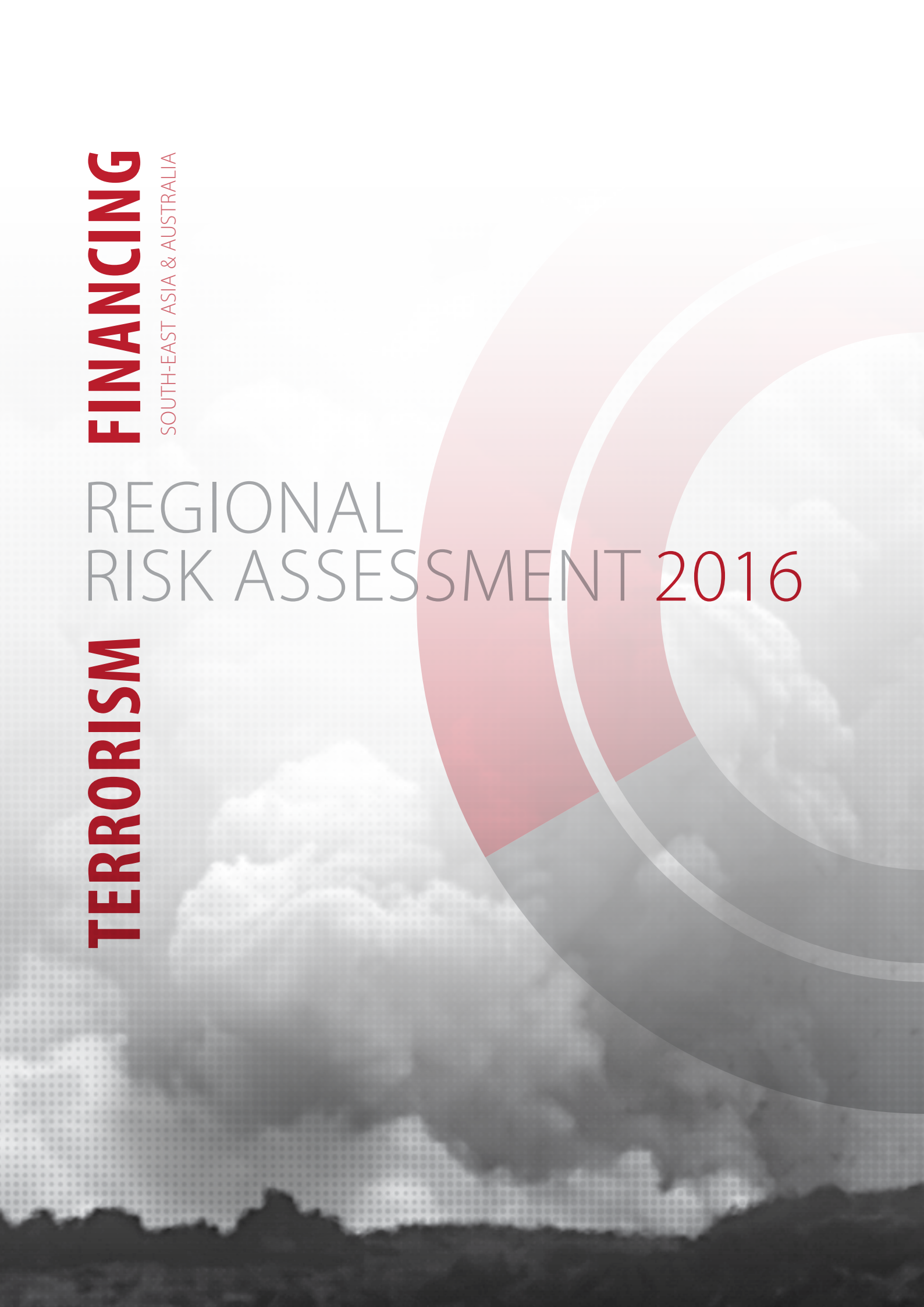
TERRORISM FINANCING

SOUTH-EAST ASIA & AUSTRALIA

REGIONAL RISK ASSESSMENT 2016



Contact us

For enquiries regarding the licence and any use of this report please contact AUSTRAC Media and Communications at media@austrac.gov.au.

You can also get a copy of this report from PPATK at: contact-us@ppatk.go.id

CONTENTS

KEY JUDGEMENTS

The Syria-Iraq conflict and the rise of the so-called Islamic State of Iraq and the Levant (ISIL)[1] have energised extremists and their sympathisers across South-East Asia and Australia. The region is also dealing with long-running domestic conflicts and insurgencies that share the characteristics of terrorism, even if they are not connected to ISIL or violent global extremism. This highly-charged and dynamic security environment has intensified terrorism financing risks in the region, posing new challenges for authorities.

Small-cell terrorist activity, foreign terrorist fighter travel and the growing number of lone actors will see continued use of self-funding to raise funds and cash smuggling to move them. These proven, easy-to-use terrorism financing methods reduce the need for terrorists and their supporters to resort to more complex financial activity or adopt new payment systems. The region's porous land and close maritime borders, as well as informal cash-intensive economies, also influence the continued use of established methods.

Terrorism financing funds flowing out of the region are currently channelled mainly into the Syria-Iraq conflict, but comprise only a small portion of international funding to factions fighting in that area. While outflows to foreign conflict zones pose a high risk, concern is growing over signs of funding entering the region to support local terrorist actors.

HIGH RISK

Regional countries assess self-funding from legitimate sources as high risk. For the majority it is the most commonly used method of raising terrorism funds across the region, particularly for foreign terrorist fighters travelling to or operating in conflict zones. Self-funding is highly likely to remain a key risk across the region over the next three to five years. Proactive detection of self-funding activities will remain difficult and financial intelligence units (FIUs) should focus on improving guidance to reporting institutions on customer risk profiles and suspicious financial characteristics.

While countries have identified only a small number of cases where non-profit organisations (NPOs) have been misused for terrorism financing, the risk is high due to the capacity of NPOs to raise large amounts undetected. The limited cases of detected misuse is at odds with the number of potentially vulnerable NPOs across the region, particularly those that receive funds sent from foreign regions or that send funds abroad or have links to conflict zones. Regional countries need to identify higher-risk NPOs and adopt targeted oversight and outreach to mitigate the risk of NPO misuse for terrorism financing.

The cross-border movement of cash is the highest-risk method of moving terrorism funds across the region. Porous land borders and close maritime boundaries allow extremists and terrorist networks in parts of the region to move funds across borders with ease. Poor visibility over cash smuggling routes compounds the problem. Border authorities also face challenges in detecting and stemming cash flows through regulated cross-border channels. Deeper cross-border and cross-agency ties are required to develop effective responses.

As a baseline assessment, countries assess that terrorism funds within the region are more likely to be used for operational rather than organisational expenditure – namely for personnel mobility and travel, and the purchase of weapons and explosives. Countries should continue to concentrate efforts on detecting and disrupting terrorist actors, groups and their financing methods.

MEDIUM RISK

Use of social media and crowdfunding platforms to raise terrorism funds in the region has been minimal, largely opportunistic and involves self-directed individuals as opposed to groups or networks. Stronger controls and targeted monitoring of online activity are needed to detect and reduce extremist messaging and fundraising.

Criminal activity is an important source of revenue for some terrorist groups in some regional countries. Countries need to improve the timely sharing of critical intelligence between national security and law enforcement agencies to detect and disrupt criminal financing of terrorism.

Banking and remittance sectors continue to be used to move terrorism funds within countries and to foreign regions. Terrorism funding through the banking sector is often small-scale and hard to distinguish from the volume of legitimate ordinary daily financial transactions. Authorities have some degree of visibility over remittance financial activity including international transfers where funds flow through bank channels. However, suspicious transaction reporting (STR) from remitters is generally lower than expected when considering the sector's high vulnerability to misuse. This problem, combined with the challenges the sector poses for regulatory oversight, raises concern that actual terrorism financing misuse of remitters may be higher than currently detected.

1 This assessment adopts the Financial Action Task Force's use of ISIL rather than Islamic State (IS) or Islamic State of Iraq and Syria (ISIS).

POTENTIAL

Two key potential changes could alter the regional terrorism financing picture in the future. These are:

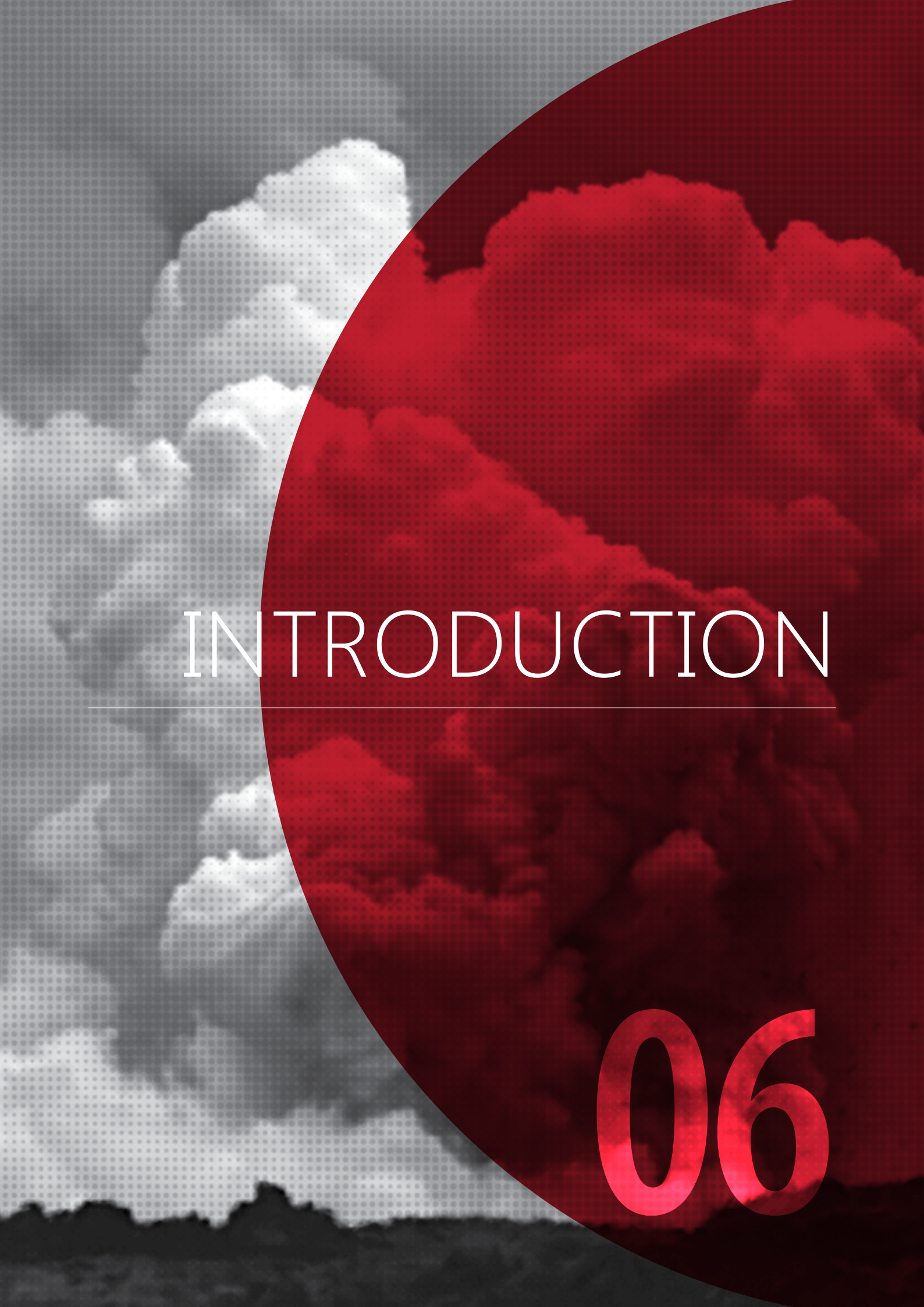
- A likely greater uptake of stored value cards and online payment platforms if detection and disruption of commonly used methods force a shift in financial activity.
- Increased funding into the region from foreign-based terrorist groups, particularly ISIL.

