



Australian Government

Safeguarding your organisation against terrorism financing

A guidance for non-profit organisations






Australian Government

Safeguarding your organisation against terrorism financing

A guidance for non-profit organisations



ISBN: 978-1-921241-84-0

© Commonwealth of Australia [2009]

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, 3-5 National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>

Table of Contents

SECTION A: Introduction	3
SECTION B: Best Practice Principles	8
SECTION C: Australia's international obligations	9
SECTION D: Listed individuals and organisations	10
SECTION E: Legal obligations	14
SECTION F: Due diligence	15
SECTION G: Transparency and accountability	17

What does this Guidance mean for Non-Profit Organisations (NPOs)?

This Guidance is not a legal document.

This Guidance is intended to help NPOs understand their obligations under Australian law. Like all Australian legal and natural persons, Australian NPOs must comply with Australian laws.

The Australian Government recognises the vital contribution that NPOs make in Australia and overseas. In minimising the risk of misuse of NPOs, the Australian Government is mindful of the need to not disrupt or discourage legitimate NPO activities. This Guidance is intended to support NPOs to continue their important work.

Complying with the Best Practice Principles

The Best Practice Principles (**Section B**) are intended as a guide only to describe 'best practice'.

This is not an exhaustive or comprehensive compilation. Many NPOs already have internal controls in place to promote transparency and accountability in their financial operations. Some NPOs have already implemented specific measures to reduce the risk of being misused for the purpose of terrorism financing.

NPOs should not abandon proven internal controls and practices, but should review them with a view to strengthening these controls and practices to further reduce the risk of misuse for terrorism financing.

These Principles will be reviewed and updated as necessary to ensure that they reflect emerging risks and evolving best practice.

SECTION A

Introduction

A.1 Purpose

NPOs are at risk of being misused by individuals or other organisations to finance or support terrorist activity.

This misuse can have serious consequences for NPOs. This can include criminal penalties.

This Guidance is intended to:

- build awareness of the risk of being misused for the purpose of terrorism financing
- outline **Best Practice Principles** which NPOs can adopt to help reduce this risk, and
- assist NPOs to understand and comply with legal requirements in relation to terrorism financing.

A.2 How do terrorist organisations misuse NPOs?

Terrorist activity requires financial support. One way of acquiring this support is to redirect funding intended for charitable purposes.

There are a number of ways that this can occur, including fraudulent collection of monies and infiltration of a NPO by terrorists (without the knowledge of the staff or donors).

For example, a number of terrorist organisations have created a 'front organisation' that delivers, or claims to deliver, humanitarian services. These front organisations may seek the assistance of NPOs to raise funds for a charitable cause in their region, or may be engaged by other NPOs as 'delivery organisations' (that is, they will provide the services 'on the ground' on behalf of the NPO). The front organisation may redirect part or all of the funding received from the NPO to terrorist activity. In addition, these front organisations have been known to exploit the goodwill generated in the community through the charitable activity to recruit members to their cause.



A.3 Why do terrorist organisations target NPOs?

Terrorists may target NPOs for the following reasons:

- NPOs enjoy the public trust
- NPOs can have access to relatively large sources of funds
- NPOs often use 'hard currency' (i.e. currency that is a reliable store of value and can be traded globally)
- A number of NPOs have a global presence that provides a framework for national and international operations and financial transactions
- A number of NPOs regularly work within or near those areas that are most exposed to terrorist activity, and
- NPOs are sometimes subject to 'lighter touch' regulation by government and are subject to less official scrutiny.

A.4 Why is this issue important to NPOs?

The consequences of becoming involved in terrorist financing are significant, and can include loss of reputation, status and donor confidence.

Individuals or organisations, including NPOs, may face criminal penalties if they provide financial support to a terrorist individual, organisation or act.

The *Criminal Code Act 1995* (Cth) ('the Criminal Code') sets out criminal penalties (up to life imprisonment) for providing support intentionally or recklessly to a terrorist organisation.

Penalties also apply under the *Charter of the United Nations Act 1945* (Cth) ('the Charter of the UN Act') for making assets available to a proscribed person or entity.

Section E provides further information on these laws.

A.5 What is the risk of being misused by terrorist organisations?

The NPO sector is large and diverse, with as many as 700 000 NPOs estimated to be operating in Australia.¹

Currently, the scale of known terrorist links to NPOs operating in Australia is small in comparison to the number of NPOs.

