Australian Government

AUSTRAC

AUTORITI MONETARI BRUNEI DARUSSALAM

PUSAT PELAPORAN DAN ANALISIS TRANSAKSI KEUANGAN

PPATK

2018

NON-PROFIT ORGANISATIONS & TERRORISM FINANCING

RED FLAG INDICATORS

COPYRIGHT

Contact us

For enquires regarding the license 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 – and from AMBD at fiu@ambd.gov.bn.

NPO RED FLAG INDICATORS

INTRODUCTION

Red flag indicators of suspicious financial activity are valuable tools for detecting potentially illicit behaviour linked to terrorism financing (TF), money laundering and other crimes. This report provides a set of red flag indicators related to non-profit organisations (NPOs) at high risk of misuse for TF in South-East Asia, Australia and New Zealand.

These indicators should particularly help reporting institutions, as well as national authorities and NPOs, to better identify and mitigate suspicious activity potentially linked to TF in the region.

This report reflects input from the financial intelligence units (FIUs) of the eight countries involved in producing the *Non-profit organisations and terrorism financing: regional risk assessment 2017* ('NPO assessment 2017').[1] The indicators are informed by case studies and intelligence from regional FIUs, law enforcement and NPO regulators. Financial institutions that handle NPO finances and have obligations to report suspicious activity also provided input.

As a group, the eight FIUs collected and analysed a large body of information to identify primary and secondary red flag indicators. Primary indicators are likely to be present in cases where NPO misuse for TF has occurred. Secondary indicators point to more general suspicious activity that requires other information, or enhanced due diligence, to support suspicions of NPO involvement in TF (or potentially other crimes including money laundering). In the absence of information to the contrary, primary and secondary indicators when combined should strengthen the grounds for filing a suspicious transaction report (STR)[2] with the national FIU.

To maximise its value, this report should be read in conjunction with the NPO assessment 2017. This is important for understanding the general risk context that exposes some NPOs in the region to potential TF misuse.

1 www.austrac.gov.au/regional-not-profit-sector-risk-assessment-2017

2 International anti-money laundering and counter-terrorism financing (AML/CTF) standards require financial institutions and other reporting institutions to report promptly to the national FIU if they suspect, or have reasonable grounds to suspect, that funds are the proceeds of criminal activity or related to TF. 'STR' is the common term for this type of report, as is suspicious analysis report (SAR). In Australia it is called a suspicious matter report (SMR).

Officers from the following eight FIUs developed and produced this report:

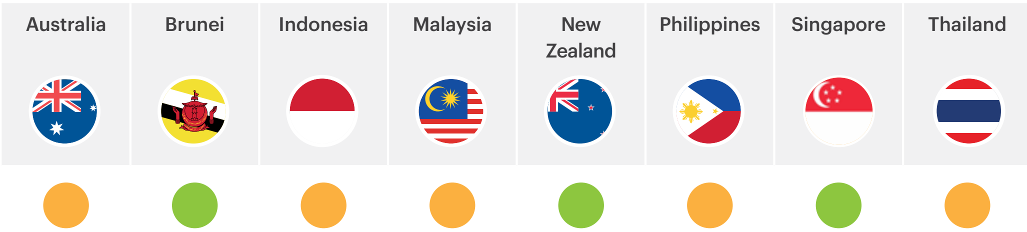
- AUSTRAC, Australia
- Financial Intelligence Unit, Autoriti Monetari Brunei Darussalam (AMBD), Brunei Darussalam
- Pusat Pelaporan dan Analisis Transaki Keuangan (PPATK), Indonesia
- Bank Negara Malaysia
- New Zealand Police Financial Intelligence Unit
- Anti-Money Laundering Council, the Philippines
- Suspicious Transaction Reporting Office, Singapore
- Anti-Money Laundering Office, Kingdom of Thailand.

AMBD, AUSTRAC and PPATK jointly led the project. It follows on from the NPO assessment 2017, launched at the third Counter-Terrorism Financing (CTF) Summit, in Kuala Lumpur, Malaysia, in November 2017. That summit endorsed the assessment's recommendation that a project to develop red flag indicators for NPOs be undertaken, to provide more refined guidance to reporting institutions and improve the quality of the NPO-related STRs authorities receive.