The largely unforeseen outbreak of the conflict in Syria and resurgence of fighting in Iraq with the rise of ISIL have had significant repercussions for not only the region's security environment but also the terrorism financing risks countries now face. FIUs and other intelligence agencies, on a country basis and regionally, need to improve warning capability to anticipate future strategic shocks and their effect on terrorism financing activity in the region.

RECOMMENDED PRIORITIES

Underpinning efforts to counter terrorism financing (CTF) in the region is an urgent need for deeper intelligence cooperation, strengthening domestic and regional frameworks and better understanding of high-risk terrorism financing channels. Based on the findings of this assessment, priority actions to address terrorism financing should focus on the following highest priority risks:

- self-funding from legitimate sources
- at-risk NPOs
- cross-border movement of funds/value
- external funding into the region.



INTRODUCTION

06

In response to a highly charged and dynamic terrorism environment, Indonesia and Australia recognised the important need to develop a deeper, shared understanding of the drivers behind terrorism financing in the region. The two countries' FIUs, AUSTRAC and the Pusat Pelaporan dan Analisis Transaksi Keuangan Indonesian (PPATK), co-hosted the first South-East Asia Counter-Terrorism Financing Summit. Held in Sydney in 2015, the summit brought together officials and international experts from multilateral organisations and 19 countries, including from outside the South-East Asia region.

"...THE WORK UNDERTAKEN FOR THIS ASSESSMENT HAS FOSTERED A GENUINE SPIRIT OF COOPERATION AND COLLABORATION AMONG PARTICIPANT COUNTRIES THAT WILL ENDURE WELL BEYOND PUBLICATION..."

A key outcome of the 2015 summit was agreement to conduct the first regional risk assessment of terrorism financing in South-East Asia to improve the intelligence picture of the heightened risk environment and guide the work of the 2016 summit in Indonesia. To that end, this assessment focuses on the terrorism financing methods and channels currently presenting the highest risks, as well as those forecast to pose increasing risks over the medium term (three to five years). These include channels that present joint country or intra-regional risks. This assessment also identifies priority areas where regional efforts could be focused to strengthen CTF capability and better mitigate terrorism financing risk.

This assessment is intended to inform responses to wider global terrorism financing issues under consideration by international anti-money laundering and counter-terrorism financing (AML/CTF) bodies, such as the Financial Action Task Force (FATF) and the Egmont Group of FIUs. As one of the first regional risk assessments of terrorism financing in the world, this assessment should also contribute to the refinement of analytical tools to better assess terrorism financing risk.

The work undertaken for this assessment has fostered a genuine spirit of cooperation and collaboration among participant countries that will endure well beyond publication. The strong informal networks forged through this process provide important ties for deeper intelligence exchange and will strengthen the region's capacity to proactively confront the challenges ahead.

The Regional Risk Assessment team comprised senior officers and intelligence analysts from the following FIUs:

- AUSTRAC, Australia
- Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) Indonesia
- Bank Negara (BNM), Malaysia
- Anti-Money Laundering Council (AMLC), the Philippines
- Suspicious Transaction Reporting Office (STRO), Singapore
- Anti-Money Laundering Office (AMLO), Kingdom of Thailand.

IN-SCOPE REGION

Under the co-leadership of PPATK and AUSTRAC, this assessment draws on information and expertise from the FIUs from Australia, Indonesia, Malaysia, the Philippines, Singapore and Thailand. The assessment team acknowledges the support that Cambodia provided to the project.

The countries involved in this assessment all face a range of terrorism and terrorism financing risks, some of which are shared due to cross-border links and activity. Moreover, the transit of foreign terrorist fighters across the region as they travel to and from the Middle East requires joint country responses even where no common border exists.

METHODOLOGY

This assessment examines risk as a combination of threats, vulnerabilities and consequences. The key concepts used in this assessment are defined on the following page. More detail on the methodology is at **Appendix 1.**

This assessment also uses a range of guidance and reporting from the FATF and other international bodies on risk assessment methodology, ISIL financing methods and emerging global terrorism financing risks.

CAVEAT

As with any analysis of clandestine behaviour, information on terrorism financing can be fragmented, inconsistent and incomplete. The assessment team collected a valuable body of information from participating countries but does not purport to be comprehensive in all of its findings. This assessment recommends deeper analysis of several terrorism financing channels where gaps in understanding contribute to vulnerabilities and overall risk.

REPORT STRUCTURE

The first section of this assessment provides important context for understanding current and emerging terrorism financing risks in the region. It examines the impact of the global security environment on regional terrorism threats, discusses major features that characterise the regional terrorism financing landscape, and provides an overview of general CTF measures, capabilities and challenges across the region.

The second section concentrates on the highest current or emerging risks in the region. It assesses vulnerabilities associated with those risks and identifies opportunities to strengthen measures to mitigate them. It is broken up into four components:

- raising funds to finance terrorism
- moving funds to finance terrorism
- using funds to finance terrorism
- potential change factors.

In conclusion, priority actions to address the highest terrorism financing risks are proposed.

DEFINITION OF KEY CONCEPTS

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.
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. Vulnerabilities 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.
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.

TERRORISM FINANCING LANDSCAPE

10

GLOBAL SECURITY ENVIRONMENT AND THE IMPACT ON OUR REGION

Terrorism and extremism have become core drivers of insecurity in the region and present a dynamic threat. The threat is increasingly characterised by the influence of terrorist and extremist groups operating within the Syria-Iraq theatre, especially the group known as ISIL. ISIL has effectively used social media to radicalise and recruit primarily young men, in the region and globally. While ISIL is currently the main focus of efforts to counter terrorism and violent extremism, other transnational terrorist organisations including al-Qa'ida and its associates (such as Jabhat al-Nusra), continue to pose a credible threat. Domestic conflicts with few or no known links to violent global extremism also present serious security challenges to the region.

"...TERRORISM AND EXTREMISM HAVE BECOME CORE DRIVERS OF INSECURITY IN THE REGION AND PRESENT A DYNAMIC THREAT..."

The Syria-Iraq conflict has attracted thousands of individuals from countries throughout the region. Several hundred have travelled to Syria-Iraq to train and fight, or to support militant groups, in particular ISIL. These individuals – called foreign terrorist fighters – may seek to organise future attacks on their countries of origin if they return. They may also seek to undertake operations in other countries. The current threat returned foreign terrorist fighters pose is potentially more significant than that posed by returnees of previous conflicts.

Far more foreign terrorist fighters from the region have fought in Syria-Iraq than those who went to Afghanistan, Pakistan and other conflicts after the September 11 attacks in the United States. They also eclipse in number the waves of recruits that went to Afghanistan during the 1980s to fight alongside the mujahedeen against the Soviet Union.

ISIL is radicalising a new generation of extremists while re-energising previously degraded ones in the region. Some groups based in the region have overtly pledged their support for ISIL, along with a growing pool of individuals committed to violence to establish a regional caliphate. These individuals and groups have diverse interests and objectives but share a commitment to destroy common enemies.

Recent attacks in the region have direct links back to the conflict in Syria-Iraq, and demonstrate the capacity of groups such as ISIL to influence those operating beyond the central theatre of conflict. Many of these attacks have been low-capability, individual/small-cell events, instigated by ISIL-inspired individuals. However, large-scale sophisticated attacks, long featured as a hallmark of terrorist tactics, cannot be ruled out.

In addition to the threat Syria-Iraq poses, remnants of terrorist capability in the region remain from earlier conflicts and terrorist activity. This includes experienced fighters as well as released inmates. While the sustained counter-terrorism effort across the region over the past 15 years has helped to degrade terrorist capability, these individuals and groups have the potential to inflame the increasingly complex security climate in the region.

The region has a history of terrorist groups from different countries moving across borders to train, shift weapons and funds, or shelter from their home authorities. This continues to occur, primarily across the southern Thailand border with Malaysia and the border-maritime area adjoining the southern Philippines, Indonesia and Malaysia. The transnational nature of the terrorist and extremist threat demands continued multinational cooperation, intelligence exchange and the strengthening of domestic capabilities.

COUNTRY TERRORISM PROFILES

The main terrorism challenges each country faces are summarised below. The regional map on pages 14–15 provides a breakdown of recent attacks, counter-terrorism disruptions, foreign terrorist fighters and related information for each country.

AUSTRALIA

- Australia raised its national terrorism threat level to an attack being 'probable' (the level previously defined as 'high') in 2014.
- Around 110 Australians are currently fighting or engaged with terrorist groups in Syria and Iraq. Approximately 40 have returned to Australia.
- A suspected 190 people in Australia actively support extremist groups in Syria and Iraq.
- 'Lone actor' ISIL-inspired attacks pose the highest risk and present major challenges to detect and disrupt – individuals can move rapidly from intent to attack without betraying any warning signs.
- The international forces driving extremist ideology and capabilities are becoming more sophisticated, with extremist narratives particularly from ISIL resonating with small sections of the Australian community.

INDONESIA

- Indonesia faces a high threat of terrorism.
- Approximately 568 Indonesians are currently engaged in the Syria-Iraq conflict. A further 183 are believed to have returned home. Critically, a number of Indonesian foreign terrorist fighters in Syria and Iraq have encouraged and directed attack planning by associates in Indonesia.
- Indonesia has identified 11 active designated terrorist groups.[2] Some of the most active terrorist groups have links with ISIL and al-Qa'ida.
- Indonesian authorities have successfully disrupted a number of groups, but violent extremist networks remain intact. The January 2016 attack in Jakarta underlines the persistent threat extremist groups pose, particularly smaller, self-trained cells that can be harder to detect and disrupt.

