terrorist Financing Risk Assessment" (February 2013)
- World Bank national risk assessment tool (June 2015)
- Methodology for assessing money-laundering and terrorist financing risks that affect the internal market and related cross-border activities, an initiative of the European Union based on article 6, paragraph 5, of directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing (often referred to as "the fourth AML/CFT directive")
- IMF national risk assessment methodology on anti-money-laundering and countering the financing of terrorism (2013)

Furthermore, the experience of existing terrorist financing risk assessments was used, including the following:

- *Regional Risk Assessment 2016 – Terrorism Financing, South-East Asia and Australia*
- European Union supranational terrorist financing risk assessment (2017)
- United States of America *National Terrorist Financing Risk Assessment 2015*
- Existing terrorist financing risk assessments in the participating countries

For this project and for the development of the toolkit the workgroup also benefited from the valuable experience of the European Commission, who finalized its first supranational risk assessment for money-laundering and terrorist financing in June 2017.


ación Simulada
ción del Terrorismo
anizado por la Oficina de las Naciones Unidas Contra la Droga y el Delito
njunto con el Ministerio de Justicia y del Derecho de la República de Colombia
ección de Asuntos Antinarcóticos y Aplicación de la Ley (INL) de los Estados Unidos de Améri
MinJusticia

Chapter 1

Methodology

A terrorist financing risk assessment is a product or process based on a methodology, agreed by the parties involved, that attempts to identify, analyse and understand terrorist financing risks and serves as a first step in addressing them.

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

The purpose of the exercise is to attain sectoral, national, regional or supranational understanding of the following:

- Threats of terrorist financing (through the identification of the most relevant ones)
- Main methods used for carrying out such criminal activity
- Sectors most exposed to such risks and related criminal activity
- Vulnerabilities in the national, regional or supranational systems of prevention, investigation and prosecution of such phenomena, and the systems of control in those sectors that are at risk
- Actions to be initiated and their priorities

The analysis is aimed at identifying, analysing and assessing the main terrorist financing risks at different levels; examining the causes of those risks, and the vulnerabilities that allow such risks to arise; and the consequences of those risks.

Ideally, a risk assessment involves making judgments about threats, vulnerabilities and consequences.

Various factors and elements, both internal and external, including the general environment and circumstances in a country, can have an impact on the choice of a methodology and the implementation of an effective risk assessment.

This section considers a number of factors, including concepts; approaches; stages; methods of collecting data and assessing threats, vulnerabilities and risks; internal and external elements; and general situation in a country that could have an impact on the risk assessment.

Although the toolkit has been prepared with the aim of assisting in the assessment of terrorist financing risks, best practices from the experiences of Member States in assessing money-laundering risks have also been incorporated.

Finally, the practical examples included here are based on the experience of countries that took part in the expert group meeting.

1.1 National framework for coordination and cooperation in the countering of terrorist financing

The way in which a country organizes its national framework for coordination and cooperation in issues related to the countering of terrorist financing will have an impact on the implementation of a risk assessment.

Many countries employ a single and unique coordination mechanism or committee for the fight against money-laundering and terrorist financing. Owing to the high sensitivity and the specific features of terrorism and terrorist financing issues, however, other countries have two distinct coordination mechanisms.

In Belgium, the committee for the countering of the financing of terrorism was integrated into the national security committee, because issues related to terrorism and terrorist financing may be complementary and often involve the same persons.

The number of people invited to take part in the meeting of the committee, as well as the origin of those individuals, may also have an impact on the choice of coordination mechanism.

The committee for the countering of money-laundering could include partners and experts coming from the control authorities; civil servants from various government departments, not all involved in security issues; and individuals from the private sector. For that reason, this committee is often too large to ensure a safe and confidential exchange of sensitive information related to terrorism and terrorist financing.

Intelligence services are often not ready to share sensitive information with private sector representatives they do not trust. In addition, representatives of the intelligence community are sometimes reluctant to share information because it is considered sensitive or has been obtained from a foreign intelligence service.

The ability of those involved to handle highly sensitive and confidential information, which depends on partners involved in the risk assessment having the proper security clearances, may also have an impact on the choice of the type of coordination mechanism.

Partners belonging to the committee for the countering of money-laundering do not always have the right security clearances to access the highly confidential information required to correctly assess terrorist financing risks.

All of those issues must be taken into consideration when choosing the type of coordination mechanism. If not correctly anticipated, such factors could have an effect on the quality, comprehensiveness and effectiveness of the risk assessment and therefore on the effectiveness of the fight against terrorist financing.

Consequently, the choice of a specific model or coordination mechanism is a key consideration that will have an impact on the risk assessment.

The risk assessments could cover the money-laundering and terrorist financing risks together or countries may also decide to produce two separate risk assessments: one for money-laundering and another for terrorist financing. In countries with two coordination mechanisms, two specific risk assessments are usually issued.

Because of the sensitivity of issues related to terrorism and terrorist financing, lawmakers in Belgium decided to delegate the coordination of the fight against money-laundering to one coordinating body, and that against terrorist financing to a separate body, each composed of different stakeholders.

The terrorist financing risk assessment is a responsibility of the committee in charge of the coordination of the fight against terrorist financing.

The national coordination authority for money-laundering and the National Security Council

Belgium has one national coordination authority to assess the risks of money-laundering, and another authority to assess the risks of terrorist financing. Those two authorities establish policy and coordinate the fight against money-laundering and terrorist financing.

The national coordination authority for money-laundering consists of a ministerial committee, which coordinates the fight against money of illicit origin; the Board of Partners; the Judicial Platform; and a Joint Authority to coordinate the actions of the Board and the Judicial Platform.

The National Security Council deals with terrorism and security issues and, since 2013, also handles issues related to terrorist financing and the proliferation of weapons of mass destruction. The Strategic Intelligence and Security Committee and the Intelligence and Security Coordination Committee implement the decisions of the National Security Council. A specific terrorist financing platform was created within the Intelligence and Security Coordination Committee, in order to deal with terrorist financing issues.

The Board of Partners and a judicial platform prepare the national money-laundering risk assessment, and a terrorist financing platform prepares the national terrorist financing risk assessment.

The ministerial committee and the national security council decide the future national policies in the fight against money-laundering and terrorist financing, respectively, and they allocate the resources needed to implement such policies.

Source: Belgium

Italy opted for a similar mechanism. Italy has a strategic counter-terrorism committee, which is also responsible for handling issues related to countering terrorist financing, and which delegated the preparation of the terrorist financing risk assessment to a dedicated expert group.

Italy: Financial Security Committee

The Financial Security Committee is the national body involved in countering terrorist financing that is responsible for conducting and updating the national risk assessment.

The committee has been established as part of the Ministry of Economy and Finance of Italy and has been tasked with coordinating actions for the prevention of the use of the financial system and of the economy for purposes related to money-laundering and terrorist financing, and the financing of the proliferation of weapons of mass destruction.

The Financial Security Committee comprises key competent authorities. Its composition has been enhanced with additional representatives from participating authorities in relation to the specific subjects discussed.

The Committee established an ad hoc working group to develop a proposal for the method of analysis and to perform the assessment.

Italy: Financial Security Committee *(continued)*

The key competent authorities can share any information among themselves and are exempt from all applicable rules on official secrecy. All information acquired by the Committee is covered by official secrecy. The judicial authorities shall transmit to the Committee any information deemed useful for its purposes.

The Chair of the Committee may transmit data and information to the Executive Committee for Intelligence and Security Services and to the heads of the intelligence and security services for coordination activities to be carried out by the Prime Minister.

Source: Italy

Other countries have a single and unique coordination mechanism, even though they have several complementary arrangements in place to coordinate and cooperate on issues relating to money-laundering and terrorist financing.

In Australia, for example, a national committee coordinates the fight against money-laundering and against terrorist financing, with the assistance of competent authorities at the national or regional levels.

The Anti-Money Laundering Interdepartmental Committee of Australia

Australia has a wide range of arrangements in place for coordination and cooperation in countering money-laundering and the financing of terrorism at both the policy and operational levels.

The main federal coordinating body is the Anti-Money Laundering Interdepartmental Committee, which meets to share information and inform the strategic direction and priority setting of federal agencies working on domestic initiatives to counter money-laundering and the financing of terrorism.

Activities relating to countering money-laundering and the financing of terrorism are also coordinated through the National Organized Crime Response Plan and other interdepartmental forums that coordinate law enforcement policy.

Policy relating to countering the financing of terrorism is coordinated by the Interdepartmental Committee. Operational matters are coordinated through various investigative agencies focusing on the financing of terrorism. One of those is the National Counter Terrorist Committee, created after the 2001 terrorist attacks on the United States (see box).

The Interdepartmental Committee agrees and sets annual risk-based priorities to guide the work and resource allocation of its member agencies on matters regarding the countering of money-laundering and the financing of terrorism. Each agency must initiate changes to its resource allocation through its Minister and ultimately Parliament.

The Interdepartmental Committee uses the national threat assessment and national risk assessment to set annual risk-based priorities that guide the work and resource allocation of its member agencies on matters regarding the countering of money-laundering and the financing of terrorism.

Source: Australia

Nevertheless, although the country has a common coordination mechanism (for countering money-laundering and terrorist financing) at the federal level, the number of subcommittees could explain why the country eventually produces two separate risk assessments.

Coordination efforts could also be undertaken at broader regional and supranational levels.

The regional counter-terrorism committee established by Australia and New Zealand is such an example.

In 2012, New Zealand formally joined the National Counter Terrorist Committee of Australia. The Committee thus became a regional counter-terrorism committee and was renamed Australia-New Zealand Counter-Terrorism Committee.

The Australia-New Zealand Counter-Terrorism Committee

In September 2012, the Commonwealth, State and Territory governments entered into a formal agreement to establish New Zealand as a member of the renamed Australia-New Zealand Counter-Terrorism Committee. Previously New Zealand had only observer status on the National Counter-Terrorism Committee of Australia.

The Australia-New Zealand Counter-Terrorism Committee is a bilateral and intergovernmental high-level body or arrangement to coordinate counter-terrorism capabilities, to manage, command and control reactions to crisis events, to coordinate intelligence and investigation functions, composed of representatives from the national Government, and the federal state and territory governments of Australia and the Government of New Zealand.

The purpose of the change was to ensure the closest possible coordination and cooperation on counter-terrorism matters.

The Committee is based on strong cooperation between both countries and it has established capabilities in such areas as crisis management, command and control, intelligence and investigation and media cooperation.

The objectives of the Committee are to contribute to the security of Australia and New Zealand through:

- Maintaining the national counter-terrorism plan and associated documentation
- Providing expert strategic and policy advice to heads of Government and other relevant Ministers
- Coordinating an effective nation-wide counter-terrorism capability
- Maintaining effective arrangements for the sharing of relevant intelligence and information between all relevant agencies and jurisdictions
- Providing advice in relation to the administration of the special fund to maintain and develop the nationwide capability, administered by the Government of Australia on the basis of advice from the Australia-New Zealand Counter-Terrorism Committee

Source: Australia

The European Union has no such coordination mechanism, except that the European Commission mandate includes the coordination of the fight against money-laundering and the financing of terrorism and the European Commission has been mandated by directive (EU) 2015/849 to prepare the supranational money-laundering and terrorist financing risk assessment.

Many working groups also coordinate the Member States' responses to the risks of money-laundering and terrorist financing: the Expert Group on Money-Laundering and Terrorism Financing and the European Union financial intelligence unit platform are some examples of coordination mechanisms in place.

1.2 Approaches

The risks related to the financing of terrorism could be slightly different from the risks associated with money-laundering. At the same time, the risk indicators for assessing the terrorist financing risks may be different from the risk indicators used for money-laundering risks assessments.

In money-laundering schemes, the funds come from illegal activities and are injected into the legal economy using numerous techniques and vulnerable sectors of the economy. In relation to terrorism, the funding may be derived from criminal activities and origins, but also from perfectly legal activities or origins. The main concern is to identify those sources so as to eradicate them.

The identification of suspicious financial transactions has led to the identification of vulnerable sectors used to launder the proceeds of criminal activities.

The identification of the terrorist financing sources has led to the identification of sectors, organizations, and even public and State authorities, which could, sometimes inadvertently, be misused to obtain funds to finance terrorist activities. Those sectors, organizations and public and State authorities may present vulnerabilities that could explain their misuse to finance terrorism.

With regard to terrorist financing, the range of activities whose vulnerabilities need to be assessed is larger. Experience has shown that not only private sector actors, but also the public sector may be involved in the financing of terrorism, even if most of the time they are involved unwittingly or their involvement results from organizational vulnerabilities.

The financing of terrorism, lone actors or foreign terrorist fighters using social benefits results from organizational deficiencies and vulnerabilities in the State administration granting the allowances and from the lack of effective safeguards to detect such inappropriate use of social benefits.

Although many countries start their money-laundering risk assessments from sectors potentially subject to money-laundering activities, many countries also use the sources of terrorist financing as the starting point of their terrorist financing risk assessment.

Countries also examine the techniques used by the financiers of terrorism.

The approach of Belgium to terrorist financing threats and vulnerabilities

The national financing of terrorism risk assessment focused on the sources of funding. Belgium divided the sources of funding into two categories: microfinancing and macrofinancing of terrorism. The researchers also investigated the techniques used to finance terrorism. The assessment was a two-stage process. The first stage was a threat assessment in which open source data were collected on the sources funding terrorism.

After collecting the data, the partners started a verification process for which they were asked to assess and rate the likelihood of the presence in Belgium of the sources of funding (highly exposed to terrorist financing, reasonably exposed to terrorist financing, little exposed to terrorist financing, not verifiable). The same approach was applied to the vulnerabilities assessment. Using the knowledge and experience about potential vulnerabilities, the partners were asked to assess the likelihood of potential vulnerabilities to the financing of terrorism.

On the other hand, the national money-laundering risk assessment focussed on specific sectors. Belgium examined the various sectors sensitive to money-laundering. The assessment was conducted in two stages: an assessment of money-laundering threats and an assessment of money-laundering vulnerabilities. The results of these two assessments helped Belgium to draw conclusions on the level of risk associated with each of the sectors assessed. The money-laundering risk assessment assessed the threats in 32 sectors with 32 indicators and quantitative data from the financial intelligence processing unit of Belgium, the police, customs and the Ministry of Economic Affairs. For the money-laundering vulnerabilities assessment, the study divided the 32 sectors into distinct groups and a questionnaire was sent to the competent authorities to collect qualitative data. For each sector, the questionnaire was used to analyse the organization, supervision, business structure, product or service, distribution channels and the geographical distribution of the distribution channels.

Source: Belgium

Differentiating both assessments is reasonable and acceptable if we understand the links between them.

Common deficiencies in efforts to counter the financing of terrorism could affect or have an impact on the fight against money-laundering as well as terrorist financing. The vulnerability assessment results may be the same both for money-laundering and terrorist financing.

Elements from the money-laundering risk assessment could be useful to the terrorist financing risk assessment.

If, during the terrorist financing risk assessment, a specific sector is identified as representing a high level of threat (e.g. night shops because they handle large amounts of cash), the information obtained during the money-laundering vulnerability assessment (if this sector is also used for money-laundering purposes and the money-laundering risk assessment studied the vulnerabilities in this sector) may be important to decide on the mitigating measures to be taken.

The risk analysis has to take into account additional risk analyses, conducted at the sectoral, regional or supranational level.

The private sector could also be involved in risk analysis development. In particular, trade associations and private institutions are invited to share their experiences in the area and their assessments of specific topics identified over time.

1.3 Perspectives

The risks could be assessed from different perspectives: sectoral, national, regional (the risk assessment covers a particular specific region) or supranational (covering a group of countries belonging to an union such as the European Union, which produced a supranational risk assessment in June 2017),

as well as international (a worldwide risk assessment like the one produced in July 2010 by FATF: The Global Money-Laundering and Terrorist Financing Threat Assessment), even though the FATF obligation of assessing and understanding money-laundering and the financing of terrorism refers to the country itself (national money-laundering and terrorist financing risk assessment).

All these assessments should normally influence each other or complement to each other (in both ways). A national terrorist financing risk assessment can consist of elements from sectoral assessments (assessments by the financial institutions and designated non-financial business and professions or their professional organization or supervisory authorities), thematic risk assessments or from risk-based assessments on the type of customers or the type of products marketed by the financial institutions. The combination of various kinds of factors will contribute to the whole picture.

A regional or supranational risk assessment could be set up by pooling several country-specific terrorist financing risk assessments or could be conducted autonomously.

The choice between pooling several specific assessments and an autonomous terrorist financing risk assessment depends on the circumstances and characteristics of the countries that are part of the region or the wider territory under assessment.

An assessment of the threats and vulnerabilities in the non-profit sector could also improve the understanding of the terrorist financing risks in a given country.

Global Money-Laundering and Terrorist Financing Threat Assessment

The *FATF Report: Global Money-Laundering and Terrorist Financing Threat Assessment, A View of How and Why Criminals and Terrorists Abuse Finances, the Effect of This Abuse and the Steps to Mitigate These Threats* is a global threat assessment of money-laundering and terrorist financing.

The Report is aimed at getting a better understanding of these threats and their negative impact, and help Governments to take decisive action to minimize the harm they can cause.

The Report is based on various typological studies carried out by the FATF, the FATF-style regional bodies and their member States as well as the FATF Strategic Surveillance Initiative.