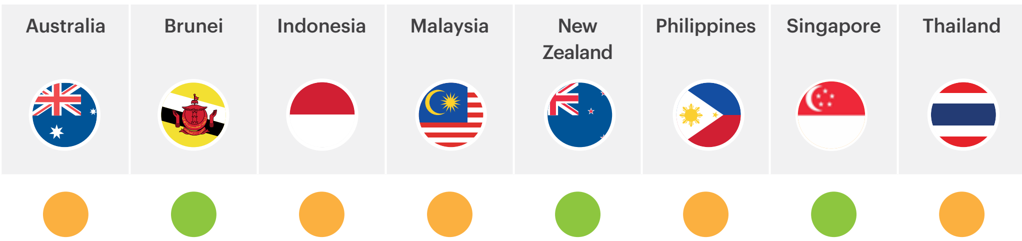
REGIONAL RISK PICTURE FOR NPOS

The overall TF risk for the region's NPOs remains largely unchanged, as assessed in 2017 as medium. Australia, Malaysia, the Philippines and Thailand face medium risks. Brunei, New Zealand and Singapore remain low risk, in line with each country's security environment. Indonesia has reassessed its NPO risk from high to medium. This takes into account new measures introduced to mitigate risk, as well as signs that misuse of social media may be displacing NPOs as a key source of TF funds. See the country dashboards for more information.

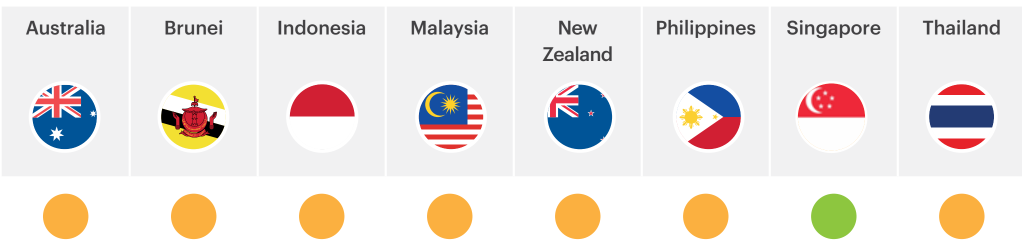
OVERALL RISK RATING - MEDIUM



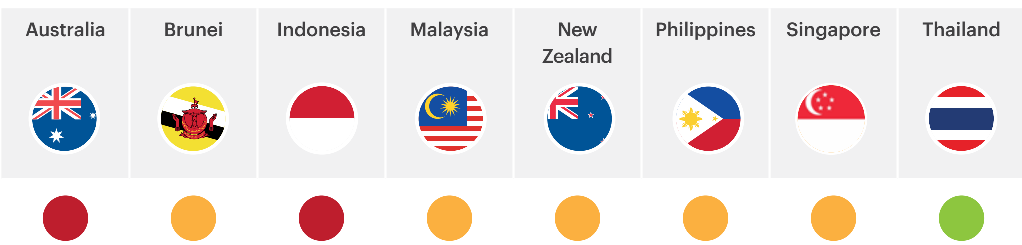
THREAT - MEDIUM



VULNERABILITIES - MEDIUM



CONSEQUENCES - MEDIUM



KEY

High Medium Low

Key factors in the regional risk environment for NPOs include:

- the threat of misuse is relatively low across most of the region
- most regional countries have identified relatively few cases of NPOs related to TF, but several instances have involved funds considered to be large in the current TF environment
- NPOs are mainly victims of misuse (for example, through manipulation or infiltration) for TF, rather than fake NPOs set up explicitly for TF
- NPO links to the so-called 'Islamic State of Iraq and the Levant' (ISIL)—both in the Middle East and domestic ISIL-inspired or directed groups—have been detected or suspected in several instances
- more broadly, a significant number of regional NPOs have links to foreign countries considered high risk for TF, as either source or destination countries for funds flows or delivery of services
- awareness of TF risk among NPOs varies, limiting their ability to protect themselves from financial misuse (as examples of terrorist infiltration indicate)
- limited visibility of the funding cycle (fundraising through to spending, domestically and abroad), compounds the vulnerabilities associated with the cash-intensive nature of most NPO activity
- NPO funds diverted or exploited for TF are more likely to be used to support operational costs of terrorist groups (training, weapons, attacks) and fund travel for foreign terrorist fighters.

These contextual factors need to be taken into account when assessing suspicious activity indicators related to NPO financial behaviour. Reporting institutions should keep in perspective the generally low level of NPO misuse and each country's risk profile when monitoring NPO accounts and transactions.[3] This is important for improving STR quality and avoiding over-reporting or defensive reporting.