MALAYSIA

- Malaysia elevated the risk of terrorism and terrorism financing in 2014 to high due to the threats posed by ISIL and foreign terrorist fighters.
- An estimated 73 Malaysian nationals have joined or attempted to join terrorist groups in Syria and Iraq. At least 19 individuals have been killed in theatre. Eight fighters have been arrested and convicted when they returned home.
- A 28 June 2016 attack in which two men threw a grenade into a Kuala Lumpur nightspot was the first successful terrorist attack in Malaysia. Police have confirmed a Malaysian ISIL fighter in Syria-Iraq directed the attack.
- Malaysia continues to be a transit country for recruits for terrorist groups active in other countries.
- Although Malaysia exercises tight border security, some of its porous border areas make it vulnerable to terrorists carrying funds between Malaysia and its neighbours.

2 These are Jemaah Islamiyah, Jemaah Anshorut Syariah, Majelis Mujahidin Indonesia, Jasirah Al Mulk, Jemaah Anshorut tauhid, Mujahidin Indonesia Timur, Mujahidin Indonesia Barat, Tauhid Wal Jihad, Jemaah Ashorut Khilafah Daulah Nusantara, Khataibul Iman, and Negara Islam Indonesia.

PHILIPPINES

- The threat of terrorism in the Philippines, specifically in the southern provinces, is high. The security environment is largely influenced by nationalist, separatist and local terrorist groups operating in the south.
- Filipino authorities report that 12 foreign terrorist fighters are fighting with groups in Syria and Iraq.
- Five local terrorist groups have pledged support to ISIL.[3] These local groups are known to have undertaken training, recruitment and fundraising in the southern Philippines, with signs of some cross-border movement of fighters between the Philippines, Malaysia and Indonesia.

SINGAPORE

- In 2015, Singaporean authorities raised the national security alert to high and increased security measures and border checks.
- Singapore has detected several cases of self-radicalised individuals since 2008, none of whom had contemplated mounting attacks in Singapore but instead were intent on making their way to conflict theatres overseas to participate in militant jihad.
- Singapore has not experienced any terrorist attacks but the threat of such an attack is at its highest as a result of the threat ISIL poses.
- In 2015, Singaporean authorities investigated eight individuals calling themselves 'Islamic State of Bangladesh'. The group allegedly raised money to purchase firearms and carry out planned attacks in Bangladesh. Singaporean authorities seized the money and prosecuted six members of the group on terrorism financing charges, four of whom were convicted.
- Singapore's role as a major international financial centre, trade/transport hub and proximity to its neighbours increases the inherent risk it will be used as a conduit by terrorists and their financiers.

THAILAND

- Thailand's national security environment is largely influenced by ethno-nationalist conflict in southern Thailand. The southern extremist groups are ethnic Thai-Malay Muslims but are not currently linked to global extremism.
- Thailand reports no known foreign terrorist fighters. Only a relatively few foreign terrorist fighters from other countries are known to have transited through Bangkok to the Middle East.
- The majority of insurgency attacks in Thailand are conducted by unknown actors. Of the known actors, Barisan Revolusi Nasional and its sub-groups, the Aba Cheali Group and Runda Kumpulan Keci, are considered to be among the most prominent and active.
- Thailand's porous national borders increase its exposure to illegal movement of weapons, people, cash or goods of exchange.

3 These are the Abu Sayyaf Group, Ansar Khilafali Philippines, Khilafaf Islamiyah Mindanao, Bangsamoro Islamic Freedom Fighters and the Maute Group.

PHILIPPINES

ATTACKS (in past 3 years)
- 63 carried out
- —* disrupted

FOREIGN TERRORIST FIGHTERS
- 12 overseas
- —* returned

FINANCIAL SANCTIONS
- 12 persons/accounts subject to targeted financial sanctions

TERRORISM FINANCING
- 53 STRs** (last 12 months)
- 1 prosecution (2013-15)

THAILAND

ATTACKS (in past 3 years)
- 1375*** carried out
- 2 disrupted

FOREIGN TERRORIST FIGHTERS
- 0 overseas
- 0 returned

FINANCIAL SANCTIONS
- 28 persons/accounts subject to targeted financial sanctions

TERRORISM FINANCING
- 24 STRs** (last 12 months)
- 0 prosecutions (2013-15)

MALAYSIA

ATTACKS (in past 3 years)
- 1 carried out
- 5 disrupted

FOREIGN TERRORIST FIGHTERS
- 73 overseas
- 8 returned

FINANCIAL SANCTIONS
- 41 persons/accounts subject to targeted financial sanctions

TERRORISM FINANCING
- 25 STRs** (last 12 months)
- 1 prosecution (2013-15)

SINGAPORE

ATTACKS (in past 3 years)
- 0 carried out
- —* disrupted

FOREIGN TERRORIST FIGHTERS
- 2 overseas
- 0 returned

FINANCIAL SANCTIONS
- —* persons/accounts subject to targeted financial sanctions

TERRORISM FINANCING
- 205 STRs** (last 12 months)
- 6 prosecutions (2016)

INDONESIA

ATTACKS (in past 3 years)
- 51 carried out
- 8 disrupted

FOREIGN TERRORIST FIGHTERS
- 568 overseas
- 183 returned

FINANCIAL SANCTIONS
- 26 persons/accounts subject to targeted financial sanctions

TERRORISM FINANCING
- 185 STRs** (last 12 months)
- 34 prosecutions (2013-15)

AUSTRALIA

ATTACKS (in past 3 years)
- 3 carried out
- 9 disrupted

FOREIGN TERRORIST FIGHTERS
- 110 overseas
- 40 returned

FINANCIAL SANCTIONS
- 4 persons/accounts subject to targeted financial sanctions

TERRORISM FINANCING
- 536 STRs** (2014-15)
- 7 prosecutions (2013-15)

* No data provided.

** STRs - suspicious transaction reports. In Australia, these are called suspicious matter reports.

*** This figure comprises three types of incidents in Thailand's southern border provinces:
(1) attacks on officials and citizens,
(2) bombings and
(3) other insurgent activities such as destruction of property and facilities. While over 60 per cent of these incidents do not result in casualties, they contribute to the propaganda warfare that the insurgents wage to cause public unrest and promote their separatist ideology.

REGIONAL TERRORISM FINANCING ENVIRONMENT

This infographic shows detail about the current terrorism and terrorism financing environment in South-East Asia and Australia.

KEY FEATURES OF THE REGIONAL TERRORISM FINANCING ENVIRONMENT

To help understand the nature and range of terrorism financing activity across the region, this assessment identified a number of key features that shape or dominate the regional environment. These comprise specific geographic and structural features, as well as broad terrorism financing behaviours.

GEOGRAPHIC AND STRUCTURAL FEATURES

The reality of geography

Porous land borders and close maritime boundaries in many parts of the region are exploited by extremists and networks to move funds across borders outside reportable channels and the scrutiny of authorities. Security and border control regimes face significant challenges with monitoring and stopping the cross-border movement of extremists, weapons, cash and other commodities[4] which are sold to fund terrorist activity.

Cash-intensive and informal economies

"...TERRORIST GROUPS ACROSS THE REGION USE TRUSTED NETWORKS OF CASH SMUGGLERS AND IT IS ANTICIPATED THIS WILL CONTINUE TO BE A CORNERSTONE OF TERRORISM FINANCING IN THE REGION..."

The prevalence of cash-intensive and informal economies in a number of regional countries assists extremists and their supporters to access and move funds anonymously. Terrorist groups across the region use trusted networks of cash smugglers and it is anticipated this will continue to be a cornerstone of terrorism financing in the region. Efforts by some countries to make it easier and cheaper for citizens to access and use mainstream financial channels will assist to reduce the size of the informal economies.

Financial and transit hubs

The region is home to a number of financial and transit hubs. Singapore, Bangkok and Kuala Lumpur all rank in the world's top 13 cities for international passenger traffic. Singapore is also one of the world's largest financial centres and a major international trade hub.

International financial centres are considered to pose higher money laundering and terrorism financing risks as their sophisticated banking, company, trade financing and related services make them attractive destinations and conduits for illicit money flows. This is especially the case for regions such as South-East Asia, where terrorist groups operate.

Transit hubs are also used as pick-up points for funds for foreign terrorist fighters and their associates travelling to conflict zones.

4 This includes trafficked humans, drugs, food and other stolen goods.

BROAD TERRORISM FINANCING BEHAVIOURS

Continued use of established methods

Regional countries face a range of terrorism financing risks depending largely on their domestic situation and geographic location. Most of these risks feature prominently in recent international reporting on global terrorism financing risks and ISIL financing.[5] However, to date the region has not been exposed to the full range of risks experienced globally, particularly the risks apparent in the Middle East region.

"...THE REGION'S POROUS LAND AND CLOSE MARITIME BORDERS, AS WELL AS INFORMAL CASH-INTENSIVE ECONOMIES, ALSO INFLUENCE THE CONTINUED USE OF THESE ESTABLISHED METHODS..."

The capability and intent of regional terrorist actors and groups influence the scale and nature of terrorism financing behaviour across the region. Small-cell terrorist activity, foreign terrorist fighter travel and a growing number of lone actors will see continued use of self-funding and cash smuggling to raise and move funds. Along with misuse of NPOs and remittance businesses, these proven and easy-to-use terrorism financing methods continue to be effective, reducing the need for terrorists and their supporters to resort to more complex methods or adopt new payment systems.

Authorities are aware of these areas of risk but the generally low-level nature of this activity and lower amounts involved reduce the ability to detect suspicious transactions or patterns of behaviour that indicate terrorism financing.

The region's porous land and close maritime borders, as well as informal cash-intensive economies, also influence the continued use of these established methods. For those groups with the capability, a significant volume of terrorism funds will continue to be raised through criminal activity.

5 This includes reports from the FATF and the Egmont Group.

Terrorism financing flowing into and out of the region

Terrorism funds flowing out of the region are currently channelled mainly to support the Syria-Iraq conflict, but comprise only a small portion of international funding to factions fighting in that area. In the past, outbound terrorism financing flows have gone to a wide range of countries[6] - sometimes through the use of conduit countries and often to support foreign terrorist fighters to train, travel and fight in conflict zones.

While the flow of funds out of the region poses a high terrorism financing risk, regional authorities are increasingly concerned by funds flowing into the region to support local terrorism networks. For example:

- PPATK estimate that foreign sources transferred more than IDR10 billion (AUD1 million) in terrorism financing into Indonesia between 2014 and 2015.
- Funding for the January 2016 attacks in Jakarta is reported to have been directed from an ISIL foreign terrorist fighter cell based in Syria-Iraq with links to an Indonesian network.

Given only small sums are required to stage a deadly attack, even modest amounts of funding from foreign terrorist groups pose a significant risk to the region's security.