This initiative to publish the Report was launched in 2008 and was meant to:

- Detect and share information on the types of criminal or terrorist activities that pose an emerging threat to the financial system;
- Develop a more strategic and longer-term view of those threats.

The aim of the Report was to tackle the techniques used for money-laundering and terrorist financing based on five themes:

- Abuse of cash and bearer negotiable instruments
- Abuse of transfers of value other than cash and bearer negotiable instruments
- Abuse of valuable goods
- Abuse of persons who can carry out money-laundering or terrorist financing transactions because of their financial expertise (non-financial professions) or persons (politically exposed persons) who can influence the applicable laws and regulations
- Criminals and terrorism financers who abuse jurisdictions with a weaker and inadequate system to counter money-laundering and the financing of terrorism.

The Report explains why criminals and terrorist financers conduct their activities utilizing these techniques to launder money and finance terrorism and considers what factors can make money-laundering and the financing of terrorism successful.

The Report also examines the influence and the negative impact of successful money-laundering and terrorist financing transactions on the international financial system and individuals, non-profit organizations, local and national communities and the international community.

The Report does not quantify the threats posed by money-laundering and the financing of terrorism, but recognizes the components of money-laundering and the financing of terrorism, the harm caused and the need for global action.

Regional risk assessments

Both regionally and globally, criminals and criminal organizations launder assets and the proceeds of their criminal activities.

The region may be exposed to a number of threats or potential factors, including vulnerabilities, which could affect countries' financial systems.

A regional risk (threats and vulnerabilities) may be understood as a risk that affects, to a greater or lesser degree, all member States of the region or of the same geographical region or subregion.

A regional risk assessment could develop in two different ways.

The risk assessment could be the result of an autonomous and completely new exercise or risk assessment or the regional risk assessment could be built on the results of the individual countries' national risk assessment or a mix of both models.

Until now, only a few regional terrorist financing risk assessments have been produced in the world. Only one region produced a full terrorist financing risk assessment (South-East Asia and Australia).

Regional risk assessment on terrorist financing 2016 in South-East Asia and Australia

In 2016, Australia, Indonesia, Malaysia, Philippines, Singapore and Thailand took part in and contributed to a regional risk assessment on terrorist financing, co-led by the Australian Transaction Reports and Analysis Centre, the financial intelligence agency of Australia, and its counterpart in Indonesia, the Financial Transaction Reports and Analysis Centre.

The assessment, published under the title *Regional Risk Assessment 2016 – Terrorism Financing, South-East Asia and Australia*, identified and assessed the major terrorist financing risks in South-East Asia and Australia. Its aim was to do the following across the region: *(a)* identify the main global drivers that drive terrorist actors, cells and groups; *(b)* analyse distinctive factors that shape regional terrorist financing behaviour and vulnerabilities; *(c)* identify key capabilities and challenges in countering terrorist financing; *(d)* highlight key methods for raising and moving terrorist funds into, across and out of the region; *(e)* recognize the use and consequences of terrorist financing; *(f)* consider potential change factors that may impact the terrorist financing landscape in the future; *(g)* point to priorities to strengthen the region's capacity to detect and combat terrorist financing more effectively.

This assessment rates the overall risk of terrorist financing across the region as a whole, taking into account country-specific contexts. Assessments are based on open-source information and intelligence provided by regional financial intelligence units and other national authorities, with validation from a range of experts.

The overall threat rating was informed by suspicious transaction reports and other intelligence holdings, the number of investigations, prosecutions and convictions, links of non-profit organizations to terrorist groups, the level of sophistication of financial typologies, and qualitative data. Vulnerability ratings were informed by key partner and stakeholder engagement, sector assessments and reviews,

and other open source reports (e.g. FATF/APG mutual evaluation and typology reports, and academic work). For the regional risk assessment and current regional assessment of non-profit organizations, the financial intelligence units of Australia and Indonesia also used national risk assessments or sector assessments where available.

The regional risk assessment also explored the links between terrorism and local crime groups and with transnational organized crime.

The European Union supranational money-laundering and terrorist financing risk assessments

The first supranational risk assessment report was drawn up by the European Commission in 2017 and covers both money-laundering and terrorist financing risks. It is contained in the document entitled "Report from the Commission to the European Parliament and the Council on the assessment of the risks of money-laundering and terrorist financing affecting the internal market and relating to cross-border activities".[1]

In the context of the European Union internal market, financial flows are integrated and cross-border by nature, and money can flow swiftly, if not instantly, from one member State to another, allowing criminals and terrorists to move funds across countries avoiding detection by authorities.

To address these cross-border risks, the European Parliament and the Council of the European Union, in directive (EU) 2015/849, have defined common rules on the prevention of and controls over money-laundering and the financing of terrorism, established common reporting obligations by financial institutions and other economic actors and created a robust framework for financial intelligence units in the European Union to analyse suspicious transactions and cooperate.

However, additional measures to close any potential gaps or monitor any new upcoming, evolving and changing terrorist financing risks could always be needed to effectively combat money-laundering and terrorist financing and the directive consequently instructs the European Commission to organize a risk assessment at the supranational level.

In line with FATF considerations that a risk-based approach could be organized at supranational level, the directive provides for such assessment at the European level.

Article 6 of the directive requires the Commission to conduct an assessment of the risks of money-laundering and terrorist financing affecting the internal market and relating to cross-border activities. The report is to be updated every two years.

It is worth noting that the first European Union supranational risk assessment was based on directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money-laundering and terrorist financing (often referred to as the "third AML/CFT directive"), in force at the time of the analysis. The conclusions and proposed mitigating measures take into account directive (EU) 2015/849.

Directive (EU) 2015/849 describes how the Commission has to conduct the supranational risk assessment and specifies that:

(a) The assessment should cover the risks of money-laundering and terrorist financing affecting the internal market of the European Union and relating to cross-border activities. It should include the areas of the internal market that are at greatest risk, the risks associated with each relevant sector and the most widespread means used by criminals by which to launder illicit proceeds;

[1] European Commission, COM(2917) 340 final.

(b) The input the Commission should consider when conducting the assessment should include that of the Joint Committee of the European Supervisory Authorities affecting the financial sector of the European Union, the expertise of representatives of member States responsible for anti-money-laundering and countering the financing of terrorism, and input from the financial intelligence units and other relevant bodies at the level of the European Union.

(c) The Commission's risk assessment should take the form of a report identifying, analysing and evaluating the risks of money-laundering and terrorist financing. In addition, the Commission should make recommendations to member States on the measures suitable for addressing the identified risks. Member States should follow these recommendations on a "comply or explain" basis.

(d) The Commission's report should be made available to member States and obliged entities to help them to identify, understand, manage and mitigate the risks of money-laundering and terrorist financing. Every two years, the report should be revised on the basis of the findings of the regular risk assessments and the actions taken based on those findings.

The directive requires the Commission to make a report on money-laundering and terrorist financing risks as well as recommendations to Member States on the measures suitable for addressing the risks identified.

The action plan for strengthening the fight against terrorist financing also requires such an assessment.

The European Union terrorist financing risk assessment must ensure in particular that the regime to counter the financing of terrorism adequately addresses higher-risk situations.

To reach this goal, it is first necessary to identify and analyse those risks and monitor how they evolve and/or change. Specific focus can then been put on situations representing a higher risk of money-laundering and terrorist financing.

The directive recognizes that the protection of the financial system by means of prevention, detection and investigation of specific cross-border money-laundering and terrorist financing threats that may affect the internal market cannot be sufficiently achieved by individual member States, as measures adopted by member States individually to protect their financial systems could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and European Union public policy.

It has been recognized that there is a need for the European Union to identify, understand and seek to mitigate risks of money-laundering and terrorist financing, which are relevant from an European Union perspective and could not be addressed effectively by individual member States. For this reason, some actions or measures can be better achieved at the European Union level.

Nevertheless, the supranational risk assessment is meant to complement member States' approach and to support member States in their own processes.

The legal framework in place is one of the key criteria to assess the level of risks. When assessing a risk, it is important to acknowledge whether the existing legal framework is commensurate to the risk inherent to a specific sector, or whether it only marginally covers the risk.

The assessment of risks affecting the European Union was carried out at a time when the legal basis was directive 2005/60/EC. Even though directive (EU) 2015/849 was adopted in May 2015, its transposition into the national legislations of the member States has not been completed yet.

In addition, in the aftermath of several terrorist attacks and the revelations relating to the so-called Panama papers, the Commission adopted a new legislative proposal to revise, through a targeted approach, the legal framework on the countering of money-laundering and the financing of terrorism.

In that legislative proposal, new mitigating measures are being proposed, but those could not be taken into consideration, as the text is still under negotiation and has not yet entered into force.

Therefore, the supranational risk assessment is based on the European Union legislation in force at the time of the assessment. This point is particularly important to stress, since some sectors were not covered by the requirements of directive 2005/60/EC, or to a limited extent only.

The Commission developed a methodology for carrying out its supranational risk assessment in line with international standards and guidance issued by FATF.

The Commission designed a tailor-made methodology for the purpose of the European Union supranational risk assessment. This methodology is based on FATF guidance on risk assessment.

The European Union supranational risk assessment uses a defined methodology to provide a systematic analysis of the terrorist financing risks linked to the modi operandi of perpetrators when financing terrorism. The methodology provided a common understanding for assessing the risks.

1.4 Key concepts

A risk assessment consists of identifying and analysing the risks of money-laundering and terrorist financing and in developing a risk-based approach to countering money-laundering and the financing of terrorism.

As stated above, ideally, a risk assessment involves making judgments about threats, vulnerabilities and consequences.

Following existing guidance for countries to help them to assess money-laundering and terrorist financing risks, the following key concepts can be defined:

A **risk** is a function of three factors: threat, vulnerability and consequence.

A **threat** is a person or group of people, object or activity presenting the potential to cause harm to the State, the society, the economy, etc. In the context of money-laundering and the financing of terrorism, this includes criminals, terrorists, terrorist groups and their facilitators, their funds, as well as past, present and future activities linked to money-laundering and the financing of terrorism that could cause harm to a State, society, the integrity of the financial system and the economy.

A **vulnerability** is something that can be exploited by the threat or that may support or facilitate the activities related to the threat. This part of the assessment focuses on the factors that represent weaknesses in systems to counter money-laundering and the financing of terrorism, or control certain features of a country, a particular sector, a financial product or type of service that make them attractive for purposes of money-laundering and the financing of terrorism. When criminals exploit vulnerabilities or weaknesses, they allow the threats to be translated into activities relating to money-laundering and the financing of terrorism.

Vulnerabilities can be assessed with respect to various aspects, such as sectors, products marketed, specific business relations, distribution channels, geographical distribution.

The risk of an event or activity relating to money-laundering or the financing of terrorism occurring depends on the likelihood the event or activity will occur and the consequences of the event or activity.

The **likelihood** depends on the existence of a threat and a vulnerability, vulnerability allowing the threat to develop its effects, and on the consequence the development of this event will have.

The likelihood is a function of the presence of threats that can produce a phenomenon of money-laundering or the financing of terrorism and the vulnerabilities of the systems and mechanisms used to mitigate such threats.

The concepts used by Turkey

In developing a methodology for the terrorist financing risk assessment, Turkey has taken into account models developed by other bodies including the World Bank and IMF, the FATF guidance on risk assessments, approaches adopted by other countries and opinions expressed by stakeholders involved in Turkish regime relating to money-laundering and the financing of terrorism.

The terminology or concepts and methodology mainly reflect the FATF guidance on risk assessments.

Risk: Turkey regards risk as a function of three factors: threat, vulnerability and consequence.

Threat: A threat is a person or group of people, or activity with the potential to cause harm to the State, society, the economy, etc. In the terrorist financing context this includes terrorist groups and their facilitators, as well as radicalized individuals that seek to exploit Turkey and its financial system to raise and move funds.

Vulnerability: Vulnerability is something that can be exploited to facilitate terrorist financing, both in the raising of funds for terrorist networks and the moving of funds to terrorist organizations. It may relate to a specific fund raising method or financial product used to move funds, or a weakness in regulation, supervision, or enforcement, or reflect unique circumstances in which it may be difficult to distinguish legal from illegal activity.

Source: Turkey

The regional risk assessment on terrorist financing 2016 for South-East Asia and Australia employs the standard risk framework (likelihood x consequence = risk) and FATF guidance on national money-laundering and terrorist financing risk assessments as a general guide. Estimates of likelihood are based on a combined assessment of the threat to, and vulnerability of, a channel to terrorist financing activity.

Concept	Definition
Risk	Risk is based on the assessment of three factors: threat, vulnerability and consequence.
Threat	A threat is a person or group of people, object or activity with the potential to cause harm — for example, to the state, society, economy, regional and global security, etc. In the terrorism financing context 'threat' includes criminals, terrorist groups and their financiers, associates and facilitators, including how they may seek to exploit funding sources and means of transferring and storing funds. Threat typically serves as the starting point in developing an understanding of terrorism financing risk. For this reason, an understanding of the general terrorism environment and how it influences terrorism financing activity is important.

(continued)

Concept	Definition
Vulnerabilities	Vulnerabilities are things that threats can exploit or that may support or enable a threat to exist. In the terrorism financing environment, vulnerabilities are characteristics of a CTF framework, or a financial or other type of system, that affect its propensity to be exploited by threats. These include, for example, political stability, the broader regulatory environment, relative size of formal and informal (cash) economies, neighbouring political and security environment, and international financial flows. Vulnerabiities may also include the characteristics of a particular sector, a financial product, type of service or channel to foreign regions or countries that make them attractive for terrorism financing purposes.
Likelihood	Likelihood of a risk manifesting is based on a combined assessment of threats to and the vulnerability of a channel to terrorism financing activity.

Source: Regional Risk Assessment on Terrorism Financing 2016 – South-East Asia and Australia

The regional threat assessment used similar concept for threat and applied the definition to the regional context of the risk assessment.

The risk rating is a balance between qualitative judgement and quantitative data (data based and scoring) approaches.

Other methodologies, for example that of Italy described below, differentiate between the inherent and residual risk.

Inherent risk is an assessment of the money-laundering and terrorist financing risks through identification of threats and the main criticalities or critical issues affecting the financial system and the socio-economic system.

The level of the country-inherent risk is calculated by combining an assessment of the level of threats taking into account the weaknesses of the financial system and the economy.

In the methodology used by Italy, the analysis of the inherent risk takes into account the weaknesses in the socioeconomic system, in particular the importance of the informal economy and the use of cash.

The analysis looks at the preventive, investigative and repressive safeguards against the financing of terrorism in place to determine the residual risk (see below).

Residual risk is the risk remaining once the safeguards against the financing of terrorism (preventive, investigative and repressive safeguards) have mitigated the threats.

The analysis also looks at the effectiveness of the safeguards against the financing of terrorism in place. For each category of obliged parties, the so-called specific risk and effectiveness of anti-money-laundering safeguards in place are assessed.

Specific risk is an estimate of the general level of risk associated with each category of obliged entities depending on their structural characteristics and their activities.

Then, for each category of obliged parties, a synthetic indicator of relative vulnerability is identified.

Relative vulnerability is the residual sectoral risk or residual risk for each category of obliged entity, once safeguards against the financing of terrorism applied by the obliged entities have mitigated the specific risk, depending on the adequacy of the safeguards.

The relative vulnerability or residual sectoral risk is achieved by combining the ratings of specific risk with the adequacy of the system to counter the financing of terrorism.

In 2014, Italy produced a first national assessment of the risks of money-laundering and terrorist financing. This exercise consisted of identifying and analysing the risks of money-laundering and terrorist financing, developing intervention guidelines for the mitigation of those risks and in adopting a risk-based approach to countering money-laundering and the financing of terrorism. This approach requires that the policies and measures to counter money-laundering and the financing of terrorism be carried out in proportion to the risks identified.

The first assessment was of an experimental nature but an update is currently ongoing in order to take into account the forthcoming evolution of the community and national regulatory frameworks, as well as indications arising from supervisory authorities, investigations carried out by police forces and analysis made by the financial intelligence unit. Subsequently, the national analysis will be updated every five years.

The methodology adopted by Italy

Italy has adopted its own methodology to assess the money-laundering and terrorist financing risks.[a] The methodology mainly manages information related to threats and vulnerabilities. The methodology adopted to assess terrorist financing risk derives from the money-laundering methodology, which was adapted in order to take into consideration specific measures to combat terrorist financing (i.e. freezing measures).

Within the assessment of threats, the methodology considers the financing of terrorism as a process developing in three distinct phases: collection, transfer and use of funds and economic resources.

The logical structure of the model aggregates the analysis of threats and vulnerabilities through the assessment of inherent risk and effectiveness of efforts to counter the financing of terrorism.

In particular, the model encompasses:

- An assessment of the inherent terrorist financing risk of the system, through identification of threats and vulnerabilities of the socio-economic system
- An assessment of the effectiveness of the regime to counter the financing of terrorism and the terrorist financing vulnerabilities as to the preventive, investigative, and repressive phases

When common criticalities and safeguards relating to countering money-laundering and the financing of terrorism are to be assessed, the results of the analysis are the same for both money-laundering and terrorist financing.

Source: Italy

[a] Italy, Ministry of Economy and Finance, Financial Security Committee, "Analysis of Italy's national money-laundering and terrorist financing risks: methodology" (2014).