---

3 The NPO assessment 2017 found that in most countries, NPOs are probably not a primary means of funding for terrorism in the region compared with other sources (particularly self-funding and in some countries, criminal proceeds).

SUBSET OF HIGHER-RISK NPOS

Understanding the characteristics that expose some NPOs to higher TF risk can help target monitoring to detect suspicious indicators. Not all NPOs are high risk and some may represent low or no risk at all. Identifying the subset of NPOs that are more vulnerable to TF misuse is important for screening large volumes of NPO financial activity and focusing on more likely suspicious transactions.

The NPO assessment 2017 identified a number of generally common characteristics and activities that leave some types of NPOs more exposed to TF. While noting the diverse NPO and security landscape across the region, the following factors have emerged in TF cases involving NPOs:

- more likely to be a service-style NPO[4]
- high cash intensity
- public donations are the main source of funds—membership fees can also be important
- support a particular ethnicity or religion
- based in provincial or capital cities
- operate in a high-risk country or have links to NPOs operating in a high-risk country
- funds flows to and from a high-risk country.

These high-risk characteristics may be useful in setting transaction monitoring systems to detect suspicious NPO activity. Since they reflect broad regional factors, advice from national authorities should also be considered, to align monitoring to the particular risk profile of each country's own high-risk NPO subset.

4 NPOs can be categorised as 'service' or 'expressive' NPOs. Service NPOs are involved in services focused on housing, social services, education and health care. In some countries this can also involve religious education and affiliated social services. Expressive NPOs are involved in programs focused on religious activities, sports and recreation, arts and culture, interest group representation, and advocacy.

PRIMARY INDICATORS

The following primary red flag indicators reflect regional cases of TF misuse, or would be present in scenarios of NPO involvement in TF. The presence of more than one of these primary indicators should increase the weight given to any suspicion of TF misuse.

Some of these indicators may also mirror legitimate NPO activity. In those circumstances, the indicators should be used as an initial step to direct deeper checks of the NPO's profile and behaviour—including its personnel, registration or licensing status, links to other organisations, and match against a country's high-risk NPO subset. Deeper analysis and enhanced due diligence where required, should enable a reporting institution to determine whether sufficient grounds exist to file an STR on TF to the national FIU.

1. NPO treasurer or employee withdraws cash from the NPO account and then deposits it into a personal account, before diverting the funds to a suspected terrorist's account.

2. Media reports the NPO is linked to known terrorist organisations or entities that are engaged, or suspected to be involved, in terrorist activities.

3. Parties to the transaction (for example: account owner, sender, beneficiary or recipient) are from countries known to support terrorist activities and organisations.

4. Funds sent from large international NPOs based in high-risk countries, to their branches in regional countries, are channelled to local NPOs based or operating in domestic conflict areas.

5. An NPO sending funds to multiple entities (individuals and companies) in a high-risk country.

6. NPO raises funds from a major public event and then authorises a third party to be a signatory to the NPO account, who uses it to send funds to high-risk countries.

7. Unusual or atypical large cash withdrawals, particularly after the financial institution refuses to wire NPO funds overseas (thus raising cross-border cash smuggling suspicions).

8. Transactions, including international and domestic transfers, with NPOs that contain terms associated with violent extremism and other terrorist ideologies;[5] for example, *ghanimah* or *fai/fay* (justified stolen funds) and *mujahid/mujaheed/mujahideen* (the term for one engaged in Jihad).

9. Vague justifications and a lack of documentation when the financial institution questions NPO requests to transfer funds to high-risk locations or entities.

10. Use of NPO accounts to accept funds from suspected terrorists and their associates (based on law enforcement agency alerts on persons of interest).[6]

11. Transactions (cash and transfers) involving key personnel of foreign NPOs associated with United Nations Security Council designated terrorist entities.

5 Reporting institutions should research and check translations and other local terms that may be high risk.

6 Reporting institutions should consult national tipping-off laws when using sensitive information related to this indicator.

SECONDARY INDICATORS

Secondary red flag indicators have been detected in some TF cases involving NPOs, but also appear in more general illicit activity (such as fraud and money laundering). Secondary indicators may come to light after a primary indicator triggers deeper checks of an NPO's behaviour. Enhanced due diligence or transaction monitoring may also identify these indicators. This should prompt further searches to corroborate initial suspicions and try to determine whether the indicators relate to TF or another crime.