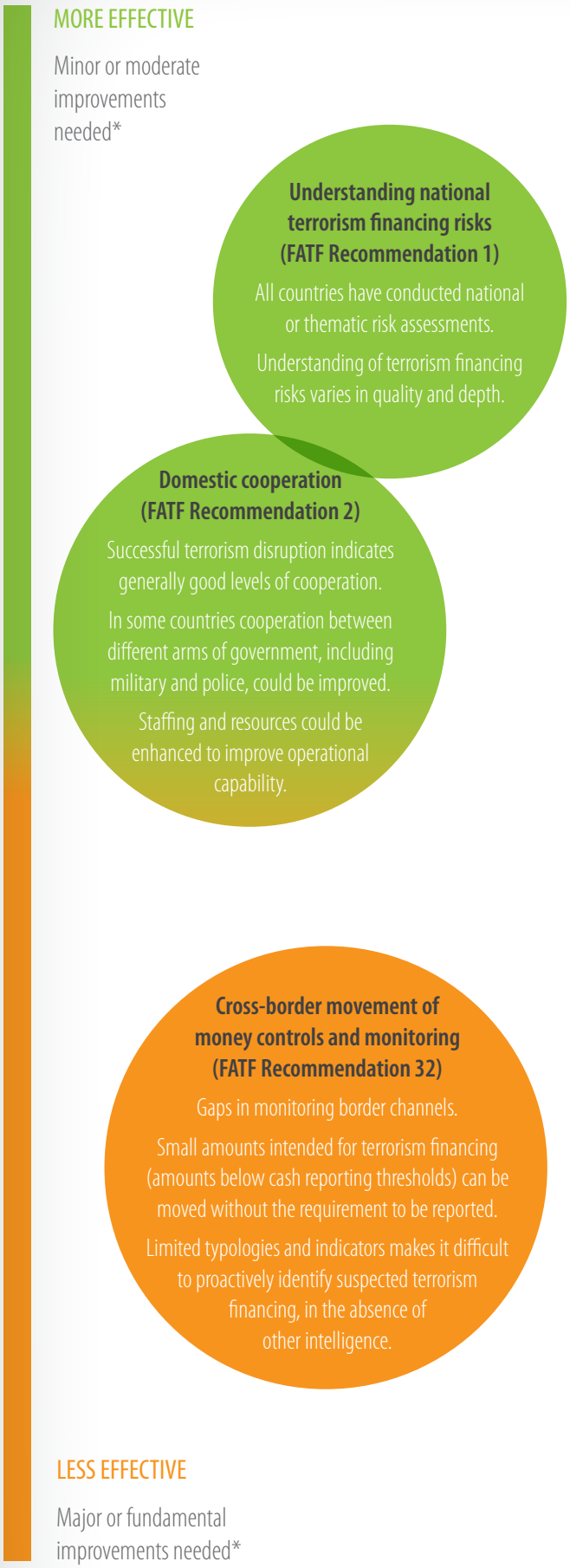
Funding from private donors, particularly in the Middle East (such as Iraq, Jordan and Syria among others), is another challenge some countries face. Donations for charitable purposes, religious schools or to support apparently legitimate causes (for example, building infrastructure) flow into the region. Some of these funds are suspected to have been channelled to support propaganda. Moreover, legitimate international assistance for religious schools or community organisations is susceptible to being diverted from its intended purpose towards terrorist groups.

6 This includes Afghanistan, Pakistan, Lebanon, Somalia, Sri Lanka and Turkey.

REGIONAL CTF CAPABILITIES AND CHALLENGES – AN OVERVIEW

In a region as diverse as South-East Asia and Australia, the implementation and maturity of AML/CTF frameworks will understandably vary. Each country will have its own range of strengths and areas for improvement. The following infographic rates the region's effectiveness against several international standards established under the FATF 40 Recommendations, concentrating on those standards central to CTF.

It is important to note that these ratings are primarily based on aggregating each country's self-assessment on effectiveness/vulnerability into an overall regional rating. Even where the region's overall performance is assessed as 'More effective' against a particular standard, some countries may need to make considerable improvements to strengthen their individual frameworks. In particular, while domestic and international cooperation works reasonably well, all countries can do more to strengthen these crucial areas to be more operationally effective and improve information sharing.



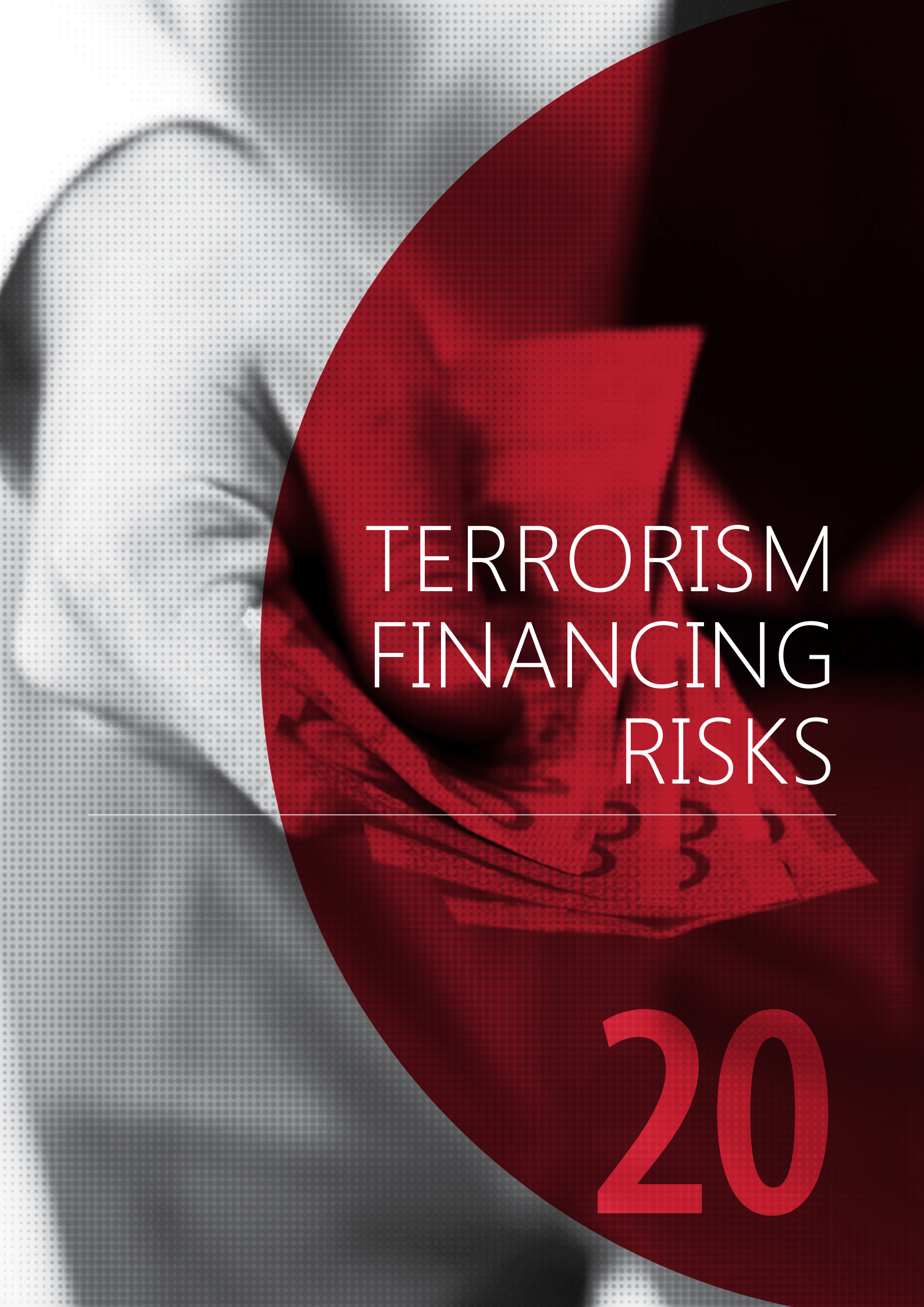
*__Key__: The scale modifies FATF effectiveness ratings. It is intended as a flexible gauge for understanding CTF capability across the region but should not be interpreted as a regional mutual evaluation.[9]

---

7 This also relates to a number of other FATF measures, particularly Recommendation 16 on wire transfers, Recommendation 20 on suspicious transactions, and Recommendation 32 on cash couriers.

8 Recommendation 16.16 and 16.17 on wire transfers.

9 See FATF, *Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CTF systems*, February 2012. FATF and the Asia/Pacific Group on Money Laundering mutual evaluations (ME) or peer-to-peer reviews of country AML/CTF frameworks have been considered where applicable. At the time of this assessment only Australia and Malaysia had published MEs under the current round of evaluations.



TERRORISM FINANCING RISKS

20

KEY TERRORISM FINANCING RISKS

This section concentrates on risks assessed as 'high' or 'medium' with serious vulnerabilities common across some or all countries across the region. It represents a subset of a broad range of channels the regional assessment team collected data on and examined. The full set of terrorism financing channels examined is at **Appendixes 2 and 3**.

The section divides key terrorism financing risks according to the key stages of terrorism financing:

RAISING TERRORISM FUNDS

MOVING TERRORISM FUNDS

USING TERRORISM FUNDS

This section also examines two key potential changes that could alter the regional terrorism financing picture in the future.

HOW TO INTERPRET THE RISK RATINGS

The overall risk assessment for each channel represents the collective level of risk posed to the region. However, across the region terrorism financing activity and the maturity of CTF frameworks to mitigate risk vary from country to country. To illuminate country differences, each risk channel also includes the individual country risk ratings and more detail about each country's own terrorism financing environment.

RAISING FUNDS TO FINANCE TERRORISM

Terrorism financing channel	Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand	Overall risk rating
	Country risk rating						
Self-funding from legitimate sources	High	High	High	Negligible	Medium	High	High
Non-profit organisations	High	High	Medium	Medium	Low	High	High
Fundraising through social media and crowdfunding	Medium	High	High	Medium	Low	Medium	Medium
Criminal activity	Medium	High	Low	High	Low	Medium	Medium

KEY

High Medium Low

SELF-FUNDING FROM LEGITIMATE SOURCES

SELF-FUNDING FROM LEGITIMATE SOURCES IS HIGHLY LIKELY TO REMAIN A KEY ENDURING RISK ACROSS THE REGION OVER THE NEXT THREE TO FIVE YEARS.

FIUs should focus on improving guidance to reporting institutions on customer risk profiles and suspicious financial characteristics associated with self-funding behaviour.

Risk rating

Except for the Philippines, all countries assess self-funding from legitimate sources as posing the highest-risk for raising terrorism funds.

Country experience

In Australia and Malaysia, self-funding is primarily used for tactical, short-term purposes, such as planning and staging lone actor or small-scale attacks, or to fund travel by foreign terrorist fighters.

In Indonesia, a terrorist group collected legitimately-sourced funds from its members which were then used to finance military training.

In Singapore, investigations into the now disrupted local Jemaah Islamiyah (JI) network revealed that it was largely self-financed. Singaporean JI members had contributed five per cent of their monthly salaries to the group. Funds were used for local activities and to financially assist less well-off members.