Factors and indicators that could help to estimate threats and vulnerabilities

Threat could be estimated based on the following factors or indicators:

- The existence of groups engaged in a particular method or channel
- The capability (size of network/group and specialist capability) of groups to use the method or channel
- The intent of groups to use the method or the channel
- The history of groups using the method or channel
- The current intelligence, that is, are groups currently using this method?
- The general security environment: is terrorist financing through this method (or in general) likely at the moment? Are groups that typically use this method active now?

Vulnerability could be estimated based on the following factors or indicators:

- Accessibility of the channel for the purpose of terrorist financing
- Utility of the channel for the purpose of terrorist financing
- Measures that are in place to deter use of the channel/method
- Law enforcement agency/government/intelligence visibility of the channel/method. Note that visibility does not equal clarity.

Source: Australia

Also important to assess are the consequences of the terrorist financing activity.

A consequence is the impact or harm that money-laundering or terrorist financing may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally.

The consequences of money-laundering or terrorist financing may be short- or long-term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector.

Short-term operational funding for travelling to the Syrian Arab Republic, for fighting with ISIL in the Syrian Arab Republic, for sponsoring individual foreign terrorist fighters or for committing a lone actor attack, may involve only small amounts of money but can cause immediate harm and consequently represent a higher risk.

Longer-term organizational funding, on the other hand, may pose a lesser immediate risk, even if it ultimately helps to fund a terrorist cell or organization.

The three boxes below detail the concepts for consequences used by Australia, Italy and during the regional risk assessment on terrorist financing 2016 in South-East Asia and Australia.

The concept of consequences used by Australia

A consequence is a judgement on the amount of funds that could reasonably be raised or moved through a particular method/channel. In Australia, consequences are estimated based on the following factors:

- Actual amounts moved or raised (for example, as observed in intelligence or cases)
- For short-term goals (for example, attacks, travel and training)
- For long-term goals (for example, organizational funding, planning of large-scale attacks)
- Potential for amounts to be moved or raised

Source: Australia

The approach to consequences followed by Italy

Assessment of the consequences is an assessment of impacts attributable to the threats (i.e. financial consequences and negative social value associated with each predicate offence).

The methodology used by Italy referred to earlier proposes to estimate the consequences by using intensity indicators such as:

- The financial importance of the threat, resulting of values or estimated values of amounts of money-laundering or terrorist financing
- The negative social value attributed to the threat (depending on the minimum and maximum penalty applicable to the criminal event/crime) and, consequently, the political sensitivity of the issue
- The concrete occurrence of the threat on the territory resulting from reports on types of offences by police, the Ministry of Justice, the Ministry of Interior and other authorities

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

After acquiring analytical data on the offences or classes of offences taken into consideration, a score is assigned to each offence. The individual scores are summed and the ranking is subject to validation by experts. Experts may jointly agree to modify the intensity indicator assigned to each threat and thus the ranking. Each change is justified.

Source: Italy

The concept of consequences used for the regional risk assessment on terrorist financing 2016 in South-East Asia and Australia

Estimates of **consequence** are based primarily on how funds are used for:

- Operational purposes (e.g. moving personnel, weapons, explosives, training, attacks)
- Organizational purposes (e.g. supporting family or widows, salaries, propaganda, maintaining networks)

Generally, terrorist financing will be for operational or organizational purposes, and short-term or long-term use. Short-term operational funding, for combat or attacks, may only involve small amounts, but can pose immediate harm and high risk. Longer-term organizational funding, on the other hand, may pose a lesser immediate risk, but ultimately may help to fund greater capability and resilience of a terrorist cell or organization.

The assessment combines quantitative and qualitative information and analysis to establish an evidence base.

Concept	Definition
Consequence	Consequence is the impact or harm that terrorism financing may cause. Immediate harms include loss of life, physical damage, and undermining community cohesion and security. Consequence also includes the effect of terrorism financing and terrorist activity on the integrity and reputation of individual financial institutions, national financial systems and the broader economy. The consequences of terrorism financing may be short or long term.

Source: Regional Risk Assessment on Terrorism Financing 2016 – South-East Asia and Australia

The European Commission also defined and used the same key concepts taken or inspired from existing guidance.

The key concepts used by the European Commission

The methodology for the European Union supranational risk assessment defined a money-laundering and terrorist financing risk as the ability of a money-laundering and terrorist financing threat to exploit a vulnerability of a sector for the purpose of money-laundering or terrorist financing.

The key concepts, taken from the FATF guidance on money-laundering and terrorist financing risk assessment, are risk, threat, vulnerability and consequence.

The risk is therefore based on the following major components for assessing each relevant sector:

(a) The likelihood of terrorist groups or organized criminal groups misusing products or services provided by a sector for illicit purposes (i.e. level of threat)

(b) The potential weaknesses of those same products or services that allow terrorist groups or organized criminal groups to misuse them for illicit purposes (i.e. level of vulnerability)

The weaknesses are assessed according to the following criteria:

(a) Inherent risk exposure of the product or service due to its inherent characteristics (based on the product, geographical or customer risks)

(b) Risk awareness of the sector and competent authorities that the products or services may be misused (organizational framework of the sector, availability of a risk assessment, level of suspicious transactions reporting)

(c) Legal framework and controls in place (existing legal framework, current implementation of the controls and of the customer's due diligence requirements, level of cooperation with competent authorities)

The assessment of threats and vulnerabilities helps to define the residual risk.

The consequences: the methodology used by the European Commission did not specifically assess the consequences and impact on the region. The methodology considered this component or factor as a fixed variable; it was assumed that money-laundering and terrorist financing activities generate a constant significant negative effect. At this stage, the methodology considered impact and consequences as a fixed variable (for reasons explained in the FATF guidance).

From a methodological point of view, it is particularly challenging to measure the consequences in quantifiable or numerical terms. It is assumed that money-laundering and terrorist financing activities generate constant significant negative effects on the transparency, good governance and the accountability of public and private institutions in the European Union, cause significant damage to countries of the European Union national security and have both direct and indirect impact on the economy of the European Union.

As the impact and consequences component is assumed as a fixed high value, the determination of the residual risk for each modus operandi or risk scenario is determined by the combination of the level of threat and vulnerability identified and with the appropriate weighting.

Source: European Union supranational risk assessment on money-laundering and terrorist financing 2017

As stated above, ideally a risk assessment involves making judgments about threats, vulnerabilities and consequences.

The analysis aims to identify, analyse and assess main risks at national, regional or supranational levels, through the examination of their causes, as well as vulnerabilities that allow such risks to arise and their related consequences.

Estimating the consequences of terrorist financing activities is more conceptually slippery.

The lack of analytical data does not always allow for accurate assessments of the impacts and consequences of a money-laundering or terrorist financing activity.

How funds channelled into terrorism are ultimately used is sometimes difficult to determine, particularly if they cannot be linked to an immediate terrorist activity (e.g. a specific terrorist attack) or are used in a non-European Union country, a country with active battlefields, a country with limited access because of the presence of terrorist groups or a country with a lack of law enforcement investigation capacity.

Given the challenges in determining the consequences of money-laundering and terrorist financing, it is generally accepted that countries may opt to focus primarily on achieving a comprehensive understanding of threats they are exposed to and their vulnerabilities.

In many risk assessments, the consequences are considered as serious and important for the financial system, the economy or the security of citizens, enough to consider and justify mitigating measures.

1.5 Stages

Although the methodology must be tailored to a given country's circumstances, it is also important to stay in line with existing national risk assessment guidance, in particular with the above-mentioned FATF national money-laundering and terrorist financing risk assessment guidance of February 2013.

It is also important to observe and follow the three stages of a risk assessment: identification, analysis and evaluation.

A risk assessment takes an all-inclusive approach covering the latest developments in terms of criminal activities and an analysis of those criminal activities, an analysis of the capacity and needs of a number of competent authorities involved in countering the financing of terrorism, and an analysis of the law and regulations prevailing in certain sectors of interest for the risk assessment.

The terrorist financing risks could be identified through an assessment of statistical information from across key government agencies, supervisory and regulatory authorities, and law enforcement agencies, complemented by qualitative information, such as a perception survey involving respondents from the law enforcement agencies, reporting entities and financial intelligence units, intelligence services or independent and external experts. Independent and external studies and public information on vulnerabilities to the financing of terrorism may also be used.

1.5.1 Identification of the criminal environment

All countries include security environment information and country terrorism profiles in their terrorist financing risk assessments. Countries collect much quantitative and qualitative information on terrorist acts within their borders and in the region to take into consideration the security environment and the national terrorist and terrorist financing profile.

For an effective terrorist financing risk assessment, it is important to have a good understanding of the criminal environment of a given country or the region or supranational territory in which the money-laundering and the terrorist financing activities and predicate offences are committed and where the proceeds of crime are laundered.

Consequently, the starting point of an effective terrorist financing risk assessment is an understanding of the context of a given country and its financial system, including an understanding of the criminal environment of that country.

A good understanding of the criminal environment depends on obtaining general and specific information on the importance, size or volume of illegal activities and on the estimated proceeds. Statistics and general information on a given country, region or supranational territory financial systems and the type and importance of the criminal activities in the country are important to understanding the criminal environment.

It is also important to identify national threats by collecting quantitative data on developments in predicate crimes showing geographic concentration, as well as prosecution information including verdicts.

Expert opinions on national predicate crimes, suspicious transaction reports and typologies could also be considered.

Qualitative data and opinions from experts from law enforcement or academia can also be sought when quantitative data are missing or are not representative of a country's criminal environment and may consequently be misleading.

Many countries also explained that they shared significant amounts of information with countries with which they have close security partnerships (Morocco for instance). Such information needs to be handled carefully for security and judicial reasons due to the confidentiality of information used in ongoing judicial or law enforcement investigations.

Law enforcement agencies and security agencies already have such information and they should be encouraged to share it with all stakeholders when the legal framework and the sensitivity of the information permit such an exchange of information.

Law enforcement authorities also have access to information from Europol and INTERPOL that should be shared with the stakeholders to be included as a source of information on national, regional or supranational terrorist financing threats.

In a regional or supranational risk assessment, security environment information and country terrorism profiles must be shared or exchanged with neighbouring countries and/or other countries involved in a regional or supranational terrorist financing risk assessment.

In regional and supranational risk assessment, the sharing of information between member States is particularly developed. The regional or the supranational terrorist financing security environment could also be outlined.

Terrorist financing security environment

The European Commission collected macro-level information, essentially qualitative information on terrorist financing and also used open-source information on the main terrorist attacks to understand the financing channels.

The risk in countries both within and outside the European Union is being further analysed as part of the European Union policy on high-risk countries outside the European Union. The Commission is developing a new methodology on identifying high-risk countries outside the European Union. It will cover elements on their security environments and country terrorism profiles.

Source: European Union supranational risk assessment on money-laundering and terrorist financing 2017

A broad and deep understanding of the criminal environment is also useful in a terrorist financing risk assessment because of the nexus existing between organized criminal activities and terrorist financing activities.

This nexus between organized crime, terrorism and terrorist financing has become relatively important, as can be seen in the conclusions of many academic studies. A good example is the recent study by King's College in London, which explored and studied the nexus between criminal activities and the financing of terrorism.[2]

Most of the terrorists involved in the attacks on Paris and Brussels in recent years appeared to have past criminal records for trafficking in drugs, theft, and selling counterfeit goods. Terrorist groups need

[2] Rajan Basra, Peter R. Neumann and Claudia Brunner, *Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus* (London, King's College, 2016).

criminal groups to supply them with weapons and other materials intended for committing their terrorist acts.

It is therefore important to include the connections between crime and sectors in the assessment.

Links between terrorism and transnational organized crime

The working group discussed links between terrorism and transnational organized crime at macro-level (i.e. general trends), but did not yet enter into a case-related or specific analysis of links between terrorism and transnational organized crime beyond the work done by Europol in the serious and organized crime threat assessment report, which was used as an input for the European Union supranational risk assessment. Classified information further underpins the analysis of specific links between terrorist groups and organized crime.

Source: European Union supranational risk assessment on money-laundering and terrorist financing 2017

1.5.2 Identification of the threats

After stating the purpose and the scope of the risk assessment, and after collecting statistics on a country's, region's or supranational territory's financial system and the criminal environment, a first essential phase of the process is to identify the terrorist financing threats that the country, the region or the supranational territory is facing.

The first step, which could be applied similarly to the threats and vulnerabilities, is then to compile a list of potential (known or assumed) terrorist financing threats and vulnerabilities, the key sectors which are exploited for terrorist financing and the reasons why those carrying out the terrorist financing activities are not intercepted, convicted and deprived of their illegal assets.

An overview of a country's, region's or supranational territory's terrorist financing threats could be the result of the analysis of a range of terrorist financing case files or police investigations. National crime threat assessments, financial intelligence unit typology reports or the experiences of financial intelligence units and law enforcement may contribute to this first important step of the risk assessment.

But the country's list of terrorist financing threats could also be built on researches of open sources on potential terrorist financing threats.

During the money-laundering risk assessment process, the Belgian experts' working group analysed in detail a range of real case files or real money-laundering case studies (mainly from the financial intelligence unit and from the police) to set up a list of sectors potentially at risk of money-laundering, sectors that may, wittingly or not, be used for money-laundering purposes and weight for each sector the level of money-laundering threats (see box below).

On the other hand, during the terrorist financing risk assessment, the National Security Council denied access to and the exchange of information on real case files. Consequently, the terrorist financing platform (see. 2.1) used open source technique research to set up a list of potential terrorist financing threats (see box below).

The terrorist financing platform then asked its members to validate or invalidate, based on their own experience in real cases (criminal, financial intelligence unit, customs and other investigations) but without sharing the content and substance of these real investigations or the potential source of terrorist financing.

Open sources identification of the threats

The terrorist financing risk assessment is a comprehensive assessment of the terrorist financing threats by experts from the financial intelligence unit, the police, the prosecutor's office, the intelligence services, the Coordination Unit for Threat Analysis, the customs and excise administration and the Ministry of Economy. All of them, except the Ministry of Economy and the customs and excise administration, are members of the terrorist financing platform.

Belgium started identifying all potential sources of financing of terrorism and techniques of financing terrorism by looking at all the available open sources, such as FATF and Egmont Group of Financial Intelligence Units typology reports and studies, INTERPOL and Europol research, documents and publications, academic studies and publications, books, conferences, newspaper articles, and analysis by other financial intelligence units.

For each source of financing identified in the open sources a fact sheet was created, even if at the time of the assessment process, there was no indication in Belgium that this source of financing may also affect or have an impact on or in Belgium. Each fact sheet provided a short description of the potential source of financing of terrorism and references to the open sources.

The terrorist financing threats and the terrorist financing techniques identified in the open source documents were divided into three subgroups: microfinancing and macrofinancing of terrorism and techniques of terrorist financing. Belgium also identified the techniques that could be used to finance terrorism or terrorist activities.

After the first stage (identification), the competent authorities involved in the terrorist financing risk assessment were invited, based on their experience, to validate or invalidate the potential sources of terrorist financing and techniques identified in the open sources.

The objective of the second stage (validation process) was to assess whether:

- Funds or other assets could be collected or obtained in Belgium using each of the identified potential sources of terrorist financing and the potential terrorist financing techniques identified during the identification process
- Country sectors of activities or even public authorities could be involved directly or inadvertently in the financing of terrorist activities
- Funds or other assets mentioned above that transited through the sectors or were obtained from public authorities could be used to finance terrorist activities in Belgium or abroad

The validation process also aimed at weighing the level of threat associated with each potential source of terrorist financing. The terrorist financing platform also rated the potential threats and techniques starting from an inexistent (or not verifiable) level of threat to a high level of threat (see section on ratings).

During the identification and validation processes, experts never exchanged information on specific case files or real case studies and criminal investigations, but each partner used their experience in handling real case files to validate or invalidate a source of funding, because, based on their experience, the source of funding was not really affecting Belgium and its financial sector.

Source: Belgium

The identification and validation processes could be the results of brainstorming sessions. The working group or stakeholders in charge of the terrorist financing risk assessment could also organize several brainstorming meetings with various experts from the financial intelligence unit, the police, the intelligence services, the control authorities to list potential terrorist financing threats.

This technique involving brainstorming sessions is used in many countries and has also been used by the European Commission in the context of the first European Union supranational risk assessment on money-laundering and terrorist financing.

Information on terrorist financing threats could be collected at the different stages of the counter-terrorist financing framework.

First, information could be collected at the detection stage by gathering information from terrorist financing case studies provided by the financial intelligence unit. Then, an analysis of a range of terrorist financing convictions (sanctioning stage) could also help to collect additional information on terrorist financing threats.

1.5.3 Identification of the vulnerabilities

Vulnerabilities refer to weaknesses or gaps in a country's measures against money-laundering or terrorist financing.

In terrorist financing risk assessment, the range of sectors that may be abused for terrorist financing activities is larger, as terrorists may fund their activities by abusing not only sectors subject to measures to prevent the financing of terrorism, but they may also abuse some public authorities, for instance public authorities granting social benefits.

The identification of terrorist financing vulnerabilities goes beyond the identification of the weaknesses or gaps affecting the sectors subject to measures to counter the financing of terrorism.

But for the sectors subject to preventive measures, the measures against money-laundering or terrorist financing may include the following elements: reporting entities' ownership controls, customer due diligence measures applied by reporting entities, conservation of identification documents and documents related to the financial transactions with customers, reporting suspicious financial transactions, internal controls and training, counter-terrorist financing supervision and the country's administrative sanction regime.