However, when considering risk, it is important to note that:

- the consequence of misuse is significant (**see Section A.4**);
- there is evidence of NPOs being misused in other countries; and
- some parts of the NPO sector are more likely to be misused than others (**see Section A.6**).

A.6 A Risk Based Approach

This Guidance recognises that the NPO sector is diverse and therefore the degree of risk of misuse across the sector will vary considerably.

NPOs should identify the specific risks to their organisation (e.g. how a terrorist may be able to infiltrate a NPO and/or fraudulently access funds) and, on that basis, form an opinion on the level of risk (e.g. high, medium or low). This assessment should inform a NPO's decision on the level of compliance with the Best Practice Principles.

In particular, NPOs face a higher risk if they:

- conduct or contribute to aid programs or projects overseas; and/or
- donate funding to other NPOs or projects overseas; and/or
- work with, or provide funding to, other NPOs that conduct programs or projects overseas.

It is important to note, however, that NPOs may still be misused even where aid or assistance is directed to beneficiaries within Australia.

The risks will increase in situations where NPOs:

- operate in regions where terrorist activity is known to occur; and/or
- use alternative remittance services or pay for goods or services in cash rather than using formal financial mechanisms (such as electronic funds transfers); and/or
- engage other individuals or organisations to deliver aid without conducting screening processes; and/or
- are not able to provide direct oversight over programs or projects.

It is important that NPOs regularly review their risks, particularly when there are significant changes to the focus or scope of the activities of a NPO.

¹ National Roundtable of Non Profit Organisations,
http://www.nonprofitroundtable.org.au/Content/NavigationMenu2/FactsandResearch/About_the_NFP_Sector/default.htm

A.7 Why is this important to the Australian Government?

The Australian Government is committed to preventing terrorism in Australia and around the world.

Australia has an international obligation to combat terrorism financing as a party to the *International Convention for the Suppression of the Financing of Terrorism* and pursuant to UN Security Council resolutions on terrorism.

Australia is also a member of the Financial Action Task Force (FATF). The FATF is an inter-governmental body which develops and promotes policies to combat money laundering and terrorism financing.

FATF Special Recommendation VIII (SR VIII) requires FATF members to 'combat the misuse of NPOs for the purpose of terrorism financing'. More information on Australia's international obligations is provided at **Section C**.

It is important that Australia contributes to reducing opportunities for terrorism financing globally. As other countries put systems in place to protect NPOs, terrorists will look to those countries where lack of awareness means that the non-profit sector is more vulnerable to misuse.

A.8 Key terms and phrases

The following section explains key terms and phrases used in the Best Practice Principles.

'All reasonable efforts' is used to reflect the need for positive action and a common sense approach, based on the level of risk, to meet legal obligations and avoid inadvertently financing terrorist activity.

'Beneficiaries' refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.²

'Funds' refers to assets of any kind or property of any kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such property or assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, debt instruments, drafts and letters of credit.³

'Listed individuals or organisations' means any individual or organisation which appears on either of the following lists:

- 'The Consolidated List' of all persons and entities subject to targeted financial sanctions under United Nations Security Council decisions and maintained by the Department of Foreign Affairs and Trade pursuant to Regulation 40 of the *Charter of the United Nations (Dealing with Assets) Regulations 2008*. This list is therefore not limited to terrorist organisations, but does include all persons and entities designated by the United Nations Security Council's Al-Qa'ida and Taliban Committee pursuant to Resolution 1267 (1999) and all persons and entities designated by the Minister for Foreign Affairs for their association with the commission of terrorist acts pursuant to Resolution 1373 (2001).
- 'List of Terrorist Organisations' – Organisations which have been proscribed by the Australian Government as terrorist organisations under the Criminal Code because they advocate the doing of a terrorist act (regardless of whether or not a terrorist act occurs), or because they are directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (regardless of whether or not a terrorist act occurs). Before an organisation can be listed the Attorney-General must be satisfied on reasonable grounds that the organisation 'is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act'.

Both lists can be accessed from: www.nationalsecurity.gov.au/npo. More information on these lists is at **Section D**.

² Financial Action Task Force, 2006. *Interpretative Note to Special Recommendation VIII: Non-Profit Organisations*.

³ This definition is contained in Section 100.1 of the *Criminal Code Act 1995* (Cth). The term 'asset' contained in Section 14 of the *Charter of the United Nations Act 1945* (Cth) is similarly defined. As the definition also includes intangible assets, this may include training or other non-monetary support.