Most countries assess self-funding from legitimate sources to be the most commonly used method of raising terrorism funds across the region, particularly for foreign terrorist fighters travelling to conflict zones. It generally occurs in small volumes, and transactions are most often conducted in cash or through legitimate financial channels. In observed cases, funds are mainly derived from income, sale of personal items, credit cards, loans, welfare payments and pension funds or superannuation.

Vulnerability

Self-funding will remain extremely difficult to detect for a range of reasons:

- funds are almost always sourced through legitimate activity
- transactions are often of low value and indistinguishable from ordinary financial behaviour
- the time-lag between an individual accessing funds and committing an attack or travelling to a conflict zone can be very short
- cash-intensive economies throughout the region allow cash to change hands unnoticed.

Detection of self-funding activities is almost always reactive (after an individual has come to public attention or authorities have placed an alert on a person of interest). It will remain difficult for reporting institutions to proactively detect and report suspected instances of self-funding until FIUs provide them with more detailed and comprehensive guidance on high-risk customer profiles.

Opportunities to respond

FIUs should provide the critical bridge between reporting institutions and intelligence and security agencies to ensure timely, secure and trusted information exchange on persons of interests and their financial activity.

Regional partners should pool their knowledge on self-funding to improve regional capacity, particularly for detecting and tracing foreign terrorist fighter money trails.

FIUs should continue to support international research projects, such as those which the FATF and the Egmont Group are conducting, to identify common self-funding characteristics and provide better guidance to reporting institutions on high-risk customer profiles.[10]

10 This could involve regional studies of the financial footprints associated with foreign terrorist fighters, lone actor and small-cell, small-scale attacks.

NON-PROFIT ORGANISATIONS

COUNTRIES IN THE REGION NEED TO DEVELOP A CLEARER PICTURE OF THE LEVEL OF MISUSE OF NPOs FOR TERRORISM FINANCING, THROUGH IDENTIFYING HIGHER-RISK ORGANISATIONS.

NPOs receiving funds from foreign regions or sending money to, or operating in or close to, conflict zones are generally most vulnerable to terrorism financing abuse.

Risk rating

With the exception of Singapore, regional countries assess NPOs as a medium or high risk. While regional authorities have detected only a few cases of terrorism financing through NPOs, this channel has been rated as a 'high' risk because of the significant number of potentially vulnerable and at-risk NPOs operating within the region, coupled with their capacity to raise large volumes of funds.

Country experience

In Thailand, some NPOs have diverted money to fund propaganda to support the insurgency in the south.

In the Philippines, a NPO used donated funds to build social housing with cheap material and diverted unspent monies to fund terrorist activity.

In Australia, two cases from the mid-2000s involved community-based NPOs that raised close to AUD1 million each which was funnelled to foreign-based terrorist groups for organisational funding. Australia has also experienced suspicious 'pop-up' NPOs that appear to dissolve after raising funds for 'humanitarian efforts' in Syria and Iraq.

The actual level of misuse of NPOs[11] for terrorism financing is lower than expected across most of the region. Despite the vulnerabilities of this sector, countries have identified only a small number of cases involving NPOs. This is at odds with the number of at-risk NPOs across the region – particularly NPOs receiving funds sent from foreign regions or NPOs sending money abroad, or operating in or close, to conflict zones.

NPOs can be attractive vehicles for raising funds for terrorism. Terrorists and their supporters can exploit vulnerable NPOs, while some NPOs actively support terrorist groups behind a veil of legitimacy.

The terrorism financing risk NPOs pose is increased due to the ability of NPOs to raise large amounts of funds quickly while avoiding detection. Even if only a limited number of NPOs are exploited for terrorism financing, the consequences can be disproportionately higher than for other fundraising methods.

It is important to remember that a diverse range of NPOs operate in the region, many of which are not exposed to terrorism financing risks. Some NPOs also perform a vital role in combating terrorism through mitigating radicalisation.

11 The assessment adopted the FATF standard (Recommendation 8) that applies only to NPOs defined as 'a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works"... It does not apply to the entire universe of NPOs'.

Vulnerability

The size and diversity of this sector presents challenges for regulatory measures and oversight. Commingling terrorism financing funds with large amounts of legitimate NPO funds is a common method and can greatly decrease visibility and detection of illegitimate funds. Where funds are sent to countries with few, if any, formal banking systems or government controls, it is almost impossible to confirm the recipient or ultimate use of the transferred funds.

Without adequate governance, NPOs can be corrupted, infiltrated or have their funds diverted by terrorists or their associates. Smaller organisations are probably at most risk of being manipulated.

Given the heightened sanctions and transaction monitoring systems used within the banking sector, organisations attempting to send illicit funds to high-risk countries are likely to use conduit countries and alternative channels, decreasing the ability of authorities to detect illicit transactions.

Opportunities to respond

Countries should complete comprehensive risk assessments of their NPO sector, to identify higher-risk organisations.[12] These assessments could be combined into a regional assessment that informs joint initiatives to strengthen measures to mitigate the subset of NPOs identified as high risk. To promote a shared understanding and outreach to vulnerable NPOs, a regional forum of NPO bodies, FIUs and other stakeholders, including regional CTF working groups, should also be considered.

Where gaps exist in the AML/CTF frameworks of individual countries, these countries should fully implement FATF Recommendation 8, which requires countries to review the adequacy of laws and regulations to prevent NPOs from being misused for terrorism financing.

FIUs in the region should collaborate more closely with:

- relevant NPO supervisors or regulators to improve governance and oversight
- reporting institutions to ensure they apply proportionate customer due diligence and transaction monitoring in relation to high-risk NPOs they deal with
- NPO peak bodies to include AML/CTF measures in codes of conduct to inform risk assessments and build community trust in the NPO sector.

FIUs should also work with NPO peak bodies to develop guidance to NPOs and communities on safe ways to donate to humanitarian efforts in high-risk countries. FIUs could explore opportunities to lead or participate in multi-agency working groups to identify and monitor higher-risk NPOs, and match customer[13] data with intelligence holdings (financial, criminal and national security).

Increased use of Egmont multilateral information sharing and direct bilateral requests to trace high-risk NPO remittance activity could improve visibility of the end user of the funds.

Strengthening NPO oversight – the Malaysian experience

Malaysia's experience in strengthening its regulatory framework for NPOs and increasing its oversight and outreach activities across the sector provides a good example for its regional partners. In contrast to many regional countries, Malaysia has conducted a comprehensive risk assessment of the sector and has adopted targeted approaches to risk mitigation. This has included implementing strong regulatory measures involving law enforcement and regulators.

12 This would be in line with the FATF standard on NPOs which require targeted approaches towards NPOs at higher risk of terrorism financing exploitation.

13 'Customer' refers to the organisation and all related office bearers. These details should be held by the relevant sector oversight body.

FUNDRAISING THROUGH SOCIAL MEDIA AND CROWDFUNDING

Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand	Overall rating
Medium	High	High	Medium	Low	Medium	Medium

ONLINE FUNDRAISING ACTIVITY HAS BEEN MINIMAL, LARGELY OPPORTUNISTIC AND INVOLVES SELF-DIRECTED INDIVIDUALS AS OPPOSED TO GROUPS OR NETWORKS.

Obtaining proof of user identity and intent to use funds for terrorism will remain a challenge for authorities but the digital footprint from online use may help deter terrorism financing activity and provide detection opportunities.

Risk rating

Countries assess the risk of fundraising through social media and crowdfunding as medium (Australia, Thailand and the Philippines) to high (Indonesia and Malaysia). While very few cases have been detected, the risk associated with this channel is increased due to the inherent vulnerabilities that online fundraising presents to authorities.

Country experience

Online fundraising activity has been reported more in Indonesia and Malaysia than other regional countries. In identified cases, individuals have made donations into a bank account after a call was made for donations online.

The number of identified cases of online fundraising for terrorism varies throughout the region, but is minimal overall. Most online activities are highly visible and – without sophisticated understanding of computing and use of encryption tools – can leave a trail that can be used for successful prosecution. This may deter future uptake of online platforms for raising terrorism funds.

Terrorists and their financiers mainly use social media as a communication channel to solicit and broadcast calls for funding. Funds originate from different sources and are then often stored in, or moved through, mainstream channels such as bank accounts and electronic transfers. Because fundraising activities via social media and crowdfunding platforms often intersect with mainstream banking or remittance channels, intelligence-driven monitoring is likely to lead to increased detection and disruption of illicit activity. This will require greater sharing of information among governments and with the private sector.

Money raised through this channel is primarily used to fund individual travel to conflict zones or support terrorist activities – both within the region and further afield.

Vulnerability

Social media and crowdfunding platforms are widely accessible, low-cost and can reach a global audience. Social media accounts can be accessed on demand and from any internet connection around the world. The volume of legitimate funding activity that occurs on these platforms may also mask the small amount of illegitimate activity.

Opportunities to respond

FIUs could consider forming dedicated 'cyber operations teams' to enable them to better collaborate with security and investigation agencies and relevant online providers to monitor and identify suspicious fundraising activity and related accounts.

Social media platforms also present an opportunity to detect terrorism financing and other suspicious activity through outreach to at-risk communities and public calls for information – these initiatives could be included in broader 'countering violent extremism' strategies.

CRIMINAL ACTIVITY

Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand	Overall rating
Medium	High	Low	High	Low	Medium	Medium

CRIMINAL ACTIVITY IS A KEY SOURCE OF FUNDS FOR SOME TERRORIST AND EXTREMIST GROUPS IN THE REGION.

The secure and timely sharing of critical intelligence about national security and criminal investigations is necessary for countries to detect and disrupt criminal financing of terrorism.

Risk rating

Use of criminal proceeds by extremists and terrorist groups varies markedly, but is a very high risk for the southern Philippines and other pockets across the region.

Country experiences

In Australia, criminal activity to obtain funding has so far been limited. While few links between extremists and criminals have been detected, they appear to be based on informal, personal or ad hoc ties.

In Indonesia, violent robbery is the most common crime type terrorists use to raise funds. Cybercrime and hacking attacks have also been detected.

The Philippines has experienced a wide range of crimes – including smuggling of goods and weapons and trafficking of people and drugs – but kidnap-for-ransom and extortion are the main income streams.

In Thailand, southern extremist groups have stolen cars and smuggled oil, but mainly extort other crime groups to obtain funds. Authorities also detected a mass marketing scam targeting offshore victims.

For some extremists and terrorist groups in the region, criminal activity provides a key source of funding for organisational and operational expenses. Individuals and groups engage in a variety of offences which range from opportunistic to well organised. The nature and extent of these activities largely reflects the different security environments and authorities' ability to disrupt crime as well as terrorism in their respective country.

Internationally, authorities have uncovered established financial connections between specific terrorist groups and criminal groups. Within the region, the extent of the relationship between terrorist groups and organised crime groups for terrorism financing is unclear.[14] To date, it appears any such connections in most countries are largely ad hoc and fluid. Some authorities suspect informal personal ties exist between criminals and extremists, but these remain unconfirmed.