The preventive measures also include the effectiveness of the analysis of suspicious transactions, national cooperation with other competent authorities, international cooperation with other financial intelligence units and non-financial intelligence authorities, dedication of resources and dissemination to law enforcement authorities.

The country investigative and criminal frameworks and safeguards include the effectiveness of the analysis of suspicious transaction reports, the effectiveness of the investigative techniques, the dedication of resources, the effectiveness of the cooperation with other authorities, the capacity to punish perpetrators of money-laundering and terrorist financing activities and the capacity to seize and confiscate assets issued from criminal activities or aimed at financing terrorist activities.

Most of the time, significant amounts of information on the country's vulnerabilities could be found in the country mutual evaluation report (FATF, the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism or IMF/World Bank mutual evaluation process), in supervisory reports, reporting entities' own risk assessments and from the experience of financial intelligence units, law enforcement authorities and prosecution authorities.

Not all the sectors identified during the first stage of the risk assessment (the threat assessment) that presented a high, medium or low level of money-laundering or terrorist financing threat were reporting entities subjected to measures to prevent the financing of terrorism.

Additional information on the vulnerabilities associated with some specific sectors may be required if the mutual evaluation report and other country reports do not cover all the sectors subjected to terrorist financing threats.

This is the case in terrorist financing risk assessments where the threat assessment identifies sectors which are yet subject to measures to counter the financing of terrorism.

Usually mutual evaluation reports do not provide information on the structure of sectors, their organization, the products, distribution channels and geographical distribution of the distribution channels.

The analysis of national vulnerabilities can also receive input through brainstorming sessions or through a questionnaire sent to the supervisory authorities of the reporting entities or to other competent authorities, which may have information on the structure, organization, supervision and control of the sector (including non-counter-terrorist financing control measures such as tax audits, which could reduce and impact the risk of a sector's getting involved in or being misused for terrorist financing activities) and the effectiveness of the supervision and control measures in the sector, the type of products or services provided by the sector and the nature of the products.

Even if the mutual evaluation report is a recent publication, some information may be missing from it and the use of a questionnaire to clearly understand the sectoral vulnerabilities may be an unavoidable requirement.

Experts or people with academic expertise could also be approached to get their opinions on the vulnerabilities that limit the effectiveness of the regime to counter the financing of terrorism.

For the sectors that are subject to supervision to counter the financing of terrorism, supervisory authorities may provide useful information on the effectiveness of the measures to prevent the financing of terrorism in the sector. Results from off-site and on-site inspections could help to determine the sector-specific vulnerability scale.

For the sectors that are not subject to measures to prevent the financing of terrorism, other kinds of control activities by authorities not directly responsible for countering the financing of terrorism (inspections by tax authorities, customs and ministries of economic affairs) could help to mitigate the risk of money-laundering or terrorist financing.

An assessment of these additional measures would be required to assess the vulnerability affecting these sectors.

The organization of the competent authorities and supervising authorities with respect to human resources (staff and expertise), financial resources, tools, equipment and training also need to be considered in a vulnerability assessment.

As in the Italian methodology, the vulnerability assessment could be divided into the investigative phase, the preventive phase and the prosecution phase.

Statistics on the number of cases of involvement of reporting entities in terrorist financing activities and investigations, as well as the number of breaches of the counter-terrorist financing framework or deficiencies and irregularities identified during on-site inspections (and counter-terrorist financing sanctions), could be used to assess the quality of the existing safeguards against the financing of terrorism.

Italy: The methodology, analyses and assessments of the safeguards mitigating the inherent risk

The analysis of the safeguards was conducted by breaking down the system into the following stages: prevention, investigation and prosecution. The effectiveness of the anti-money-laundering and counter-terrorist financing regime was assessed as to the: preventive phase (preventive safeguards), investigative phase (investigative safeguards) and the prosecution phase (prosecution safeguards). Within such phases, the model analyses their respective vulnerabilities.

Italy uses a model by which it performs an analysis of the effectiveness of the safeguards applied by each category of reporting entities: financial intermediaries, professionals and non-financial operators. The model also looks at some specific safeguards, such as cross-border cash controls or measures for the transparency of legal entities, and assesses the effectiveness of suspicious transaction reports.

The analysis starts with quantitative data and information on the results of inspections or off-site inspections, reports of irregularities and sanctions, information from other supervisory authorities. However, the final assessment is left to experts from the supervisory authorities, the financial intelligence unit, the police and other authorities, and includes a qualitative assessment.

The number of cases of involvement of the reporting entities in money-laundering or terrorist financing activities, the number of deficiencies identified during the inspections or the number of sanctions applied to the obliged entities are factors that could be used to assess the vulnerability level of the obliged entities.

Using the same methodology the effectiveness of the investigative (analysis of the suspicious transaction reports, investigation by the judicial authorities and law enforcement) and prosecution (convictions and seizure and confiscation of proceeds of crime) safeguards are also assessed.

The analysis can also be extended to entities not subject to money-laundering legislation, whereby close attention is required.

A so-called specific risk and the anti-money-laundering safeguards are assessed for each obliged entity. The specific risk is an estimate of the general level of risk associated with each category of obliged entities, depending on their structural characteristics and their activities.

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

The analysis is common both for money-laundering and the financing of terrorism, except for measures specifically designed to combat the financing of terrorism, such as the assets freezing measures decided by United Nations sanctions committees.

Source: Italy

1.5.4 Steps followed during the European Union supranational risk assessment

The methodology for the European Union supranational risk assessment provided for five main steps:

1) The first step listed all the modi operandi for terrorist financing (also named risk scenario). At this first stage, the objective was to identify the nature of the risk scenarios and those that are the most relevant considering the scope of the European Union supranational risk assessment. In the context of the assessment, the risks scenarios are intended as terrorist financing mechanisms going beyond the specificities of national jurisdictions, whether they arise in one or several member States, and may represent a risk from the perspective of the internal market of the European Union.

2) For each modus operandi, the risk assessment working group (see below) assessed the level of the threat. The threats related to the estimated intent and capability of criminals and terrorist financing facilitators to exploit existing or innovative mechanisms of terrorist financing.

3) For each modus operandi, the risk assessment working group also assessed the level of the vulnerability for the sectors covered by a specific modus operandi. The vulnerability assessment focused on existing safeguards in place in the sectors that may be exploited for each terrorist financing modus operandi.

The European Commission analysed specific terrorist financing vulnerabilities for each sector based on quantitative and qualitative information and also identified scenarios specific for terrorist financing and not considered relevant for money-laundering (e.g. consumer credit, non-life insurance etc.) and for which a specific vulnerability assessment relating to the financing of terrorism was carried out.

4) Ultimately, the risk assessment working group defined the level of residual risk for each modus operandi by combining the threat level with the level of vulnerability. In so doing, the working group decided to grant a higher weighting to the vulnerability (60 per cent) than to the threat (40 per cent).

5) In the light of the identified risk, the European Commission is responsible for managing the risks. The Commission identified measures necessary to address the identified risks (risk management).

For each of the scenarios identified under step 1 above, the methodology assessed the level of threat on a four-point scale: (slightly significant (1), moderately significant (2), significant (3), very significant (4).

The assessment is to be based on the estimated combined assessment of intent and capability of criminals to change or transfer illegitimate or legitimate funds.

The intent component of the threat assessment relies on known intent (concrete occurrence of the threat), whether the intended activity was successfully carried through or was foiled, and the perceived attractiveness of money-laundering and terrorist financing through a specific mechanism. While the broad intent to launder money and finance terrorism is assessed as being constantly high, the intent to use a specific modus operandi differs depending of the attractiveness of the modus operandi, and the known existence of safeguards against money-laundering and the financing of terrorism. The risk assessment therefore considers, case by case, the level of intent to exploit money-laundering and terrorist financing mechanisms.

The capability component of the threat is understood as the capability of criminals and terrorist financing facilitators to successfully change or transfer illegitimate or legitimate funds to financially maintain a terrorist network.

(continued)

The assessment of the capability component will consider the ease of using a specific modus operandi to launder money or finance terrorism (amount of technical expertise and support required) and the accessibility and relative costs (financial capacity) of using a specific modus operandi.

For each of the scenarios (money-laundering and terrorist financing processes versus exploitable sector) identified under step 1 above, the methodology also assessed the level of vulnerability according to a four-point scale: (slightly significant (1), moderately significant (2), significant (3), very significant (4).

For each of the scenarios identified under step 1, the vulnerability assessment focuses on the existence and effectiveness of the safeguards in place. The more effective the safeguards, the lower the vulnerabilities and the risk.

The vulnerability component is the most useful in determining the risk level. The level of vulnerability is likely to increase the attractiveness and hence the intent of criminals and terrorists to use a given modus operandi, thus ultimately affecting the level of risk.

Under the methodology, a specific framework has been developed for defining the level of vulnerability that depends on three main components: inherent risk exposure (the risk exposure before mitigating measures are put in place), awareness of the risk (the level of risk understanding among the public and private sectors), control measures in place. For each of those components, the methodology has defined a number of factors to be assessed.

1) Inherent risk exposure

- Product: speed and anonymity of transactions, delivery channels, volume of transactions, cash involvement, management of new technologies and payment methods;
- Customer: high-risk customers, management of benefifical owner risks;
- Geographical risk: high-risk areas, size of cross-border transactions.

2) Awareness of the risks and vulnerabilities

- Awareness on the part of the sector; organizational framework;
- Awareness on the part of competent authorities; law enforcement agency capacity to counter money-laundering and terrorist financing;
- detection and analysis by the financial intelligence unit.

3) Legal framework and controls in place

- Existing legal framework;
- Effectiveness of controls put in place by public entities: internal controls, reporting of suspicious transactions;
- Domestic and international cooperation between anti-money-laundering authorities.

The aim of the European Union supranational risk assessment was not to pass judgment on a sector as a whole, but to identify circumstances in which the services and products it delivers or provides could be abused to launder money or finance terrorism.

The rating itself is not a panacea. It only represents efforts to objectivize a line of reasoning by summarizing a complex analysis through a figure. Therefore, the methodology did not over-emphasize the risk rating, but always referred to the underlying analysis, namely, the material elements of the threats or the vulnerability that explain or justify the rating.

This supranational risk assessment also focused on vulnerabilities identified at European Union level, both in terms of legal framework and in terms of effective application.

Source: European Union supranational risk assessment on money-laundering and terrorist financing 2017

1.6 Weights and ratings

Various rating techniques and ratings could be used to assess the level of threats and vulnerabilities and consequently the risks of money-laundering or terrorist financing for each threat and vulnerability identified during the identification process.

At this stage, the risk assessment adopts an approach that will attempt to rate the extent of the different risks to assist with prioritizing mitigation efforts.

The rating itself is not a panacea. The rating only represents efforts to objectivize a line of reasoning by summarizing a complex analysis with a figure.

Although quantitative data, where available, are important in rating a threat or a vulnerability, collecting the opinion of experts is also useful, because sometimes quantitative data or the lack of data on a specific threat can alter the results of the risk assessment.

It is also important to have material elements that explain or justify the rating.

Rating the level of vulnerability is important to correctly allocate resources when implementing measures to mitigate the risks. The rating helps to classify the risks depending on their intensity and to allocate the unavoidably limited amount of resources to the most vulnerable sectors.

It is entirely unproductive to allocate resources to sectors or sources of terrorist financing with a low level of risk and then lacking resources to mitigate the risks in high-risk sectors.

Various kinds of rating techniques may be used to rate the level of threat or vulnerability for each sector or source of financing terrorism:

- 1 to 4 ➲ inexistent (or not verifiable, or negligible), low, medium, high
- 1 to 4 ➲ insignificant, slightly significant, moderately significant, very significant
- 1 to 3 ➲ low, medium, high

Insignificant does not necessarily mean non-existent or irrelevant, but the threat intensity is very low.

When talking about vulnerabilities, some countries use the following ratings: Insignificant vulnerability, slightly significant vulnerability, moderately significant vulnerability and very significant vulnerability.

Quantitative methods

An analysis of a range of money-laundering or terrorist financing case files and a range of indicators could be used to assess the level of threat for a sector.

A range of indicators could be used to classify sectors depending on their level of threat.

A sector's level of threat could be assessed using the following indicators: number of police investigations, number of financial intelligence unit case files, number of cash declarations received by the customs authorities, number of offences identified by the economic affairs ministry involving the sectors under assessment, geographical concentration of the criminal activities (criminal group active in one region of a country, or in multiple regions), international or only national flows of money, involvement of high-risk jurisdictions, a low or high number of suspects involved in a case, the involvement of foreign companies, whether underlying criminal activities are committed by organized criminal groups, involvement of foreign nationals or foreign residents, the seriousness of the predicate offences, the length of the offence period and the average amount of the financial transactions.

A high number of financial intelligence unit case files or law enforcement investigations with regard to a specific sector result in a higher level of threat for the sector. A very large number of files relating to terrorist financing over a lengthy period results in a higher level of threat. A terrorist being able to collect

large amounts of money over a very long period of time results in a greater threat of terrorist financing to a given country.

Such data could be collected in a range of cases dealt with by the financial intelligence unit, the police (investigation reports), customs authorities (reports of seizures of cash) and economic affairs (checking compliance with restrictions on payment in cash) and the data could be converted using the above-mentioned indicators to compare and rank all of the analysed sectors.

Such a multiple-criteria analysis is based on processing quantitative data available from authorities involved in combating money-laundering (financial intelligence unit, police, customs, and economic affairs ministry).

On the other hand, Australia used a five-point scale: negligible, low, medium, high, and very high.

Australia: risk assessment model

The assessment model uses the concepts explained in the previous chapter **(risk = likelihood x consequences, likelihood = threats + vulnerabilities)**, and adapts them to suit to an assessment of terrorist financing.

Likelihood is estimated based on a combined assessment of threats to, and vulnerabilities of a channel to terrorist financing activities. Estimates of likelihood in the assessment draw largely on operational intelligence and information from the Australian Transaction Reports and Analysis Centre, the country's financial intelligence unit.

Threat is estimated by taking into account the existence of terrorist-related groups and their intent and capability to use the techniques linked to terrorist financing through a specific channel to terrorist financing activity.

Vulnerability is a mix of a channel's accessibility and utility, measures to deter terrorist financing and other risks, and intelligence visibility over the channel.

Assessments of risk consequence in the national risk assessment are based on estimates of: *(a)* the amounts that have or can be raised or moved through a channel, and whether funds are likely to be for *(b)* operational or organization ends over *(c)* the shorter or longer term. This enables gradations of risk consequence to be differentiated across methods and channels. Estimates of consequence are tentative, but avoid the pitfalls of grouping all terrorist financing activity as worst case.

In addition, risk ratings take into account a country's financial sector, political governance and regulatory framework where possible.

Likelihood (threat x vulnerability)	Consequence: Low	Consequence: Medium	Consequence: High
More likely	Medium	High	Very high
Possible	Low	Medium	High
Less likely	Negligible	Low	Medium

Methodology to assess high-risk countries

A risk matrix is also employed for the chapter on high-risk countries. It is based on general indicators that shape a country's risk profile for Australia:

- Are migrants from the country present in Australia with possible or potential ties to extremist and terrorist organizations based in or linked to the country?
- Do other communal links exist between groups in Australia and terrorist or affiliated movements in the country?
- Is it a destination for radicalized individuals and extremists?
- Is it in conflict or unstable and at risk of conflict involving terrorist activity?
- Is it a potential destination or conduit for terrorist financing flows?

In addition, risk ratings take into account a country's financial sector, political governance and regulatory framework where possible.

Source: Australia

The Italian methodology uses multiple steps or stages to assess the risk of money-laundering or terrorist financing, which consist of assessing the inherent risk, the relative vulnerabilities or residual risk using specific ratings tables.

Italy: experience in rating threats and vulnerabilities

The level of inherent risk is assessed through the combined assessment of threats and weaknesses using the rating table below:

Threat					
	Very significant				Very significant
	Moderately significant			Moderately significant	
	Slightly significant		Slightly significant		
	Insignificant				
		Non-significant	Slightly significant	Moderately significant	Very significant
		System weaknesses			

(continued)

The relative vulnerabilities, or the residual risk, are assessed through the combined assessment of specific risk and vulnerabilities of the preventive safeguards using the rating table below:

Specific risk				
Very significant				Very significant
Moderately significant			Moderately significant	
Slightly significant		Slightly significant		
Insignificant				
	Non-significant	Slightly significant	Moderately significant	Very significant

Vulnerabilities of preventive safeguards

Relative vulnerabilities could also be broken down by preventive safeguards, investigative safeguards and the repressive safeguards using the following rating tables:

Specific risk					
4	High risk				Very significant
3	Significant risk			Moderately significant	
2	Average risk		Slightly significant relative vulnerability		
1	Low risk	Insignificant relative vulnerability			
		Insignificant	Slightly significant	Moderately significant	Very significant
		1	2	3	4

Vulnerabilities of preventive safeguards

Source: Italy

The regional risk assessment on terrorist financing 2016 in South-East Asia and Australia used a more sophisticated risk model or ratings including ratings on risks and a matrix measuring the likelihood of the threats and vulnerabilities.

The regional risk assessment employed the standard risk framework (likelihood x consequence = risk) and the likelihood was based on a combined assessment of the threat to and vulnerability of a channel to terrorist financing activity.