A combination of primary and secondary indicators should be considered highly suspicious and likely grounds to file an STR.

12. NPO transactions for which there does not appear to be a logical economic purpose or link between the NPO's stated activities and the other parties in the transaction.
13. NPO uses crowd funding and social media to solicit donations, then its online presence vanishes or shuts down.
14. NPO's account shows signs of unexplained increases in deposits and transaction activity.
15. NPO is unable to account for the final use of all its funds/resources.
16. NPO uses unnecessarily complex banking arrangements or financial networks for its operations, particularly overseas.
17. NPO, or NPO representatives, use falsified or conflicting documentation.
18. Inconsistencies between the pattern or size of financial transactions and the stated purpose and activity of the organisation.
19. Unexpected absence of contributions from donors located in the country.
20. Large outgoing transactions to the country of origin of NPO directors who are foreign nationals, particularly if the country is high risk.
21. NPO appears to have few or no staff and limited or no physical presence, which is at odds with its stated purpose and scale of financial activity.
22. NPO funds commingled with personal/private or business funds.

CASE STUDIES

Case studies illustrate how some primary and secondary indicators included in this report can help identify suspicious NPO activity related to TF. These case studies show that the presence of one or more red flag indicators can be used as a basis for reporting good-quality STRs for FIUs and national authorities to use in detecting, disrupting and tracing the misuse of NPO financial and other activity for TF.

CASE STUDY 1 — AUSTRALIA

An NPO received domestic electronic funds transfers from multiple third parties, and frequent large cash deposits into its NPO account. The NPO had links to a religious organisation that media reporting claimed was associated with violent extremist views. Some entities transferring funds into the NPO account were reportedly linked to terrorist groups or entities. While the majority of the funds were traced as going to local charitable activity, some of the funds remained unaccounted for and raised suspicions about their ultimate use. Australian authorities continue to monitor the NPO's financial activity.

In this case, FIUs and national authorities would find the following information included in an STR to be useful intelligence:

- a summary of account activity
- details of the account holders/signatories and any associated accounts held at the same financial institution
- a list of the entities donating funds and
- any information on the end-use of the funds.

INDICATORS PRESENT: 2, 3, 14

CASE STUDY 2 — INDONESIA

A foreign NPO headquartered in the Middle East had an international network of branches. Mr X, who headed an NPO branch in South-East Asia, is a member of Jemaah Islamiyah (JI), an Al Qaeda (AQ) affiliate. According to the United Nations, Mr X exploited the South-East Asian NPO to channel funds from AQ to the JI network, under the cover of humanitarian activities in the region. Information revealed Mr X and the JI cells used the funds to buy weapons and finance other terrorist activities.

Useful information in this case:

- a summary of account activity
- details of the foreign sending account
- local NPO account holder and signatories and
- recipients of regional transfers.

INDICATORS PRESENT: 4, 11, 13, 14

CASE STUDY 3 — INDONESIA

An unregistered (and unincorporated) local NPO ('NPO A') organised a large public event to raise funds. It arranged for the funds, in cash and electronic transfers, to be deposited into the account of another, registered NPO ('NPO B'). While apparently separate entities, NPO A's management controlled NPO B's account, with authority to withdraw and transfer funds. NPO A gradually used the account to withdraw funds for a variety of purposes. Some of the funds were sent to a Middle East conflict zone. This gave rise to suspicions of commingling and that some of the money ultimately went to terrorist groups active in the Middle East.

Useful information in this case:

- summary of account activity
- details of the account holders, authorised signatories and beneficial owners and
- details of overseas transfers and foreign recipients.

INDICATORS PRESENT: 6, 7, 9, 21

CASE STUDY 4 — THAILAND

A private religious school was suspected of links to terrorism in the south of Thailand. Key individuals connected to the NPO received donations mainly from members of an insurgent group. The individuals transferred the funds to the school under suspicion. Authorities suspected an executive of the school (Person A) of abetting and providing financial aid to the insurgents. Person A allegedly allowed the insurgent group to use the school to promote violent ideology, deliver training and stockpile arms. A seizure order was issued to restrain the school's land, valued at 591,090 Baht (USD17,853). In December 2015, the Civil Court forfeited the land and vested it to the state.

Useful information in this case:

- details of the account holders and persons paying into the account
- transaction activity and
- any information on end-use of funds.

INDICATORS PRESENT: 10