Vulnerabilities

Most authorities in the region have limited visibility of any links between terrorist and criminal groups and their respective funding channels. Intelligence quality, information sharing and coordination among agencies can be improved.

Where security environments are particularly volatile, militant and terrorist groups engage in a wide range of criminal activities or extort criminal groups for funding purposes. In these complex political environments, authorities face serious challenges in disrupting illicit activities.

Opportunities to respond

Countries should create multi-agency and cross-border task forces to enhance information sharing between authorities and to more readily identify links between persons of interest to both national security and law enforcement investigations.

Wherever possible, countries should conduct national security investigations and parallel terrorism financing investigations to leverage shared intelligence and disrupt criminal financing of terrorism.

14 The terror/crime nexus generally occurs when a crime group controls a market that a terrorist group needs to access – such as firearms, money laundering or encrypted communications – or when a crime group provides funding or material support to the terrorist group.

MOVING FUNDS TO FINANCE TERRORISM

Terrorism financing channel	Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand	Overall risk rating
	Country risk rating						
Cross-border movement of funds/ value	High	High	High	High	Medium	High	High
Banking system	High	Medium	Medium	Medium	Medium	Medium	Medium
Alternative remittance and money service businesses	High	Medium	Low	Medium	Medium	Low	Medium

KEY

High Medium Low

CROSS-BORDER MOVEMENT OF FUNDS/VALUE

Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand	Overall rating
High	High	High	High	Medium	High	High

UNDERSTANDING OF CASH SMUGGLING ROUTES ACROSS THE REGION IS LIMITED.

Deeper cross-border and cross-agency ties are required to develop effective responses.

Risk rating

Aside from Singapore, all countries assess cross-border movement of cash and other items of value for terrorism financing within and across regional borders as high risk.

Country experience

The chains of islands stretching between Indonesia and the Philippines have long-served as stepping stones for the movement of illicit cash. The porous land and maritime borders straddling the Sulu Archipelago are exploited to smuggle cash by both extremists and criminals linked to conflict in the southern Philippines. Cash smuggling is also observed in the majority of kidnap-for-ransom cases in the Philippines.

Similarly, insurgents move across the border between southern Thailand and Malaysia with funds or items of value (e.g. gold).

In Australia and Malaysia, cash is mostly smuggled in small amounts.

The now disrupted JI network in Singapore used cash couriers[15] to deliver funds intended for terrorism financing into Malaysia and Indonesia.

The cross-border movement of cash is a proven terrorism financing methodology and the predominant method for moving funds across the region. It is a reliable and easy way to move funds of varying amounts, with low risk of detection.

Extremists and terrorist networks exploit the porous land borders and close maritime boundaries in many parts of the region to move cash outside monitored cross-border reporting channels. Trusted networks of cash smugglers are also used and will continue to be a key element of regional terrorism financing activity. Security and border control regimes face significant challenges in monitoring and stemming the flow of illicit cash and other commodities (such as gold and precious items) which are sold to fund terrorist activity.

Foreign terrorist fighters and their supporters also move funds through border channels when they travel to conflict zones. Given that only relatively small amounts need to be carried, these funds do not need to be disclosed if they are below the reporting threshold for cross-border movements.[16]

15 Cash couriers move illicit funds or value through monitored reporting channels (e.g. customs or immigration control points). They may disclose to authorities reportable amounts they are carrying, calculating that they will not attract attention or raise suspicion.

16 Cross-border movement reporting thresholds range from amounts just under USD 8,000 to USD 20,000 across regional countries.

Vulnerabilities

"...LARGE INFORMAL, CASH-INTENSIVE ECONOMIES IN SOME COUNTRIES CREATE A PERMISSIVE ENVIRONMENT FOR EXTREMISTS AND THEIR SUPPORTERS TO ACCESS AND MOVE CASH ANONYMOUSLY..."

FIUs have limited visibility of preferred cash smuggling routes within the region. Porous land and close maritime borders will continue to complicate efforts to detect and deter the illicit movement of cash and other items of value. Money changers[17] at border crossings are also used to mask illicit transactions.

Large informal, cash-intensive economies in some countries create a permissive environment for extremists and their supporters to access and move cash anonymously.

The ability of foreign terrorist fighters and terrorist supporters to move funds below cross-border reporting thresholds poses a major challenge for detection. Unless border authorities have intelligence and movement alerts related to the traveller, money for terrorism financing can be moved across borders with low risk of detection, even when amounts above the threshold are disclosed.

In some countries, gaps exist in cross-border movement reporting frameworks, leaving loopholes for terrorists and their financiers to exploit.

Gaps in knowledge also exist over the cross-border movement of stored value cards and bearer negotiable instruments (BNIs)[18] for terrorism financing. While cash is mainly moved, use of stored value cards and BNIs for terrorism financing represents a potential vulnerability for regional border enforcement regimes.

Opportunities to respond

To improve understanding of critical border points and detection of cross-border funds movement, countries should ensure closer working ties and intelligence exchange among relevant national security, border security and law enforcement agencies, and financial intelligence units (as well as the military where required).

National authorities should also strengthen and extend, where required, their cross-border reporting frameworks and monitoring capabilities, particularly to cover critical border points.

Where regional neighbours share cross-border risks, they should work jointly to share intelligence and strengthen border controls.

17 In line with the FATF requirements for currency exchange businesses (bureaux de change), money changers are obliged to report transactions to authorities in most countries, but compliance across the region is low.

18 In the regional terrorism financing context, relevant BNIs include money orders and travellers' cheques.

BANKING SYSTEM

Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand	Overall rating
High	Medium	Medium	Medium	Medium	Medium	Medium

DISTINGUISHING TERRORISM FINANCING FLOWS FROM LEGITIMATE ACTIVITY WITHIN THE BANKING SYSTEM WILL REMAIN A CHALLENGE ACROSS THE REGION.

National authorities need to engage more closely with the banking sector to improve the sector's ability to detect and deter terrorism financing.

Risk rating

Most countries assess the risk of terrorism financing through the banking system as medium risk.

Country experience

Compared with other countries in the region, Australian banks are frequently used to send funds to individuals engaged in foreign conflicts. This largely reflects the central role of banks in the Australian economy, in contrast to the larger cash economies in some regional countries.

In Malaysia, a terrorist group used a bank account to provide financial support to Malaysian foreign terrorist fighters and ISIL affiliates in the Philippines. For Malaysia, the use of domestic banks accounts to send money to terrorist groups in Syria is emerging as a risk.

In the Philippines, the banking system has been used to move kidnap-for-ransom payments, but the link to terrorism financing remains unclear.

Despite relatively mature AML/CTF frameworks throughout the region, the banking system is still exploited to move terrorist funds across the region and to foreign countries. The most common services misused for terrorism financing are bank accounts (personal and business) and international funds transfer instructions. Many terrorist groups operating in the region use third parties to obscure money trails.

Foreign terrorist fighters also use automated teller machines (ATM) at transit points within the region to withdraw cash using debit and stored value cards while travelling to the Middle East. False identification documents and other concealment methods – such as accounts held by family members or associates – also feature in terrorism financing cases.

Vulnerability

Bank accounts are highly vulnerable to terrorism financing as they:

- can be used to access other financial systems and products
- can be used to build false customer profiles
- enable individuals to withdraw cash around the globe, including in high-risk countries
- are vulnerable to misuse by third parties.

Terrorism financing through the banking sector is often small-scale and, particularly with self-funding, indistinguishable from the multitude of legitimate financial transactions undertaken each day.

In the absence of law enforcement intelligence or sophisticated high-risk customer profiles, detection can be highly challenging for frontline bank staff and bank transaction monitoring systems. Most countries considered financial institutions need to improve the quality and timeliness of STRs they submit.

Opportunities to respond

FIUs should continue to build close, trusted and collaborative working partnerships with banks to ensure the banks' transaction monitoring programs are updated to respond to and detect current terrorism financing risks.

FIUs should assist financial institutions to better monitor ATM activity in key foreign terrorist fighter transit routes.

FIUs and other national authorities should identify opportunities to collaborate on CTF training initiatives with inter-agency[19] and industry participants.

19 This could include representatives from national security agencies, law enforcement and regulatory bodies.

Engaging with the private sector

AUSTRAC's direct engagement with the private sector is an encouraging example of how close partnerships can improve terrorism financing STR reporting. In response to the heightened terrorism threat in 2014, AUSTRAC increased its consultation and information sharing with financial institutions. In response, the number of terrorism financing-related STRs submitted by industry increased by more than 300 per cent in 2014–15. The increase can also be partly attributed to increased media coverage of terrorist activities.

AUSTRAC shared profiles of common suspicious customer behavior with banks which has improved not only the amount but also the quality of STR reporting to AUSTRAC. Operational agencies accepted 98 per cent of terrorism financing STRs for investigation.

ALTERNATIVE REMITTANCE AND MONEY SERVICE BUSINESSES

Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand	Overall rating
High	Medium	Low	Medium	Medium	Low	Medium

ACTUAL MISUSE OF REMITTERS FOR TERRORISM FINANCING IS LOWER THAN THE SECTOR'S HIGH VULNERABILITY AND INHERENT HIGH RISK.

Detected cases of remitters exploited for terrorism financing are fewer than expected when considering the sector's high vulnerability and prevalence in most regional economies. The cash-intensive, informal and low-cost nature of remittance businesses makes them an attractive avenue for moving terrorism funds.

Strong links to remitter networks in or surrounding foreign high-risk countries also exist, particularly in the Syria-Iraq region. Funds sent to support families and communities in high-risk foreign countries provide opportunities for concealment through commingling terrorism financing with legitimate remittances.

Some of the ways remitters operate create inherent terrorism financing risks. In particular, offsetting arrangements, such as 'hawala',[20] pose a key risk in the region.

20 Hawala systems involve remitters in different countries offsetting credits and debits between themselves to get funds to customers in overseas locations, without needing to wire transfers or interact with banks.

Hawala can be exploited to conceal the amount of money transferred and the identity of those involved in the transfer (i.e. the actual sender and beneficiary). This method of transferring value is widely used across the region and by remitters in foreign high-risk countries. Due to its inherently opaque nature, the extent of hawala's misuse for terrorism financing in the region is largely unknown.

Risk rating

In general, countries assess the overall risk of remitters being misused for terrorism financing as medium. Many recognise their remittance sector as inherently vulnerable to misuse even where it is subject to supervision and oversight. Gaps in regulatory coverage and intelligence visibility suggest this rating could change to high, particularly if foreign funding into the region through remitters were to increase.

Country experience

Despite Australia having one of the smaller informal cash economies in the region, remittance businesses feature in the majority of Australian cases of terrorism financing. This possibly reflects the large size of Australia's remittance sector and the sector's role as a financial channel for moving remittances to foreign countries in high-risk regions. Australia has detected foreign terrorist fighters and groups of different size and sophistication using remitters to transfer funds overseas. Australian authorities cancelled the registration of one remittance business mainly on the ground that it posed an unacceptable terrorism financing risk.