The ratings in the risk model are classified as high, medium or low and the likelihood is classified more likely, possible and less likely.

Risk ratings

Weightings of low, medium and high risk were developed to produce risk ratings for each channel.

	Risk statements
High	Financing source or transfer channel requires immediate attention to migrate risks, particularly severe operational consequences
Medium	Financing source or transfer channel requires attention and/or further monitoring to mitigate risks
Low	The risk of the financing source or transfer channel being used for terrorism financing is low and/or may be difficult to determine

Likelihood matrix

THREAT

Measuring threat factors

Main information sources:

- Statistical data
- Cross-border movement of funds/value
- Supervision inspections
- FIU information exchange
- Law enforcement agency information exchange
- Extradition request
- Number of terrorism financing investigations or counter-terrorism operations including a terrorism financing component

VULNERABILITY

Measuring vulnerability factors

Relevant FATF recommendations:

- Recommendation 1
- Recommendation 2
- Recommendation 5
- Recommendation 6
- Recommendation 8
- Recommendation 14
- Recommendation 16
- Recommendation 20
- Recommendation 29
- Recommendation 32
- Recommendation 36
- Recommendation 37
- Recommendation 40

	Threat statement
High	Channel is perceived as attractive and is easy to access for terrorism financing activity
Medium	Channel is perceived as moderately attractive and requires some knowledge to access for terrorism financing activity
Low	Channel is perceived as relatively unattractive and is difficult to access for terrorism financing activity

	Vulnerability statement
High	There are limited or no measures and controls in place to deter and detect terrorism financing activity, or they are not working as intended
Medium	Deterrence measures and controls have some effect at deterring and detecting terrorism financing activity
Low	Deterrence measures and controls are reasonably effective at deterring and detecting terrorism financing activity

	Likelihood statement
More likely	Individuals and/or terrorist groups regularly use the channel for terrorism financing activity
Possible	Individuals and/or terrorist groups sometimes use the channel for terrorism financing activity
Less likely	Individuals and/or terrorist groups rarely use the channel for terrorism financing activity

Source: Regional Risk Assessment 2016 – Terrorism Financing, South-East Asia and Australia

Qualitative methods

Qualitative methods include brainstorming sessions and workshops in which experts from the financial intelligence unit, police, intelligence services, judicial authorities and other services assess the level of threat or vulnerability for each sector and source of financing.

The final level of threat or vulnerability is the result of an assessment made by several experts, each one using his or her own experience to assess and fix the level of threat or vulnerability.

Experts could agree on the level of threat or vulnerability or the final level of threat or vulnerability could be an average of their respective assessments.

This methodology was used for the European Union supranational risk assessment on money-laundering and terrorist financing 2017, where experts from the 28 European Union member States were invited to identify money-laundering and terrorist financing threats and vulnerabilities and invited to estimate for each threat and vulnerability identified the level of threat or vulnerability: slightly significant (1), moderately significant (2), significant (3) and very significant (4).

Each member State provided its own appraisal of the level of threats and vulnerabilities, the final result being an average of appraisals made by the experts of all 28 member States.

Experts may reach a consensus on a particular rating or the rating may be an average of the individual ratings proposed by each member State for a specific threat or vulnerability.

When, for instance, three member States of a total of six estimated the level of threat as being moderately significant (2) and the rest of the member States estimated the level of threat as being significant (3), the final level of threat was rated 2.5.

On the other hand, if a majority of member States estimated the level of threat as being moderately significant (2) and only a few countries asked to rate the threat as being significant (3), the final level of threat was rated 2.0.

Chapter 2

Competent authorities

2.1 Risk assessment working groups

When dealing with their risk assessments, countries prefer to establish formal inter-agency working groups.

Round-table discussions and working groups of experts from different agencies are examples of inter-agency working groups. Each expert brings the information and data available in his or her agency. One agency will be designated as leading and coordinating authority. Round-table discussions could also be complemented by interviews, questionnaires and assessments of the levels of threat and vulnerability affecting the country in question.

The competent authorities include authorities and experts with knowledge in the field of money-laundering (and predicate offences) and in the field of terrorism and terrorist financing.

It is important to also include, if acceptable to all stakeholders involved, the supervisory authorities of the reporting entities and other competent authorities in the public sector, as they have experience with the sector's vulnerabilities.

Competent authorities include:

- Policymaking bodies (as users of the results of the risk assessment)
- Law enforcement and judicial authorities (police, customs)
- Intelligence services
- Financial intelligence units
- Regulatory and supervisory authorities
- Ministry of finance (in most countries, the treasury is in charge of freezing assets related to United Nations resolutions), ministry of foreign affairs
- FATF-style regional bodies of which a country is a member may also be useful source of information on risk, in particular regarding work carried out elsewhere in the region to identify and understand risk. FATF-style regional bodies could also be useful to understand regional terrorist financing risks and their contribution to subnational risk assessments could be very useful and interesting. Regional bodies could also facilitate exchanges of information on risks between

foreign partners, such as authorities from other countries, having potential useful source of information.

- Supervisory authorities
- Representatives from the private sector to the extent that their participation in the process may be appropriate and useful to the understanding of the terrorist financing risks
- Representatives of civil society, researchers and academics

The involvement of certain authorities is not straightforward when sensitive information is being exchanged, as is the case in a terrorist financing risk assessment. The involvement of supervisory authorities and the private sector in a terrorist financing risk assessment is essential, mainly for the assessment of the terrorist financing vulnerabilities. Consequently, their involvement could be limited to providing information through a questionnaire on the vulnerabilities, rather than being involved as a permanent member of the terrorist financing risk assessment working group.

Information on vulnerabilities collected during the money-laundering risk assessment may also be used to assist in the terrorist financing risk assessment.

Various mechanisms or risk assessment working groups exist among the countries that participated in an expert group meeting to identify good practices on terrorist financing risk assessments.

Depending on the options made by the participating countries, the risk assessment working groups could include a limited number of stakeholders or a large number of stakeholders may be engaged in the preparation of the risk assessment working group.

The Belgian terrorist financing platform or working group

The National Security Council and the Intelligence and Security Coordination Committee of Belgium set up various platforms, one of which is the terrorist financing platform.

The Financial Intelligence Processing Unit of Belgium is the leading authority of the terrorist financing platform in charge of preparing the national terrorist financing risk assessment. Members of this platform include representatives of the Federal Prosecutor's Office, law enforcement (federal police), intelligence services (civil and military), the Coordination Unit for Threat Analysis, the Chamber of Prosecutors-General, the General Administration for Customs and Excise, the finance ministry (treasury, responsible for the United Nations and European Union sanction lists) and the foreign affairs ministry.

Belgium also has a Coordination Unit for Threat Analysis. The Unit is comprised of members of the Federal Prosecutor's Office, police, civil and military intelligence services and customs office and continually analyses the terrorist threat in Belgium. To this end, the unit collects information on potential threats and individuals that could lead to these threats. Foreign terrorist fighters who have left for or returned from the Syrian Arab Republic are obviously among those individuals.

Source: Belgium

Lebanon opted for a large number of stakeholders

The financial intelligence unit of Lebanon, the Special Investigation Commission, led the national risk assessment project, engaging stakeholders from the public and private sectors, and the two national committees responsible for countering money-laundering and the financing of terrorism, which, alongside the Special Investigation Commission, include the following authorities: Bank of Lebanon, General Prosecutor's Office, Internal Security Forces, Customs Directorate, Ministry of Justice, Ministry of Finance, Ministry of Economy and Trade, Ministry of Interior and Municipalities, and Banking Control Commission.

Also, several representatives of the private sector were asked for their opinions and additional information, namely: Association of Banks, Association of Money Dealers, Association of Jewellers, Association of Finance Companies, Association of Insurance Companies, Association of Certified Public Accountants, Association of Real Estate Builders, Association of Notaries, Association of Lawyers, Casino and others.

Non-governmental actors were also involved through meetings and questionnaires.

Source: Lebanon

Italy: Financial Security Committee

The Financial Security Committee is the national anti-money-laundering and counter-terrorist financing body and is responsible for conducting and updating the national risk assessment.

In particular, the national risk assessment was conducted by a dedicated working group with representatives from all the authorities of the Financial Security Committee, in consultation with other agencies involved.

To assess the terrorist financing risk, Italy decided not to involve non-governmental actors, since in this specific field, the country relied on investigations conducted by the authorities, both from the preventive and repressive sides, and on qualitative data arising from the intelligence.

In assessing the money-laundering risk, on the other hand, academia was involved as a non-governmental actor.

Source: Italy

The experience of Australia

The following competent authorities are involved in the national risk assessment in Australia: national, federal state and territory counter-terrorism and law enforcement authorities including intelligence agencies, central policy departments and, to a lesser extent, sector regulators.

The financial intelligence units of Australia and Indonesia have also engaged their regional embassies and met with regional authorities (mainly financial intelligence units and counter-terrorism, intelligence and security agencies) to develop the regional picture.

Open source information including FATF/APG reporting has also been used. Diplomatic posts have been a very good source of foreign country and regional information.

Owing to the sensitive nature of the national risk assessment on terrorist financing, the first undertaken in Australia, limited consultation with non-government actors was undertaken.

The results were shared through various outreach and industry consultative bodies afterwards. Since then, our sector assessments that combine money-laundering and terrorist financing include heavy private sector engagement through consultation, surveys and focus group work. The same approach was applied to the recent national risk assessment on non-profit organizations in Australia.

Source: Australia

Turkey: steering committee

As the scope and nature of terrorist financing risk assessments should ultimately meet the needs of their users such as policy makers, supervisors, operational agencies, financial institutions, and designated non-financial businesses and professions, Turkey included all of them in the terrorist financing risk assessment process.

The participating organizations are the financial intelligence unit, other domestic intelligence units, relevant ministries (Ministry of Justice, Foreign Affairs, Finance, Interior Affairs, Customs and Trade), various law enforcement agencies, the supervisory institutions, professional associations from financial and non-financial sectors and non-profit organizations.

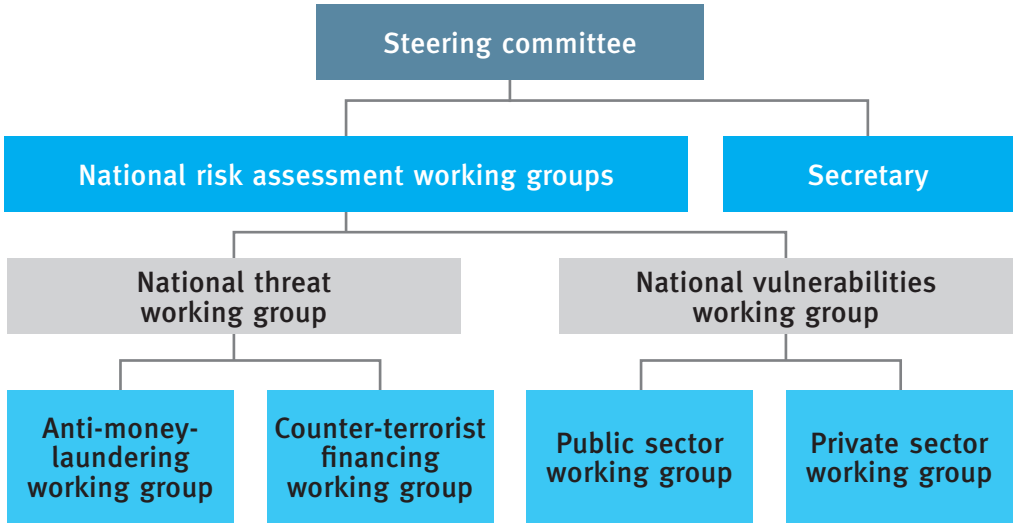
Turkey founded a steering committee, which is the designated authority responsible for coordinating and conducting the country's national money-laundering and terrorist financing risk assessment and various working groups.

The financial intelligence unit of Turkey, the Financial Crimes Investigation Board, carries out the secretariat work and is also responsible for coordinating the national risk assessment process.

The organizational structure of the national risk assessment is shown below. Each working group has its own coordinator.

The coordinators are responsible for exchanging and sharing information with the members through email and in face-to-face meetings.

Source: Turkey



The private sector and non-profit organizations could also be involved by providing data and statistics whenever requested, by providing opinions through answering perception surveys or through discussions in the focus group. Academia could also be involved to provide its expert views.

In Europe, the European Commission also worked with working groups and meetings to identify the relevant modi operandi (scoping), carry out the analysis (risk analysis) and define mitigating measures (risk management).

The European Commission actively worked with stakeholders from within the European Union institutions, with member States experts and with the civil society.

The European Union supranational risk assessment on money-laundering and terrorist financing 2017

The European Union supranational risk assessment on money-laundering and terrorist financing 2017 was conducted from November 2015 to March 2017.

The Commission organized a series of meetings to identify the relevant modi operandi (scoping), carry out the analysis (risk analysis) and define mitigating measures (risk management).

The analysis involved three layers of stakeholders.

Within European Union institutions

The European Commission, being responsible for the supranational risk assessment, put in place an inter-service group responsible for steering the process. It involved all the interested services of the European Commission, in particular the Directorate General for Justice and Consumers, the Directorate General for Migration and Home Affairs, the Directorate General for Financial Stability, Financial Services and Capital Markets Union, the Directorate General for the Internal Market, Industry, Entrepreneurship and Small and Medium Enterprises, the Directorate General for International Cooperation and Development, the European External Action Service, the Secretariat General, and the

(continued)

Legal Service. The European Commission adopted the methodology, monitored its implementation and discussed the outcome. Ultimately, the Commission adopted the report of the supranational risk assessment (including the mitigating measures).

In addition, directive (EU) 2015/849 requires the European supervisory authorities to submit a joint opinion on the risk affecting the European Union financial sector as an input for this exercise. The European supervisory authorities put in place a specific anti-money-laundering committee that prepared the opinion.

The European Union Intelligence and Situation Centre provided intelligence for the risk assessment and participated in the specific workshops on the financing of terrorism.

The European Commission also bilaterally consulted Europol to receive specific input, in particular for assessing the threat.

Involvement of member State experts

The European Commission organized a series of workshops on the supranational risk assessment with member States experts for carrying out the analysis. The Commission organized dedicated workshops on money-laundering versus terrorist financing. The Commission prepared background documents that were discussed in this workshop. The workshops brought together in the same room representatives from European Union member States, European Union agencies and the European Commission. From the member States, national experts represented regulators, law enforcement authorities, financial intelligence units, supervisors and intelligence services. By way of this process, the perspectives of all public sector parties were fed into the analysis. Such a holistic approach was considered as crucial to enriching the analysis, and avoiding blind spots and bias in the analysis. It was the main driver for carrying out the analysis.

In addition, specific Commission expert groups composed of member State experts were consulted or debriefed throughout the process. For instance, the Commission consulted the Expert Group on Money-Laundering and Terrorist Financing, the European Union Financial Intelligence Units' Platform and the Expert Group on Gambling Services.

In addition, the Expert Group on Money-Laundering and Terrorist Financing collected statistics on the number of obliged entities and suspicious transaction reports by member States.

Involvement of civil society (the private sector and NGOs)

The European Commission intensively engaged with the private sector during the process. It organized four thematic groups with the following stakeholders:

- Financial sector (banks, payment institutions, money remittances, etc.)
- Legal professionals (lawyers, notaries, accountants) and other designated non-financial businesses and professions (real estate agents, chambers of commerce, diamond dealers, virtual currency providers, etc.)
- Gambling sector (because it is a newly regulated sector)
- NGOs and academics
- Consumer organizations

(continued)

Three rounds of consultations with representatives from civil society were organized through dedicated meetings for each thematic group of stakeholders.

Those workshops were held at three crucial stages:

- First meeting (February 2016): following the preliminary risk identification (to collect input for identifying modi operandi)
- Second meeting (November 2016): after the preliminary results of the analysis carried out by the European Commission following the workshops on the supranational risk assessment (to test and challenge the preliminary results with civil society)
- Third meeting (March 2017): after determining possible mitigation measures (to test and challenge possible mitigating measures with civil society)

Civil society was invited to submit their contributions in writing after each workshop. With regard to terrorist financing, specific meetings were held with NGOs to discuss terrorist financing risk posed by NGOs (see recommendation 8). NGOs were heavily involved in the discussion of this matter.

The public was informed of this targeted consultation process through the publication of a road map. The Commission invited all European stakeholders that had submitted contributions for the proposal of directive (EU) 2015/849, as well as those stakeholders having contacted the Commission to be involved in the public sector consultation process.

For the private sector consultation, the Commission worked with European federations and platforms that were accompanied by experts from national federations.

The consultations also helped to better identify what the private sector needs to improve in its sectoral risk assessment and the implementation of its obligations.

FATF-style regional bodies and the Egmont Group of Financial Intelligence Units have not yet been involved or consulted, but in the future, the Egmont Group will be consulted as a new observer of the European Union financial intelligence unit platform.

Source: European Commission

2.2 Lead agency

In a given country, the agency with the best terrorist financing operational and strategic knowledge should lead the national terrorist financing risk assessment working group. This could be the main agency dealing with terrorism issues.

In many countries the financial intelligence unit presented is the agency that possesses the best operational and strategic knowledge in the field of terrorist financing.

That is why financial intelligence units are often the agency designed to lead the terrorist financing risk assessments.

Nevertheless, it is worth mentioning that financial intelligence units may not always have sufficient inside knowledge of terrorism and terrorist financing activities beyond the detected financial flows and terrorist financing money trails resulting from the analysis of suspicious transaction reports received.