Suspected terrorists in Indonesia used a hawala dealer to send money to Indonesian students in the Middle East.

Authorities in the Philippines suspect kidnap-for-ransom payments have been moved through remitters but links to terrorism financing remain inconclusive.

Hawala dealers have also been used to receive and transfer funds sent from private donors overseas to religious and teaching organisations within the region. An international corporate remitter was also used to move funds from an ISIL cell in the Middle East to the network that staged the January 2016 attack in Jakarta.

Vulnerabilities

Remittance sectors operating in the region are generally subject to a range of AML/CTF obligations, including registration or licensing. However, regulatory coverage varies across the region. In some countries, gaps exist in supervision and oversight of large parts of the sector. Remitter non-compliance with AML/CTF requirements increases the difficulty for regulators, FIUs and law enforcement agencies in monitoring activity in remittance sectors.

Authorities have some visibility over remittance financial activity and international transfers where funds flow through bank channels. However, transaction reporting from remitters tends to be poor quality. In particular, levels of STR reporting on suspected terrorism financing are low. This may reflect the low level of terrorism financing through remitters in some countries. But it is likely that non-reporting and false reporting obscure the real level of terrorism financing in the sector. Smaller remitters also often lack the resources and capacity to detect and mitigate the risks they face.

All countries recognise that an unknown number of remittance businesses continue to operate 'underground', outside the regulatory framework. Supervisory authorities have taken action to clamp down on illegal remittance operators. Low barriers to market entry and the ability for remitters to operate out of other businesses (such as travel agencies and convenience stores) makes detection challenging.

Opportunities to respond

Similar to the measures required to mitigate high risks associated with vulnerable NPOs, authorities should identify the types of remitters at high risk of being misused for terrorism financing. A better understanding of high-risk factors and activity would help strengthen targeted oversight, outreach and intelligence monitoring of financial behaviour, including remittance corridors linked to high-risk countries outside the region.

USING FUNDS TO FINANCE TERRORISM

COUNTRIES GENERALLY ASSESS THE USE OF TERRORISM FINANCING FOR OPERATIONAL FUNDING AS A HIGHER LIKELIHOOD AND RISK THAN ORGANISATIONAL FUNDING.

Given the higher likelihood of operational funding and its potentially serious consequences, countries should continue to target efforts on disrupting terrorist actors, groups and their financing methods.

Regional countries assess that terrorism financing is likely to be used for two broadly defined purposes:

1. **Operational** funding or direct use
2. **Organisational** funding or indirect use

Generally terrorism financing operational funding will have more severe consequences culminating in attacks and physical harm. The consequences of organisational funding can be less immediate but help support terrorist actors and networks to conceal themselves, build operational capability, and prepare for and stage attacks. Organisational funding helps terrorist groups to recruit, expand networks and entrench their presence in communities.

Ratings in the following table provide a baseline assessment of the most likely use of terrorism financing, noting authorities face significant challenges in tracing how funds are ultimately used.

OPPORTUNITIES TO RESPOND

FIUs should continue to identify opportunities to establish information exchange agreements with counterparts in high-risk terrorism financing destinations, as well as strengthen regional collaboration to exchange information formally and informally to improve tracing of the end-use of terrorism funds.

The higher likelihood of organisational funding being used to support families and dependants of terrorists and for propaganda provides opportunities to:

- monitor the financial activity of family members and dependants of terrorists to generate intelligence leads and identify terrorism networks, including their financial facilitation structures
- develop programs to counter the messaging and propaganda of violent extremist groups.

COUNTRY RATINGS OF LIKELY USE OF TERRORISM FINANCING

Operational

Likely use of terrorism financing	Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand
	Country risk rating					
Personnel mobility/travel	High	High	High	High	Low	Low
Weapon and explosive materials	Medium	High	High	High	Medium	Medium
Training personnel	Low	High	Medium	High	Low	Low

Organisational

Likely use of terrorism financing	Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand
	Country risk rating					
Widow and family charity	Medium	High	High	Medium	Medium	Medium
Propaganda, radicalisation, meetings	Negligible	High	Medium	High	Medium	Medium
Salary	Low	Medium	Low	Medium	Low	Low
Terrorist network maintenance	Negligible	High	Medium	Medium	Medium	Medium

KEY

High Medium Low

POTENTIAL CHANGE FACTORS

This assessment identified two key potential changes that could alter the regional terrorism financing environment in the future.

UPTAKE OF NEW PAYMENT METHODS

THE USE OF STORED VALUE CARDS AND ONLINE PAYMENT PLATFORMS FOR TERRORISM FINANCING IS MORE LIKELY TO INCREASE IF DETECTION OR DISRUPTION OF COMMONLY USED METHODS FORCES A SHIFT IN FINANCIAL ACTIVITY.

These payment methods are very accessible, easy to use and provide good protection from detection.

Stored value cards are an increasingly popular method of legitimately moving money offshore. In the context of terrorism financing, foreign terrorist fighters have used them before and after departure to their destination. They can be loaded domestically with cash or via non-reportable electronic methods, easily carried (or posted) offshore and are not subject to reporting requirements. Funds can be redeemed through multiple offshore ATM withdrawals, restricted only by ATM withdrawal limits. Cards can also be regularly reloaded remotely and anonymously by third parties, meaning that the face value of some cards can understate the cards' actual risk level.

Online payment platforms provide an effective and efficient means of transferring funds or purchasing goods online. While these platforms are not commonly used for terrorism financing across the region, they are likely to grow in popularity. They will be particularly appealing to those individuals who are regular online users – the 'digital native'. While online payment platforms intersect with mainstream banking channels, the large volume of transactions made across these platforms makes detection of suspicious transfers difficult.

Opportunities to respond

Countries should consider regulating stored value cards to better protect them from misuse and collect valuable customer due diligence and transaction information.

FIUs should remain vigilant to overseas developments and any potential shifts in use of stored value cards and online payment platforms for terrorism financing, particularly as authorities harden other channels against misuse.

INCREASED ISIL AND OTHER INTERNATIONAL FUNDING INTO THE REGION

FOREIGN FUNDING INTO THE REGION COULD INCREASE, PARTICULARLY AS ISIL AND OTHER FOREIGN-BASED TERRORIST GROUPS SEEK TO DIRECT OR INSPIRE REGIONAL ACTORS TO STAGE DOMESTIC ATTACKS.

ISIL's suspected involvement in funding the January 2016 attack in Jakarta highlights the severe consequences when foreign terrorist groups finance terrorism within the region. While the majority of regional terrorism funds will continue to be raised domestically, funding from foreign-based terrorist groups carries disproportionately high risks that go beyond financing attacks. It can strengthen foreign influence over regional actors and amplify their ability to radicalise a larger number of new extremists. It also has the potential to strengthen links, including financial ties, among ISIL affiliates in the region

Closer regional cooperation among CTF authorities is crucial to improve visibility over the financing patterns of foreign-based terrorist groups with links to the region. The unforeseen 'shocks' of the 'Arab Spring' across northern Africa and the Middle East, the anti-government uprising in Syria and rapid rise of ISIL are also reminders that the geopolitical landscape can shift rapidly, with repercussions for terrorism financing activity and risks.

Opportunities to respond

The Regional Financial Intelligence Consultative Group should explore innovative ways to exchange information securely and near to 'real-time'. Sharing and data-matching of 'watch' lists[21] would improve visibility over funds flowing into and across the region. It would also support ongoing work to understand the financial methodologies ISIL affiliates use in the region. Egmont protocols to protect information exchange could be used to establish a secure framework.

Analyst exchange programs – where FIU staff from one country work alongside their counterparts in another country on investigations of joint interest – would also enhance the sharing of information on 'targets' or persons of interest, as well as strengthening analytical techniques to improve detection.

FIUs and other intelligence agencies need to maintain a close watch on global terrorism risks and geopolitical change. The CTF Summit should consider including strategic forecasting discussions on global and regional security developments, involving experts from international organisations and outside government, as part of its yearly agenda.

21 This could include national security agency watch lists, national criminal target lists, and details of blocked accounts and black lists held by industry.

COUNTERING TERRORISM FINANCING RISKS

38

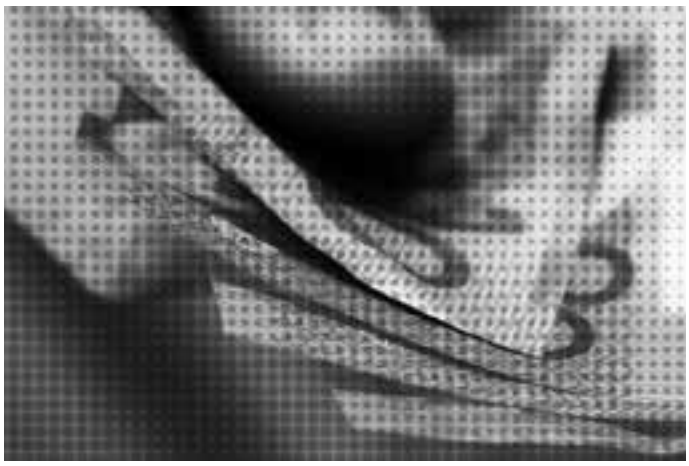
PRIORITY ACTIONS

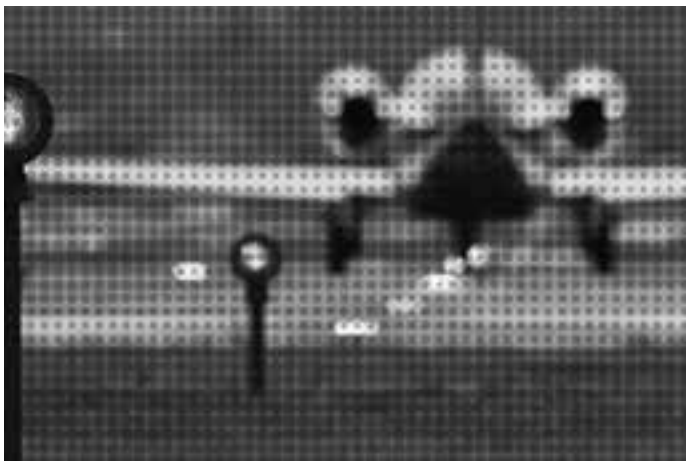
Based on the key risks, relative vulnerabilities and potential change factors assessed in the previous sections, this assessment considers four major terrorism financing risks to the region which require priority action:

- self-funding from legitimate sources
- cross-border movement of funds/value
- at-risk NPOs
- funding from external sources into the region, primarily from ISIL and its affiliates.

For consideration at the 2016 CTF Summit, this assessment proposes a series of priority actions to address the four major terrorism financing risks in the region. It also recommends that progress on implementing these proposals, including any outcomes in mitigating major risks, be reported at the 2017 CTF Summit.