It is not an obligation to have the financial intelligence unit as the leading authority. The leading authority could be another competent authority, like in Morocco, where the leading authority for the terrorist financing national risk assessment is the Ministry of Interior.

The authorities in Morocco decided to give the leadership of the terrorist financing risk assessment working group to the Ministry of Interior because the Ministry plays an important role in the fight against terrorism.

The authorities in Malaysia decided to give the leadership of the assessment to the Central Bank of Malaysia, because the Central Bank heads the secretariat of the National Coordination Committee to Counter Money-Laundering and, consequently, leads the national risk assessment.

2.3 Information-sharing and data protection issues

All participating organizations should be able to share potentially sensitive information. If this is not the case, the effectiveness of the risk assessment will be affected.

The key competent authorities involved in the terrorist financing risk assessment should be authorized to communicate any information while being exempt from all applicable rules on official secrecy.

Partners having security clearance could help to improve and guarantee an effective sharing of relevant information.

Agreed procedures should apply to the exchange of information. It is better to have a clear and prior agreement on which kind of information could be exchanged between participating organizations working on a terrorist financing risk assessments.

It is also important that all the participating organizations clearly know that the information obtained may not be disseminated without the prior consent of the other participating organizations.

If such principles are respected, problems of data protection could be circumvented.

Inside the working groups contributing to the risk assessments, senior officers could be appointed to oversee the assessment and ensure information are shared and undertakings are honoured.

In Italy, the authorities represented within the Financial Security Committee communicate any information and are exempt from all applicable rules on official secrecy. However, all the information acquired by the Committee during the terrorist financing risk assessment process is covered by official secrecy.

To that end, before starting the risk assessment, the working group identifies and the actors who can contribute to risk analysis consider whether there are any limits to the exchange of relevant information between these actors.

Source: Italy

Terrorist financing risk assessments always contain sensitive information that countries do not want to share with all the recipients of the money-laundering risk assessment (the reporting entities, their supervision authorities and self-regulatory bodies).

It is very important to overcome intelligence and operational sensitivities that can restrict the sharing of information.

Joint training sessions, attended by several national agencies, on joint case files investigations and/or on information-sharing among competent authorities could slightly improve and enhance national coordination and information-sharing inside the working group dedicated to the terrorist financing risk assessments. Such training sessions help to build trust between people and partners who will later on have to work together on the risk assessments.

It is also important for managing the understandable tendency of "frontline" staff diverting their attention towards operational priorities at the expense of contributing to assessments.

Information-sharing within the risk assessment working group took place through several meetings and exchange of documents between the partners.

Ad hoc request for specific data and information, as well as the collection and sharing of information could be dealt with through regular communications via emails and face-to-face discussions.

Where the financial intelligence unit is the lead agency for the terrorist financing risk assessment, it could be important that all relevant domestic agencies should be represented in the board of the financial intelligence unit.

It is mandatory to discuss financial intelligence unit terrorist financing cases in a small restricted committee with representatives from all competent authorities in charge of fighting terrorism and terrorist financing: police, ministry of justice, ministry of interior and the financial intelligence unit.

However, the sharing and processing of personal data during the risk assessment is not an absolute requirement.

As explained below, the working group involved in the terrorist financing risk assessment of Belgium was denied access to and exchange of information on real case files. The European Commission worked with sanitized information and did not exchange information protected by the secrecy principle of ongoing criminal investigations.

For the terrorist financing risk assessment workshops, during the threat (modi operandi) assessment stage, only member State experts with the right and sufficient security clearance were invited.

Exchange of information, data protection and security clearance

For the supranational assessment, the European Commission did not collect information on money-laundering and terrorist financing cases involving named persons, but relied on public source information to have illustrative evidence (e.g. serious and organized crime threat assessment report, available threat assessments, FATF reports on ISIL financing, open source information). The Commission did not process personal data during the process. The Commission relied on member State experts to provide sanitized and anonymized information in an aggregated format. When member State experts needed to share operational information to illustrate their assessment, that information exchange was classified, and ultimately the Commission collected the outcome of the assessment, not the underlying operational information.

There was a project group within the Commission working on terrorist financing risk assessment. It regularly exchanged information.

Relevant experts from member States, European Union agencies and Commission services have been invited to discuss and share information during meetings. This sharing of information during workshops made it possible to work in an interactive way.

(continued)

The Commission organized classified meetings to share information on terrorist financing. Experts participating in those workshops had to hold a security clearance. The exchange of information was subject to restrictions applicable to classified information. The only challenge was that certain member State participants could not participate or contribute to the sharing of classified information, because they did not hold the requisite security clearance.

The supranational risk assessment workshops on terrorist financing were subject to higher security measures than those for money-laundering. The first two workshops for listing terrorist financing modi operandi and analysing the terrorist financing threat were classified. Those meetings took place in the Commission secure zone, and security clearance was necessary and dissemination of certain documents restricted. Similarly, information provided by the European Union Intelligence and Situation Centre for money-laundering and terrorist financing was classified.

Source: European Commission

2.4 Involvement of FATF-style regional bodies or the Egmont Group

Many countries use the methodology developed by the World Bank and receive the assistance of the World Bank to develop their own risk assessment. This is the case for the terrorist financing risk assessment of Morocco, which uses the World Bank risk assessment tool.

Other countries received assistance or consulted their FATF-style regional bodies, as in the case of Australia. The financial intelligence units of Australia and Indonesia consulted APG during the development of the regional risk assessment, and are doing likewise with the current regional assessment of non-profit organizations.

Other countries envisage to present their experience and the conclusion of their national risk assessment to their respective FATF-style regional body or to the Egmont Group once their national risk assessment is completed (Morocco intends to present the conclusion of its terrorist financing risk assessment to Middle East and North Africa Financial Action Task Force and the Egmont Group).

However, to date, according to the replies received to the questionnaire sent after the expert group meeting on the identification of good practices on terrorist financing risk assessments, FATF-style regional bodies and the Egmont Group have not yet been involved in a large number of terrorist financing risk assessments, which remain a national competence of their member States.

Nevertheless, the involvement of FATF-style regional bodies to coordinate and help in regional terrorist financing risk assessment is a best practice that has been suggested during the expert group meeting on the identification of good practices in terrorist financing risk assessments, held in Vienna on 4 and 5 April 2018.

2.5 Public-private partnerships

All domestic agencies dealing with the fight against terrorism and terrorist financing need to be involved in the risk assessment through meetings, questionnaires and discussions.

It is also important to involve the private sector partners early on and to maintain a close relationship with them throughout the risk assessment process.

As mentioned below, continuous engagement sessions are important to improve public-private partnerships.

Malaysia will engage the private sector, such as the financial institutions, through a compliance officer's networking group whenever matters arise that need to be discussed.

The compliance officer's networking group comprises financial institutions' compliance officers from the banking and insurance industries.

In Belgium, the private sector was involved in the money-laundering vulnerability assessment through its supervision and control authorities.

The results of both risk assessments will be shared with the private sector (compliance officers of the reporting entities).

Chapter 3

Timeline

A national risk assessment, regional risk assessment or a supranational risk assessment requires significant investments in time and resources, mainly when a given country, region or supranational territory commits to the risk assessment for the first time. Updates will be less time-consuming.

Until now, only a few countries have updated their risk assessment. This section is based not only on the experience of the countries participating in the expert group meeting on the identification of good practices in terrorist financing risk assessments, held in Vienna on 4 and 5 April 2018, but also on assumptions made by countries on how and when they will update their risk assessment.

Most countries need between one and two years to finalize a risk assessment. Only a few countries finalized their risk assessment in less than 12 months.

This timeline will necessarily have an impact on a given country's capacity to determine a reasonable frequency for updating the assessment process.

In many countries, the legal framework in place provides for an update of the risk assessment after two years. This is also the timeline the directive (EU) 2015/849 determined for the update of the European Union supranational risk assessment (money-laundering or terrorist financing).

In Malaysia, the national risk assessment is based on a three-year cycle. However, the assessment will be continuously updated to respond to any emerging risks.

The risk assessment must be conducted on an ongoing basis and must be kept up to date. The terrorist financing risk assessment should be continuously updated to respond to any emerging risk. Continuous involvement of different parties of the public and private sectors is important to ensure the risk is recognisable by the country.

The frequency of an updated risk assessment depends on the country and how quickly and significantly the risks may change.

A two- or three-year update cycle is common, while countries update the risk assessment when required if shifts in the risk environment warrant doing so or if the circumstances of the country risks require such regular updates, because of the existence of high-risk environments or changing and emerging risks.

Updates could be shortened if there is little change in risks or if the risks changed in a few areas where updating is required.

A national risk assessment, regional risk assessment or supranational risk assessment is a heavy investment in time and resources. They could be updated by including additional information gathered from controls conducted by supervisory authorities or from sectoral terrorist financing risk assessments, rather than by starting a new assessment.

The time and effort of all those involved in conducting a national risk assessment, and particularly a regional risk assessment or supranational risk assessment, need to be taken into account. This is particularly important for keeping key contributors (who are often very busy operational staff) engaged.

The updating process depends on the country's circumstances and exposure to terrorist financing risks.

Terrorist financing risks could evolve rapidly in certain countries and, consequently, when new risks emerge, regular updates will be important. On the other hand, in other countries, risks evolve slowly and updates of the risk assessment every two or three years will be enough, unless new significant terrorist financing risks arise between two updates.

Except in dynamic high-risk environments, enough time needs to elapse for changes or emerging risks to appear. Alternatively there would be merit in one- or two-year updates that can be short if little change in risk has occurred, or if risk updates are required in a limited number of areas only.

Nevertheless, some countries decided to update their risk assessment after a longer period of time, with safeguards in case of emerging new risks.

Experience of Italy

In Italy, in accordance with the methodology, the assessment is updated for the first time after three years, and then every five years in order to take into account the evolution of the community and national regulatory frameworks, as well as indications arising from supervisory authorities, investigations carried out by police forces and analysis made by the financial intelligence unit.

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

Following the increasing threats of terrorism and terrorist financing in Europe, Italy reassessed the terrorist financing threat in 2016 and published the analysis in the context of the annual report to Parliament.

Source: Italy

Experience of Turkey

Turkey produced an action plan signed by the Prime Minister in order to carry out the national risk assessment process across the country, which includes the main steps taken and the timeline for those steps. Accordingly, Turkey will have drafted a national risk assessment report by the end of 2017.

According to the action plan, as Turkey assesses risks on an ongoing basis, its financial intelligence unit is responsible for keeping the national risk assessment report updated. The frequency with which a risk assessment is updated will be determined by the country's financial intelligence unit, based on a number of factors, including how quickly and how significantly the risks may change.

Source: Turkey

A good practice is to continuously update the terrorist financing analysis, taking into account current terrorism and terrorist financing threats, through the investigations/studies conducted by law enforcement agencies and competent national authorities, paying special and continuous attention to these uses.

Continuous engagement with the authorities and enforcement agencies is important.

In Malaysia, these are driven by the National Coordination Committee to Counter Money-Laundering to ensure that the country has coordinated initiatives and responses to evolving threats.

Timeline and updating

In practice, the first supranational risk assessment takes almost two years, starting from scratch, if a due process is followed (involvement of different agencies, stakeholder's consultation, analysis, etc.).

The European Commission plans to update the supranational money-laundering and terrorist financing risk assessment every two years, except if exceptional circumstances require more frequent updates. In practice, permanent monitoring is needed. The risk assessment is a permanent process.

European Union legislation requires updates of the risk assessment at least every two years.

Source: European Commission

Chapter 4

Collection of data on threats

The collection of data is a key component of any risk assessment and needs to be properly monitored and reinforced, if required, when concrete, accurate and effective data are not available.

The starting point of the analysis is the collection of data and information, and the sharing of cases or typologies of criminal conducts identified by the police, the ministry of justice and the financial intelligence unit.

The reference period could be the last period for which data are available with regard to the different areas of analysis to ensure consistency in the ratings.

The mapping of the risks of money-laundering and terrorist financing requires availability of data from different sources, such as police forces, intelligence, financial intelligence unit, supervisory authorities within their competence fields, financial institutions and professionals, the ministry of justice, the national statistical institute and the private sector.

The data are normally collected by those authorities that are supposed to have them, among other things to prove their effectiveness in fighting terrorist financing and the predicate offences.

The sources of information of a risk assessment could be diverse and multiple: statistical reports, case studies, independent reports, perception surveys, expert views, and focus groups or engagement sessions.

Information could be public information (open source information) or more confidential information (intelligence collected by the intelligence services).

Data could be collected by sectors or by sources of financing of terrorism.

Limitations in data collection or the collection of inaccurate data can affect the quality of the risk assessment process.

As mentioned before, it is important that the working group develop a methodology for conducting the periodic national risk assessments, including a methodology to collect quantitative and qualitative data.

The working group needs to determine beforehand what parties need to be involved, because they can contribute to risk analysis, create a model or mechanism of identification of the terrorist financing threats and vulnerabilities, a way or mechanism to analyse the data collected and assess the terrorist financing risks.

Forms and procedures to collect the data are important, as well as the involvement of the private sector.

The Collection of data during the regional risk assessment on terrorist financing 2016 in South-East Asia and Australia

Two collection tools were used during the regional risk assessment to gather information from project participants and other experts in the region: a questionnaire and a terrorist financing assessment package.

Each participating financial intelligence unit completed a questionnaire, comprising a series of questions collecting quantitative and qualitative data on its own country's terrorist financing risk environment and measures to counter the financing of terrorism.

Each participating financial intelligence unit also completed a terrorist financing assessment package. The assessment package sought perspectives on current terrorist financing risks, as well as capabilities and vulnerabilities in countering terrorist financing in each country.

Respondents were asked to rate these factors on a scale of 1 to 9 (i.e. a sliding scale from low to medium to high).

Two regional in-country workshops (one in Medan, Indonesia, and one in Manila) were conducted to ensure analytical rigour and accuracy of assessment findings. Most participating financial intelligence units attended these workshops.

Structured consultations with a number of terrorist financing and industry experts were held to collect additional information, capture a wide range of intelligence, policy and supervisory perspectives and evaluate findings and judgements.

Source: Regional Risk Assessment on Terrorism Financing 2016 – South-East Asia and Australia

Open source information was also collected to validate findings and assessments, including a review of relevant publications produced by the FATF, APG and other top bodies.

Origin of data

Different kinds of information may be collected from different sources:[3]

- Judiciary-type information, both quantitative and qualitative, on significant investigations related to terrorist financing and criminal activities
- Financial estimates on proceeds from money-laundering predicate offences, as well as on money-laundering and terrorist financing
- Cases or typologies of criminal conduct identified by the police and the financial intelligence unit
- Information on obliged parties
- Information, both of a qualitative and quantitative nature in relation to the type, frequency and seriousness of the irregularities identified, processed by the relevant supervisory authorities on the basis of anti-money-laundering checks carried out
- Information on penalties imposed
- Information on the number and quality of suspicious transaction reports
- Qualitative and quantitative information on cooperation between national authorities and between those authorities and foreign authorities

[3] See footnote a.

The analysis of reports drawn up by international bodies, academic studies, and specialized press is also a key source of information of terrorist financing risk assessment.

Nonetheless, the collection of data is only the necessary starting point of a risk assessment.

Data need to be contextualized and interpreted by the working group (composed of experts) in order to properly identify, analyse and assess both threats and vulnerabilities.

More important is the analysis of the data collected to assess their accuracy, and to interpret them in the context of the country in question and the risk assessment.

Data can be collected in different ways and the data can come from different sources.

Open source information

Open source information could be used to validate and confirm the results of the national, regional or supranational threat assessment and to endorse the range of threats identified during the national, regional or supranational risk assessment.

Open source information could also be used when intelligence gaps exist.

It may happen that a source of funding is not identified by the risk assessment because law enforcement and intelligence services are not aware of their existence or do not know whether the country could be affected by this source of funding.

For that reason, open source information could also be used as a starting point of a risk assessment to feed a national, regional or supranational risk assessment, rather than as sources of information when intelligence gaps exist or when the competent authorities' only reply is that there is a known or unknown threat.

Many countries use open source information at the starting point of their terrorist financing risk assessment to ensure that all potential sources of funding of terrorism or all potential terrorist financing threats have been fully identified. Consultation of open source data could help law enforcement and intelligence services to identify sources of funding that previously went unnoticed.

News, independent views, research, local and international studies, interviews, questionnaires, and reports could be used as sources of information.

The collection of data during the European Union supranational risk assessment on money-laundering and terrorist financing 2017

The data were collected from regulators, law enforcement authorities, judicial authorities, financial intelligence units, supervising authorities, the financial sector, legal professionals and other designated non-financial businesses and professions, the gambling sector, NGOs, academics and consumer organizations through:

- Literature review as a starting point (FATF reports, risk assessments, open source information)
- Questionnaire for member States
- Written contributions and assessments

(continued)

- Specific requests to services (Europol, European supervisory authorities)
- Supranational risk assessment workshops to collect information

The European Commission collected statistics and quantitative data from member States and Commission services to analyse the size of the sectors and collected statistics on the regime to counter money-laundering and the financing of terrorism (see article 44 of directive (EU) 2015/849).

Finally, the Commission collected qualitative information in written formats (reports and contributions). However, the main qualitative substantive input came from the discussions in the supranational risk assessment workshops where member State experts shared information.

In the context of supranational risk assessment, data collection is particularly challenging. When the information is directly available to European Union institutions (Eurostat, market analysis by policymaking directorates general), the information can be more easily available and accessible wherever it exists. Where it is not, it is necessary to set up a data collection mechanism involving 28 member States, with various member State departments responsible for delivering the data. The Commission spent large amounts of time to define common templates and a first methodology for data collection by Member States to facilitate the comparison and compilation of data. Although necessary for supranational assessments, that exercise was resource intensive and challenging.

In the absence of reliable data, the Commission relied more on qualitative data provided by experts. In all cases, there should be no excessive reliance on quantitative data, which may bias judgment. Information on all relevant factors may not be expressed or explained in numerical or quantitative form, and there is a danger that risk assessments relying heavily on quantitative information may be biased towards risks that are easier to measure and discount those for which quantitative information is not readily available.

The data collected covers both source of terrorist financing (funding sources) and the channels and techniques used to fund terrorism.

The Commission services in charge of certain policy areas (development policy, humanitarian aid) provided information to consider the impact of measures to counter money-laundering and the financing of terrorism on those policy areas.

Source: European Union supranational risk assessment on money-laundering and terrorist financing 2017

Real case studies

The collection of data on real case studies is sometimes complicated because of the confidentiality of the criminal investigations and the refusal by law enforcement and judicial authorities to share data about ongoing investigations.

A good practice would be to overcome such difficulties and to share as many data and information as possible with all the stakeholders involved in the risk assessment. If this is not done, the results of the risk assessment may be biased.

The data available and utilized may be accurate, but their collection represents a necessary starting point for an analysis, as data need to be contextualized and interpreted by the working group of experts involved in the risk assessment in order to properly identify, analyse and assess both threats and vulnerabilities.

Quantitative data versus qualitative data

Qualitative data, including expert opinions, and quantitative data (statistics) are used in a risk assessment. Statistics are not always reliable by themselves, and the subjective opinions of experts are a must to help to analyse statistics.

Most countries indicated, during the workshop and in their replies to the questionnaire, that they use quantitative and qualitative data on the financing of terrorism, but also on terrorist acts in the country and in the region.

The collection of quantitative data also depends on the quality of the statistics available in a country, region or supranational territory.

Some countries indicated that the insufficiency or lack of statistics was a problem at the time of their risk assessment, or that the available statistics were not reliable enough to be used.

This creates a shortage of quantitative data that needs to be compensated by expert opinions.

Quantitative data are sometimes not available and the lack of quantitative data may bias the results of the terrorist financing risk assessment.

It is therefore important not to rely on quantitative data alone and to include qualitative data such as open source information, academic studies, expert judgements, any kind of intelligence, thematic assessments, typology studies, strategic analysis, regional or supranational risk assessment, private sector input, surveys, subjective information and perception indexes.

Malaysia: the national risk assessment is a combination of a quantitative and a qualitative assessment

The national risk assessment of Malaysia is largely a combination of a quantitative and a qualitative assessment.

- Quantitative statistical information is obtained from across key government agencies, supervisory and regulatory authorities, and law enforcement agencies, and used as part of risk indicators.
- The quantitative information is complemented by qualitative information sources such as perception surveys involving respondents from officers of the law enforcement agencies, reporting institutions and foreign financial intelligence units, intelligence insights, independent and external studies and public information on current and emerging threats, to form a consolidated picture of the country's terrorist financing environment.

Source: Malaysia

How to collect the data

In all countries, the collection of data on terrorist acts and their organizers is a process carried out by the ministry of home affairs and security, the relevant police departments and the intelligence services.

Standardized questionnaires, brainstorming workshops, specific workgroups, meetings and interviews are good means to collect information. The main information may be collected in written form and during the work groups and meetings. Owing to its sensitivity, some information may be exchanged orally and not in written form.

Law enforcement authorities also have access to information from Europol and INTERPOL that should be shared with the stakeholders and be included as a source of information on a country's, region's or supranational territory's terrorist financing threats.

Counter-terrorism information could also be shared on ad hoc basis and through relevant police information exchange systems such as INTERPOL and Europol.

In Italy, for instance, information from Europol and from the annual report to Parliament by the Department of Intelligence and Security has been used as a source of information on the terrorist and terrorist financing threats.

The Financial Security Committee membership of all relevant actors in the fight against the financing of terrorism ensures national coordination and access to relevant data. The private sector was not involved at that time. Italy is considering having a specific session with the NGO sector for the future.

The experience of Turkey in collecting data

Regarding the risk identification stage, Turkey focused on gathering quantitative and qualitative information, including operational data, such as the information on terrorist acts in Turkey and the region through consultation with stakeholders, questionnaires and the use of open sources. Turkey held many workshops, interviews and bilateral meetings with relevant stakeholders. The country reviewed academic studies on emerging terrorist financing risks.

Risk identification involves making judgments about threats, vulnerabilities and consequences. Therefore, given the challenges in determining or estimating the consequences of terrorist financing, Turkey is focusing primarily on achieving a comprehensive understanding of the threats and vulnerabilities.

The data collected were disaggregated, for example by the means of financing used, country of origin, terrorist groups, whether the terrorists were domestic or foreign.

Turkey has almost completed the data collection process and consultation studies with stakeholders have been going on to complement insufficient data and statistics and to address inconsistencies related to raw data.

The second stage is about analysing the data provided by all stakeholders to establish risks and understand their impact. At this stage, Turkey is working to establish its own risk rating model.

Source: Turkey

Authority to collect data

It is important to have the authority to collect data relevant to the terrorist financing threat and the vulnerability assessment from competent authorities. The authority coordinating the risk assessment must have enough authority over other participating organizations, otherwise those organizations could refuse to provide the information or will not communicate all the information they have.

The leading authority could be a ministry, and in this case its minister could oblige other participating organizations to deliver the requested information.

The national legal framework could also clearly stipulate that the participating organizations must communicate all the information they have to the leading authority and the national risk assessment working group.

The example of Turkey

The financial intelligence unit of Turkey has the authority to request any kind of information from all parties, including public institutions and organizations, natural and legal persons, unincorporated organizations and the private sector. Thus, for terrorist financing risk analysis purposes, Turkey did not encounter any problems during the collection of the relevant data.

Source: Turkey

Chapter 5

Cross-border risks

The cross-border risks should be identified on the basis of existing terrorism or terrorist financing cases and in publications on regional terrorist financing risks.

Countries assessed their border, their strategic geographic position and the controls in place. These are likely to affect a country's vulnerability to terrorism and terrorist financing activities such as:

- Movement of funds to support militants abroad
- Travelling of militants to and from a conflict zone, such as the Syrian Arab Republic

If a country, region or supranational territory is located close to a conflict zone or particularly affected by criminals or terrorist activities coming from such nearby zones, it is important to focus on understanding and analysing the cross-border risks, in particular with regard to the financing of terrorism.

The Turkey cross-border effect

Since Turkey's geographical position is very close to conflict zones, such as in the Syrian Arab Republic and Iraq, the country attaches great importance to understanding and analysing cross-border terrorist financing risks.

Information regarding cross-border risks (data, statistics, threats and vulnerabilities) was collected mainly from law enforcement authorities, including the customs administration and coast guard command. Law enforcement authorities were asked to share their risk analysis work with the financial intelligence unit so that it was able to a produce national and regional risk assessment.

(continued)

The country's authorities exchange information with their regional partners and counterparts in other countries. For instance, the financial intelligence unit exchanges and shares information through the Egmont secure web. In addition, the financial intelligence unit will benefit from the reports prepared by the FATF and Egmont Group in the identification of cross-border risks.

Source: Turkey

Certain international organizations collate statistics on these types of criminal activities.

Information on cross-border financial flows is also a valuable source of data that needs to be taken into account in a risk assessment and furthermore during a regional risk assessment.

In order to identify cross-border risks, countries could exchange information with regional partners as well as with Europol and INTERPOL and rely on the expertise of law enforcement agencies, representatives of financial intelligence units and interior ministries, which in turn exchange information with their international counterparts.

Seeking opinions through discussions with law enforcement is also an approach to cross-border risks.

It is important to exchange information with regional partners, neighbouring countries, law enforcement authorities or financial intelligence units.

Most of the participants indicated that they do not involve FATF-style regional bodies or the Egmont Group in the identification of cross-border risks or coordinating the regional risk assessment.

The consultation of FATF-style regional bodies and the Egmont Group in national, regional and supranational risk assessments should be encouraged because these bodies could have information on the cross-border risks and could assist countries in identifying cross-border risks.

FATF-style regional bodies could also take the lead in regional risk assessments.

Chapter 6

Potential change factors: emerging terrorist financing risks

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

Emerging terrorist financing risks are sometimes difficult to predict, and can certainly not be foreseen merely by looking at past trends or past terrorist financing risks, typology reports or by studying case files investigated by police or the financial intelligence unit.

In that regard, information obtained from open source studies, academic studies, non-governmental studies and institutions are very interesting, as they can provide input and confirm potential change factors and emerging terrorist financing risks.

As explained above, starting from open source research, not limiting the research to open sources from the country in question but broadening it to neighbouring countries, to countries presenting a similar level of development, countries with which the country in question has sizable commercial relations and international organizations is a way to include potential change factors and emerging terrorist financing risks into the terrorist financing risk assessment.

Identifying potential emerging terrorist financing risks is one step; assessing the probability of occurrence of the emerging terrorist financing risks in the assessed country is another.

The experience and knowledge of the experts nominated to deal with the terrorist financing risk assessment is important.

Each expert may rate differently the probability of occurrence of the terrorist financing emerging risks. Different views could be managed by averaging the experts' estimated probabilities of occurrence of the potential terrorist financing risks.

The strategic outlook of Australia

The strategic outlook is an assessment of the risk for each risk area over the next three to five years.

The outlook takes into account operational intelligence, current terrorist activity and predicted technological, market and other developments.

Risks that may change quickly or are highly likely to change over the next three years are assessed as dynamic or potentially dynamic.

Risks that are likely to remain unchanged or to change slowly over the next three years are considered stable.

Where there are significant intelligence and/or information gaps about low-level money-laundering threats, the outlook is considered undetermined.

Gaps in the intelligence and the often unpredictable impact of overseas events on the terrorism environment in Australia affect the effectiveness of the process aimed at detecting emerging terrorist financing risks.

Source: Australia

It is also important to review international trends, changes to the payment system, new financial technology that have the potential to change the risk profile and to gather information from the private sector and the civil society organizations.

Chapter 7

Priority actions

Impact of the legal framework

When assessing a risk and deciding about mitigating measures, it is important to acknowledge whether the existing legal framework is commensurate to the risks inherent to a specific sector or only marginally covers those risks.

The legal framework of a country is not static; it evolves during the risk assessment process, which could take one or two years.

The terrorist financing risk assessment provides a snapshot of the money-laundering and terrorist financing risks and requires clear-cut timing.

As explained below, the risks affecting the European Union were assessed at a time when the legislative framework was still directive 2005/60/EC. Although directive (EU) 2015/849 was adopted in May 2015, its transposition into the national legal systems of the member States had not yet been completed at the time of the risk assessment. Some member States had already implemented the new directive, others had not, which meant that different member States had different legal frameworks in place.

New legislation could enter into force during the risk assessment process or new legislative proposals affecting the counter-terrorist financing framework could be put forward and adopted while a terrorist financing risk assessment is in progress.

The priority actions need to take that into account, because a clear-cut timing is not possible when the assessment is a two-year endeavour.

A risk identified during the assessment process could already be under control by the time the assessment ends, because during the assessment process new legislative measures have been adopted or will enter into force soon.

(continued)

Results of the European Union supranational risk assessment

Through the implementation of the supranational risk assessment methodology and based on the internal and external input received, the European Commission has identified 40 products and services that are considered potentially vulnerable to money-laundering and terrorist financing risks at the level of the internal market.

These 40 products and services cover 11 professionals sectors, including:

- The sectors defined in directive (EU) 2015/849: credit and financial institutions, money remitters, currency exchange offices, high-value goods and assets dealers, real estate agents, trust and company service providers, auditors, external accountants and tax advisers, notaries and other independent legal professionals, and gambling service providers.
- Sectors outside the scope of the directive (EU) 2015/849 but nonetheless considered relevant for the risk assessment, such as the use of cash, virtual currencies, crowdfunding platforms and NGOs. Certain illegal means used by perpetrators such as Hawala and other similar informal value transfer services providers are also included.

The analysis was based both on quantitative data (statistics) and qualitative information (consultation of experts).

Risk mitigation

In determining the money-laundering and terrorist financing risk mitigating measures, the supranational risk assessment does not prejudge the mitigating measures that some member States are applying or may decide to apply in response to their own national money-laundering and terrorist financing risks.

They may therefore be implementing some of the recommendations already included in the supranational risk assessment, or have adopted stricter rules than the minimum rules defined at the level of the European Union.

The vulnerabilities mitigating measures identified in the supranational risk assessment report should therefore be considered a baseline that could be adapted, depending on the national measures already in place.

The risks posed by some high-risk non-European Union countries, the geographical risk analysis, was not part of the first supranational risk assessment, because the analysis of the risks posed by those jurisdictions is currently conducted in the context of a separate process.

Priority actions

The supranational risk assessment report contains two parts, one on risk assessment and one on mitigating measures. The unit in charge of carrying out the risk assessment was also in charge of preparing the mitigating measures to address the risks identified. Those mitigating measures have formally been adopted by the European Commission and an action plan been prepared to monitor the implementation of the different deliverables announced in the supranational risk assessment report.

When designing the mitigating measures, the European Commission had to balance necessity, proportionality and adequacy with fundamental rights and data protection.

The impact of the various options to address the risks identified were assessed internally. As with an impact assessment, the Commission looked at various options regarding the status quo, self-regulation, soft law and regulatory measures (targeted measures up to far-reaching measures and prohibitions), and decided to retain the mitigating measures, which showed the best cost-benefit ratio, considering the balancing exercise and potential impact.

Member States have to implement the recommendations issued by the European Commission on a comply-or-explain basis.

The implementation of the action plan will be assesses as part of the next supranational risk assessment report, in 2019.

Types of action taken

Action to mitigate vulnerabilities could consist of new legislation, new rules or new country-wide or sectoral regulations, which could include the application of measures to prevent the financing of terrorism to new sectors identified during the risk assessment process as presenting a high risk of money-laundering or terrorist financing.

In Lebanon, a risk-based action plan was designed after finishing the national terrorist financing risk assessment. The national policies and the priority actions designated to serve as risk mitigation measures were clustered according to the following needs: amend an existing law, enact new legislation, amend an existing regulation or executive order, issue a new regulation or executive order, allocate additional resources to a certain high-risk area, highlight the high-risk area to the relevant authority to allocate resources, strengthen inter-agency coordination, strengthen controls and increase awareness at reporting entities.

Source: Lebanon

The impact on the private sector and civil society of the measures identified in the priority action plan needs to be assessed to ensure that the burden is commensurate with the risks identified.

The action plan should also be implemented in a manner that respects the obligations of the country in question under international law, including human rights law (e.g. non-discrimination and equality).

Affecting and allocating resources

Some measures require the allocation of financial and human resources.

As resources are limited, a risk-based approach needs to be applied.

As explained below, rating and weighting the extent of the different risks to assist with prioritizing mitigation efforts is important when resources are limited.

Responsibilities

The working group preparing the risk assessment or the national counter-terrorist financing coordination committee(s) must consider how to use the results of the risk assessment to guide policy decisions and resource allocation, and must consider how financial institutions and other obliged entities could use the results of the risk assessment in support to their specific business risk analysis.

The implementation of policy decisions and resource allocations require commitment at a high level.

The endorsement of the risk assessment conclusions and the adoption of the proposed mitigating measures or the action plan by the prime minister, the Government as a whole or the parliament is a pledge to make the implementation a success.

Regular reporting to the parliament on the implementation of the action plan and the results obtained could also contribute to the success of its implementation.

The results of national terrorist financing risk assessments will provide valuable input in the formulation or calibration of national policies and action plans to counter the financing of terrorism, but may also affect a number of competent authorities and the manner in which they carry out their responsibilities.

When implementing the priority action plan, countries taking part in the expert group meetings indicated that they had faced the problem that various agencies and competent authorities involved in the risk assessment had different priorities.

A commitment at a high level could help to solve the problems resulting from those different priorities.

The action plan of Italy

In Italy, with regard to prevention and investigation, in order to mitigate regulatory vulnerabilities, some effective operational solutions were highlighted in the conclusions of the national risk assessment. For example, to mitigate specific risks, the Financial Security Committee took into consideration ad hoc safeguards to counter the financing of terrorism and adopted a plan. Competent authorities have also to report to Parliament on the preventive action taken in the framework to counter money-laundering and the financing of terrorism. The risk-based approach was used in Italy even before the FATF standard determined this to be a key element effectively combating the financing of terrorism.

Source: Italy

The action plan of Malaysia

The action plans are incorporated into the national strategy to counter money-laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction for the period 2015–2020 to address findings and gaps identified through the risk assessment process, the mutual evaluation report 2015 and other domestic needs.

The national strategy is endorsed by the National Coordination Committee to Counter Money-Laundering, with the Central Bank of Malaysia acting as its secretariat. It coordinated and followed- up on the progress of the action plans with the relevant enforcement agencies through the relevant subcommittee formed under the Committee.