REGIONAL AUTHORITIES ALSO NEED TO MONITOR THE GLOBAL ENVIRONMENT FOR UNPREDICTABLE GEOPOLITICAL SHOCKS THAT MAY INFLUENCE TERRORISM FINANCING ACTIVITY AND GENERATE NEW EXTERNAL SOURCES OF TERRORISM FUNDING INTO THE REGION.





SELF-FUNDING

Challenges with detecting self-funding should be addressed through strengthened partnerships with industry. As a bridge between intelligence agencies and reporting institutions, FIUs should consider broadening intelligence cooperation and providing better guidance to industry, particularly on profiles of high-risk customers.

Establishing secure and trusted channels for information sharing would allow FIUs to share information about watch lists with reporting institutions and assist them to monitor high-risk customer financial activity. This would improve the ability of reporting institutions to detect instances of self-funded terrorism financing.

Countries should ensure that their legislative frameworks and information sharing culture allow the greatest degree of sharing of financial intelligence, while appropriately balancing data protection and privacy risks and requirements.

CROSS-BORDER MOVEMENT OF FUNDS/VALUE

To address cash smuggling and couriering risks, two priorities are recommended:

1. The Regional Financial Intelligence Consultative Group should consider conducting an in-depth study of cross-border cash movements in the region, with a view to recommending strategies for stronger monitoring at critical border points. The study should seek to identify smuggling routes and develop strategies for detecting the cross-border movement of cash for terrorism financing through cross-border currency and BNI reporting channels (including detecting amounts that fall below cash reporting thresholds).

   In addition to engaging FIUs, the Consultative Group should engage border authorities and counter-terrorism agencies, and possibly money changers.

2. Regional partners with shared cross-border risks should prioritise efforts to strengthen their cross-border monitoring and disruption capabilities. These efforts should be informed by the results of the Regional Financial Intelligence Consultative Group's study of cross-border cash movements. In addition, based on joint country efforts, national authorities should consider where to extend and strengthen their cross-border reporting measures and monitoring frameworks.

AT-RISK NPOS

Each regional country should consider updating their assessment of higher-risk NPOs to serve as a basis for targeted oversight and outreach. Consideration should also be given to combining updated country assessments into a regional overview of critical NPO risks to help identify regional initiatives to combat terrorism financing misuse of NPOs.

A regional forum of NPO bodies, FIUs and other stakeholders including regional CTF working groups should also be considered to promote shared understanding and outreach to vulnerable NPOs.

EXTERNAL FUNDING INTO THE REGION

The Regional Financial Intelligence Consultative Group should explore ground-breaking ways to improve FIU visibility over incoming terrorism financing from foreign regions, particularly ISIL in the Middle East. Improving the understanding of terrorism financing flows into the region would also help FIUs to better understand and address the role regional financial and transit hubs play in regional and international terrorism financing. Egmont protocols to protect information exchange could be used as a basis for establishing a secure framework to enable FIUs to share this sensitive information.

Geopolitical shocks and terrorism financing

While terrorism financing related to the Syria-Iraq conflict is clearly a high priority for authorities, FIUs and other intelligence agencies must also monitor developments in other countries and regions that could pose terrorism or security risks. The CTF Summit should consider including strategic forecasting on its annual agenda, and include experts from international organisations and outside government to inform discussions about potential drivers of change and their consequences for the region.


APPENDIXES
42

APPENDIX 1: METHODOLOGY

AIM AND SCOPE

This assessment identifies and assesses the major terrorism financing risks in the South-East Asia region and Australia.

Across the in-scope region, it aims to:

- identify the main global drivers that animate terrorist actors, cells and groups
- analyse distinctive factors that shape regional terrorism financing behaviour and vulnerabilities
- identify key capabilities and challenges in countering terrorism financing
- highlight key methods for raising and moving terrorist funds into, across and out of the region
- recognise the use and consequences of terrorism financing
- consider potential change factors that may impact the terrorism financing landscape in the future
- point to priorities to strengthen the region's capacity to detect and combat terrorism financing more effectively.

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

RISK MODEL

The assessment employs the standard risk framework (likelihood x consequence = risk) and FATF guidance on national money laundering and terrorism 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 terrorism financing activity.

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

1. operational purposes (e.g. moving personnel, weapons, explosives, training, attacks) or
2. organisational purposes (e.g. supporting family or widows, salaries, propaganda, maintaining networks).

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 mitigate 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	VULNERABILITY
Measuring threat factors	**Measuring vulnerability 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	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		Vulnerability statement	
High	Channel is perceived as attractive and is easy to access for terrorism financing activity	**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	Channel is perceived as moderately attractive and requires some knowledge to access for terrorism financing activity	**Medium**	Deterrence measures and controls have some effect at deterring and detecting terrorism financing activity
Low	Channel is perceived as relatively unattractive and is difficult to access for 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

Measuring consequence

Generally, terrorism financing will be for operational or organisational 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 organisational funding, on the other hand, may pose a lesser immediate risk, but ultimately may help fund greater capability and resilience of a terrorist cell or organisation.

INFORMATION COLLECTION TOOLS

The assessment combines quantitative and qualitative information and analysis to establish an evidence base. Two collection tools – a questionnaire and a terrorism financing assessment package – were used to gather information from project members and other experts in the region.

Questionnaire

Each participating FIU completed a questionnaire, comprising a series of questions collecting quantitative and qualitative data on its own country's terrorism financing risk environment and CTF measures. Questions were arranged according to the relevant FATF Recommendations on CTF for ease of reference, consistency and to promote common understanding of definitions.

Terrorism financing assessment package

Each participating FIU also completed a terrorism financing assessment package. The assessment package sought perspectives on current terrorism financing risks, as well as capabilities and vulnerabilities in countering terrorism financing in their country. Respondents were asked to rate these factors on a scale of one to nine (i.e. a sliding scale from low to medium to high).

VALIDATION OF RESULTS

Two regional workshops in-country (Medan and Manila respectively) were conducted to ensure analytical rigour and accuracy of assessment findings. Most participating FIUs attended these workshops.

Structured consultations with a number of terrorism 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. Open source information was also collected to validate findings and assessments including a review of relevant publications produced by the FATF, the Asia/Pacific Group on Money Laundering and other peak bodies.

APPENDIX 2: TERRORISM FINANCING CHANNELS

This assessment collected and analysed a broad range of channels commonly associated with terrorism financing. The list of channels was drawn from recent reports from the FATF, the Egmont Group and other international bodies. Participating FIUs provided statistical information and self-assessed the risks and vulnerabilities of these channels. This information appears in **Appendix 3 and 4**.

RAISING FUNDS TO FINANCE TERRORISM

- Securities company (including investment managers)
- Wealthy private donors
- Funding from terrorist group external to the region
- Non-profit organisations
- Kidnap-for-ransom
- Self-funding through legitimate income
- Legitimate and front businesses
- Social media and crowdfunding platforms
- Other criminal activity

MOVING FUNDS TO FINANCE TERRORISM

- Emerging and other payment platforms (e.g. PayPal, Bitcoin and other digital currencies)
- Cross-border movement of funds/value
- Money changers
- Banking system
- Alternative remittance sector
- Property companies/agents
- Vehicle dealers
- Antiques and arts dealers
- Other valuable commodities (e.g. elephant ivory, endangered animals, narcotics)
- Other (e.g. casino, precious metals and stones and international trade)

USING FUNDS TO FINANCE TERRORISM

Operational

- Personnel mobility (vehicle) or travel
- Weapons or explosive material
- Training personnel

Organisational

- Widow or family charity
- Propaganda, radicalisation or meetings
- Terrorist network maintenance
- Salary

APPENDIX 3: RISK RATINGS

RAISING FUNDS TO FINANCE TERRORISM

Terrorism financing channel	Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand
	Risk and outlook rating					
Non-profit organisations	High	High	Medium	Medium	Low	High
Legitimate and front businesses	Low	High	Low	Medium	Low	Medium
Wealthy private donor	Low	Medium	Low	Negligible	Low	Medium
Self-funding from legitimate sources	High	High	High	Negligible	Medium	High
Funding generated via social media and crowdfunding platforms	Medium	High	High	Medium	Low	Medium
Kidnap for ransom	Low	Negligible	Negligible	High	Low	Low
Funding from terrorist group external to the region	Low	Medium	Low	Low	Medium	Low
Other criminal activity	Medium	High	Low	High	Low	Medium

MOVING FUNDS TO FINANCE TERRORISM

Terrorism financing channel	Australia	Indonesia	Malaysia	Philippines	Singapore	Thailand
	Risk and outlook rating					
Carrying cash or similar instruments, and cash smuggling	High	High	High	High	Medium	High
Cross-border movement of cash and BNIs	High	Low	Low	High	Medium	Medium
Banking system	High	Medium	Medium	Medium	Medium	Medium
Emerging and other payment platforms	Medium	Low	Low	Negligible	Medium	Low
Alternative remittance and money service businesses	High	Medium	Low	Medium	Medium	Low
Securities companies	Low	Low	Low	Negligible	Low	Low
Money changers	Medium	Medium	Low	Negligible	Medium	Medium
Other goods and services (e.g. casino, precious metals and stones and international trade)	Low	Low	Low	Negligible	Low	Medium
Property companies/agents	Low	Low	Low	Negligible	Low	Low
Vehicle dealers	Low	Medium	Low	Negligible	Low	Low
Antiques and arts dealers	Low	Negligible	Low	Negligible	Negligible	Low
Valuable commodities (elephant ivory, endangered animals, narcotics)	Low	Negligible	Low	Medium	Low	Low

KEY

High Medium Low

APPENDIX 4: FIU PERCEPTIONS OF TERRORISM FINANCING VULNERABILITIES

This table represents each participating country's perceptions of its level of vulnerability against the key FATF international standards (drawn from the FATF 40 Recommendations on AML/CTF).

FATF Recommendation	Number of country responses		
	Low	Medium	High
Rec 1: Understanding of national terrorism financing risks	5	1	0
Rec 2: National cooperation and coordination	5	1	0
Rec 5: Comprehensiveness of terrorism financing offence	5	1	0
Rec 6: Targeted financial sanctions relating to terrorism and terrorism financing including freezing without delay and domestic lists	6	0	0
Rec 8: Regulate NPOs, undertake domestic reviews of the NPO sector or have the capacity to obtain timely information on its activities, size and other relevant features	2	0	4
Rec 14: Money or value transfer services (remitters) including visibility of terrorism financing through this channel	3	2	1
Rec 16: Wire transfers as they apply to money or value transfer services (remitters) including visibility of terrorism financing through this channel[22]	4	2	0
Rec 20: Quality and scope of reporting of suspicious transactions related to terrorism financing	3	2	1
Rec 29: Financial intelligence units[23]	3	2	0
Rec 32: Cross-border cash couriers	1	3	2
Rec 36: International instruments	6	0	0
Rec 37: Mutual legal assistance[24]	4	1	0
Rec 40: Effectiveness of international cooperation on CTF matters	6	0	0

22 Recommendation 16.16 and 16.17 on wire transfers.

23, 24 Only five participating countries provided a rating.