The action plans will be carried out by the respective authorities and enforcement agencies. The implementation will be monitored by the relevant subcommittee of the National Coordination Committee. The subcommittee will provide periodic updates to the Committee.

The plan also considers the impact on the private sector and civil society. Feedback on the implementation of the risk-based action plan from the private sector and civil society were obtained through engagement and communication with the sectors.

Source: Malaysia

Chapter 8

Sharing the terrorist financing assessment results

The assessment output consists of a document for authorities and competent administrations on countering the financing of terrorism.

The working group involved in the preparation of the document must determine which parts or results are to be shared with the private sector (industry associations and professional associations), so that the competent authorities and obliged parties or entities will have information relevant to the risk assessment.

A specific objective of the terrorist financing risk assessment is to provide information to the public in order to enhance the general understanding of government counter-terrorist financing initiatives. A typical output of a national terrorist financing risk assessment should be a public document.

In accordance with the FATF recommendation, countries have to share the results of their risk assessments, and many countries have done so with at least the supervisory authorities and the compliance officers of the reporting entities.

Italy: the Financial Security Commission published an abstract of the national risk assessment

A sanitized version of the national risk assessment was necessary to keep certain information about investigations and/or confidential analysis confidential.

(continued)

The conclusions and the priority actions to be taken were published and the main findings were presented at the Ministry of Economy and Finance. All public and private actors involved in the national risk assessment, which concerned both money-laundering and terrorist financing risks, attended.

Furthermore, to raise awareness among the sectors involved, each authority concerned organized a sectoral forum. The abstract is also available on the Ministry's website.

Italy reports annually to Parliament on the preventative action taken to counter money-laundering and the financing of terrorism.

The report is public and available on the Ministry's website. It also serves as an information tool for the private sector. It is also a very helpful tool that Italy uses to raise awareness in the private sector.

Source: Italy

Sharing the terrorist financing assessment results

The European Union supranational risk assessment report is available to the public on the website of the European Commission and on the European Union law portal. The Commission defined a dissemination strategy by:

- Sending out a press release
- Sending out an email to all experts and civil society representatives who participated to the process
- Printing 300 paper copies of the report (disseminated to relevant experts and civil society representatives)
- Holding follow-up meetings

The European Commission is considering holding a conference on countering money-laundering and the financing of terrorism.

Source: European Commission

In other countries, the decision was made to limit the amount of information made public about national deficiencies in making mitigating measures more effective.

The experience of Lebanon with sharing the results of its risk assessment

In Lebanon, the decision was taken not to make public the national risk assessment or information about the country's deficiencies in countering money-laundering and the financing of terrorism.

Lebanon took the approach of taking risk mitigation measures without publicly admitting the country's shortages and vulnerabilities and without announcing the implementation of mitigation measures.

Lebanon preferred to direct additional resources where they were needed and alert reporting entities to money-laundering and terrorist financing risks during training events, via anti-money-laundering and counter-terrorist financing compliance examinations and at meetings, by enacting legislation and issuing regulations, by sharing findings with relevant authorities on a need-to-know basis without alerting the criminals involved in money-laundering and the financing of terrorism.

The decision taken by Lebanon was the result of country-specific circumstances such as the refugees situation and political deadlock, which at times causes delays in certain risk mitigation measures being taken.

Source: Lebanon

Regarding the regional risk assessment on terrorist financing 2016 in South-East Asia and Australia, a regional counter-terrorist financing summit was held in 2016 to discuss the priority actions to be implemented at regional level.

In the European Union, the results of the supranational risk assessment and the recommendations put forward by the European Commission at the end of the risk assessment process (action plan) was communicated to the European Union member States.

Member States have to report to the Commission on the implementation of the recommended actions.

They have to justify to the Commission why they do not apply the recommendations made by the supranational risk assessment.

In Malaysia, the national risk assessment 2013 was presented to the Economic Council, which is chaired by the Prime Minister, and engagement sessions with members of the National Coordination Committee to Counter Money-Laundering and through an engagement session.

Source: Malaysia

Turkey: Sharing the national risk assessment with the public and private sectors

Turkey produced a non-classified version of its terrorist financing risk assessment because the information in the national risk assessment is derived from classified or sensitive sources.

Once the national risk assessment was completed, public authorities were informed through the sharing of information within the working groups created to assess the threats and vulnerabilities.

In addition, appropriate information from assessments will be made available to the private sector to assist it in addressing the current risks. New and emerging threats will be shared through the website of the financial intelligence unit of Turkey and also within the working groups.

With regard to the sensitive information that is not subject to a broad distribution, sanitized information and summaries, including information on the methodology used, as well as the findings and the conclusions will be circulated through the website of the financial intelligence unit and within working groups.

Source: Turkey

Chapter 9

Evaluation

Participants in the expert group meeting on the identification of good practices in terrorist financing risk assessments who completed the questionnaire provided very little information on how to evaluate the effectiveness of their risk assessment and the effectiveness of the priority actions and strategies decided on the basis of the results of the risk assessment.

The identification and understanding of national terrorist financing risks and the obligation to conduct terrorist financing risk assessments are very new obligations added only in the FATF standards of 2012. These new obligations appeared for the first time in the FATF recommendations of February 2012, while many countries finished their first terrorist financing risk assessments only recently. In many other countries, the first terrorist financing risk assessment is still ongoing.

Nevertheless we can suggest a few techniques to evaluate the quality and effectiveness of the risk assessment and priority actions and strategies.

Countries may use:

- A validation process conducted by experts from focus groups of members of the public and private sectors and experts from academia, who could give their advice on the national risk assessment findings
- A national risk assessment assessed by FATF during a country's mutual evaluation

The effectiveness of the risk assessment could also be evaluated on the basis of a rise in the number of terrorist financing convictions and of improved inter-agency coordination on terrorist financing cases.

Report and feedback by European Union member States

The report on the European Union supranational risk assessment analyses the risks of money-laundering and terrorist financing the European Union could face and proposes a comprehensive approach to addressing them.

The report presents the main risks for the internal market in a wide range of sectors and the horizontal vulnerabilities, which can affect such sectors. On that basis, the report presents the mitigating measures that should be pursued at European Union and national levels to address those risks and puts forward a number of recommendations for the actors involved in the fight against money-laundering and terrorist financing.

In the conclusion of the supranational risk assessment, the European Commission made recommendations about appropriate measures its member States should take in order to mitigate the risks identified.

Member States must also take into account the results of the European Union supranational risk assessment for their own risk assessments.

Under article 6 of directive (EU) 2015/849, member States that decide not to apply any of the suggested recommendations in their national anti-money-laundering and counter-terrorist financing regimes are required to notify the Commission of their decision and provide a justification for it ("comply or explain").

Source: European Commission

Chapter 10

Suggested good practices

Members of the expert group meeting on the identification of good practices in terrorist financing risk assessments, which was held in Vienna on 4 and 5 April 2017, identified a range of good practices in terrorist financing risk assessments.

Prevailing legislation

- Start by ensuring that prevailing legislation covers all aspects of the terrorist financing offence as per international standards.
- Have a good overview of the legal framework existing in a given country and the new legal provisions adopted during the risk assessment process or about to be adopted. These elements are important when determining the new measures the country will require.

High-level commitments

- Have a high-level commitment from the prime minister, the Government and/or the parliament to support the risk assessment process and to endorse the results of the risk assessment and the priority action plan. The high-level commitment could be useful in resolving differences in priorities between various competent agencies.
- Establishing a body of senior officers to oversee and coordinate an assessment can help to ensure that higher-level policy and strategic factors are taken into account. This is important for ensuring that assessments focus on the wider picture and not just more detailed aspects such as cases, typologies and indicators. Senior officers can also step in to remove blockages that assessments can face, in particular failures to share sensitive intelligence that can often occur often in matters relating to terrorist financing. A body of senior officers can play an important role in translating risk assessment findings into policy, legislative change and operational priorities.

Terms of reference

- Collect and review methodologies developed by Member States and international organizations in order to identify good practices.
- Choosing your terms carefully is essential for dealing with terrorist financing risk. It is where standard risk models may at times need to be tailored and re-thought.
- Risk assessment tools should be used flexibly and tailored to a country's circumstances.
- Include sectoral risk assessment and interconnectedness between crimes and sectors.

Engagement with relevant stakeholders

- Engage with all relevant stakeholders, including law enforcement agencies, regulators, the private sector and non-profit organizations.
- Include the largest possible number of experts from different sectors and from the private sector. The involvement of the supervision authorities and partners from the private sector is important when dealing with the identification of vulnerabilities.

Terrorist financing risk assessment working group

- Have a competent authority (or a mechanism) responsible for coordinating the terrorist financing risk assessment.
- Provide enough powers to that competent authority for coordinating the terrorist financing risk assessment.
- Powers are needed to obtain the information necessary to properly manage the assessment.

Lead agency

- The lead agency could be the financial intelligence unit, but it is not an obligation. Financial intelligence units have knowledge of the detected flows of terrorist financing resulting from the analysis of the terrorist financing suspicious transaction reports received.
- Choose the agency with the best operational and strategic knowledge of terrorism and terrorist financing activities.
- If the financial intelligence unit is the lead agency for the terrorist financing risk assessment, it could be important that all relevant domestic agencies be represented in the board of the financial intelligence unit.

Trust

- Building trust between partners is important. The trust could result from partners meeting together on a regular basis, from partners being members of common working groups or national counter-terrorist financing or security committees meeting on regular basis, or from partners participating together to joint training sessions.
- Face-to-face meetings are important to build trust between partners and stakeholders.
- Work with staff that have the appropriate security clearance who can exchange sensitive information when needed, or create a trusted environment for information-sharing.

Quantitative data

- Ensure that a given country, region or supranational territory has enough reliable statistics.
- Statistical data are not a panacea. Statistical data need to be contextualized and interpreted by the working group involved in the terrorist financing risk assessment in order to properly identify, analyse and assess threats and vulnerabilities.
- Do not rely too heavily on quantitative data, because they may bias judgment. Not all relevant factors can be expressed or explained in numerical or quantitative form, and there is a danger that risk assessments relying heavily on quantitative information may be biased towards risks that are easier to measure and discount those for which quantitative information is not readily available.
- When statistics are not reliable on their own, subjective opinions from experts are a must to help to analyse statistics.
- Heavy quantitative approaches can result in confirmation bias. Qualitative analysis can be general, vague or overly influenced by current priorities.
- Data gaps are common and require qualitative methods to fill particularly good judgement and analytical reasoning.
- Improve statistical data collection on counter-terrorist financing by collecting, consolidating and analysing statistics provided by European Union member States. Having relevant, reliable and comparable quantitative data at European Union level is recognized as necessary to contribute to a better understanding of the risks.
- Ask that quantitative data be compiled in the future when a given country, region or supranational territory lacks of reliable statistics.

Collection of data

- International typologies should be used as a starting point for comparison and contrast, rather than used as a default to where intelligence gaps or "known unknowns" exist.
- The sharing of real case studies, even those of ongoing criminal investigations, should be encouraged and the barriers to such exchanges of information should be overcome.
- Carry out a questionnaire, at the start of the project, to identify practices in Member States conducting national risk assessments in order to identify good practices.
- Carry out a specific terrorist financing analysis, not only a joint analysis of money-laundering and terrorist financing to cover scenarios specific to terrorist financing and not considered relevant to money-laundering (e.g. consumer credit and non-life insurance).
- Correctly interconnect terrorist financing and money-laundering risk assessments so that they can benefit from each other.
- The analysis must be relevant in the sense that it identifies sources of funding, in particular sources of funding linked to fraud misusing the financial system for terrorist financing purposes.

Overcome barriers to exchanging data

- Overcome barriers to exchanging information by increasing the trust between the partners involved in the risk assessment.
- Agreed procedures should apply to the exchange of information.

- All the participating organizations must clearly know that the information obtained may not be disseminated without the prior consent of the other participating organizations.
- Clearly and previously agree on what kind of information may be exchanged between participating organizations working on the terrorist financing risk assessments.

Involvement of FATF-style regional bodies

- The consultation of FATF-style regional bodies and the Egmont Group in national, regional and supranational risk assessments should be encouraged because those bodies may have information on the cross-border risks and may assist countries in identifying cross-border risks.
- Encourage FATF-style regional bodies to take the lead in terrorist financing regional risk assessments.
- Create focus groups with partners from various countries and various competent authorities to analyse the current regional circumstances and threats and the cross-border terrorist financing risks.

Validation

- Have the results of the risk assessment validated by private sector and academic experts if the sensitivity of the information permits doing so.
- Involve civil society beyond the scope of obliged entities to associate sectors possibly at risk of terrorist financing but not yet regulated, such as virtual currency exchange platforms and wallets, and crowdfunding platforms.
- Involve academia and NGOs to have a more comprehensive and richer analysis by bringing an external perspective. Also, NGOs may flag issues that are not always escalated by regulators or private sector actors. Work with staff that have security clearance so that they can exchange sensitive information when needed, or create a trusted environment for information-sharing.
- Avoid working in silos; putting regulators, law enforcement, financial intelligence units, supervisors and other practitioners in the same room allows for the creation of common understanding.

Action plan and mitigating measures

- Develop an action plan based on the terrorist financing risk and adopt mitigating measures based on the results of the national, regional or supranational terrorist financing risk assessments.
- Obtain a high-level commitment (prime minister, Government, parliament) when implementing the action plan and the mitigating measures.
- Clearly specify the responsibility of each competent authority responsible for implementing the risk-based action plan and the mitigating measures.
- Supervise the implementation of the mitigating measures. Have an authority with enough power to implement the risk-based action plan and the mitigating measures.
- Impose the submission of progress reports on the implementation of the action plan and the mitigating measures to the parliament or to the committee for coordinating and cooperating on countering terrorist financing.
- Ask each competent authority to provide regular feedback about the implementation of the action plan and the mitigating measures.

Publishing the results of the terrorist financing risk assessment

- Make the terrorist financing risk assessment available to all competent national authorities, supervisory authorities and reporting entities to help them to develop their own terrorist financing risk assessment.
- Not publicly publishing the full terrorist financing risk assessment report could improve and increase the effectiveness of the mitigating measures implemented on the basis of the conclusions of the risk assessment.

Update

- Update the terrorist financing analysis continuously, taking into account current terrorism and terrorist financing threats, through investigations and studies conducted by law enforcement agencies and competent national authorities, paying special and continuous attention to such phenomena.
- Update the risk assessment on a regular basis (every two to three years) and whenever new terrorist financing risks emerge.

Chapter 11

Conclusions

Strategies to counter the financing of terrorism must mirror and constantly take into account the threat, its changing nature and level of gravity. To ensure that the strategy and the threat are coherent and complementary, it is recommended that the experts conducting national terrorist financing risk assessments are the same as those who develop the general strategy to counter terrorism. The creation of a holistic committee for countering the financing of terrorism, built on national models, in which law enforcement agencies, ministries and other relevant institutions are present, can be a viable alternative, as it allows for continuous and regular assessments of the threat level.

National risk assessments, along with all the efforts invested in combatting the financing of terrorism, remain inefficient without a strong political commitment throughout the process. Solid political support must be present from the start of the exercise, continuing throughout the drafting and finalization of the report all the way to implementation. A thorough understanding of the problem at a high political level is paramount to the production of a positive and effective outcome.

As far as the other entities involved are concerned, the establishment of efficient coordination and cooperation mechanisms among financial intelligence units, law enforcement entities and intelligence services is crucial. Without the regular and active contribution of intelligence, the production of solid and important results would be hindered considerably. The access financial intelligence units have to up-to-date information and the crucial tools they have at their disposal makes the active involvement of financial intelligence units an invaluable asset to the overall exercise.

In the presence of various contributing actors, appointing a lead agency for the development of risk assessments is also crucial.

The lead agency does not necessarily have to be the financial intelligence unit (especially if the focus lies on subregional terrorist financing risk assessments), but the determining factor in designating the lead agency is its level of experience in the field of terrorism and terrorist financing and of the commitment and management capabilities of the head of the agency. A representative figure is needed who can communicate and, if necessary, create a more formal mechanism to engage with all the relevant entities, including the private sector, and establish strong and sustainable communication channels.

As far as the methodology employed is concerned, the collection of information should rely on a multitude of sources: international sources, public sources and, to an important extent, classified information. When dealing with suspicious transaction reports, it must be noted, without compromising their importance, that transactions related to terrorist financing are also done outside of the banking system. Therefore, suspicious transaction reports may not always offer leads to the networks behind terrorist groups or organizations, nor to the sources of the threat. It is therefore necessary that the analysis include, for example, cooperation with customs authorities, as they have an overview of the incoming and outgoing flows of money and goods. Once sensitized to the threat, they can offer important contributions and insights into the types of declarations sought and share their experience and the patterns they are finding.

Having access to this type of information contributes to the overall precision and success of the exercise, as it is fundamental to identifying the vulnerabilities on which the recommendations could focus.

Alongside international cooperation, it must also be stressed that subregional, regional or supranational cooperation can bring many advantages. It can respond to the common characteristics belonging to a group of countries from a particular geographical area . Such similarities would facilitate the exchange of knowledge and experience and encourage ownership at the subregional, regional or supranational level.

This kind of cooperation plays an important role in conducting efficient risk assessments at the national level, just as it is of equal importance in the wider context of international cooperation in the area of terrorist financing.

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-3389, www.unodc.org

V.18-03185