'Non-profit organisation (NPO)' is a legal entity or organisation that primarily engages in raising or distributing funds for religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of 'good works'.⁴ This definition is not exhaustive and an entity or organisation should consider their own particular circumstances. By nature a NPO may be characterised by some of the following:

- the entity or organisation does not operate in pursuit of profit
- the entity or organisation is considered independent of the state or the political machinations of parties
- the entity or organisation may be eligible for taxation concessions under Australian law, and
- the entity or organisation derives its mandate, or reason for being, from acts that benefit or contribute to the public good.

'Suspicious activity' is any activity where a known or suspected terrorist individual or organisation is involved, or where a known or suspected terrorist act is to occur. This includes, but is not limited to, any activity involving any *listed individuals or organisations*.

'Third Party' is any individual or organisation other than a beneficiary to which the NPO provides funding or support to, or receives funding or support from, to carry out its usual functions, including fund raising and delivering aid. 'Third Party' includes, but it not limited to, partners, intermediaries, contractors, sub-contractors and service providers.

⁴ Financial Action Task Force, 2006. *Interpretative Note to Special Recommendation VIII: Non-Profit Organisations*.

SECTION B

Best Practice Principles

B.1 Overarching principle

1. NPOs must make all reasonable efforts to ensure that funds are not being directed to terrorist activities.

B.2 Legal obligations (refer Section E)

2. NPOs operating in Australia must comply with Commonwealth, State and Territory laws.
3. Australian NPOs should comply with the laws of any foreign countries that they operate in.

B.3 Risk awareness

4. NPOs should understand the level of risk that their organisation may be exposed to in relation to terrorism financing, and where risk is evident, take necessary precautions.
5. NPOs should ensure that management, staff and volunteers are aware of the level of risk that their organisation may be exposed to in relation to terrorism financing and, where risk is evident ensure that precautions are in place.

B.4 Due diligence (Refer Section F)

6. NPOs should know their beneficiaries.
7. NPOs should know the third parties they work with.
8. NPOs should regularly check that beneficiaries and third parties are not listed individuals or organisations.

B.5 Transparency and accountability (Refer Section G)

9. NPOs should conduct financial transactions where possible through regulated financial institutions, such as banks or building societies.
10. NPOs should conduct background checks of management, staff and volunteers.
11. NPOs should keep records of what assistance has been provided, who has received it, and the details of any third parties involved.
12. NPOs should conduct follow-up checks where possible to make sure that the assistance was delivered as intended.
13. NPOs should report suspicious activity to the Australian Federal Police.

B.6 Using Third Parties

Where funds are provided to a third party:

14. the NPO should make all reasonable efforts to ensure the third party is aware of, and seek assurance that the third party will comply with, all applicable laws, and the NPO should make all reasonable efforts to ensure the third party is aware of, and seek assurance that the third party will comply with these Best Practice Principles.

SECTION C

Australia's international obligations

C.1 United Nations Security Council Resolutions

On 28 September 2001, in response to the 11 September terrorist attacks in the United States, the United Nations Security Council adopted resolution 1373 (2001), imposing a series of obligations on UN Member States to suppress terrorism.

Sub-paragraph 1(c) of resolution 1373 obliges Member States to:

Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities.

C.2 Financial Action Task Force

The Financial Action Task Force (FATF), of which Australia is a founding member, has developed *Forty Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing* which include standards to combat terrorism financing. Special Recommendation VIII (SR VIII) sets out measures FATF member countries should take to ensure that NPOs cannot be misused for the purposes of terrorism financing.



SECTION D

Listed individuals and organisations

D.1 Overview

Best Practice Principle No. 8 states,

‘NPOs should regularly check that beneficiaries and third parties are not listed individuals or organisations’.

D.2 Differences between the two lists

There are two lists maintained by the Australian Government in relation to terrorism financing that NPOs should be aware of.⁵

The Department of Foreign Affairs and Trade maintains a ‘Consolidated List’ of persons and entities which are subject to a targeted financial sanction imposed by a resolution of the United Nations Security Council. This list is therefore not limited to terrorist organisations, but does include all persons and entities designated by the United Nations Security Council’s Al-Qa’ida and Taliban Committee pursuant to Resolution 1267 (1999) and all persons and entities designated by the Minister for Foreign Affairs for their association with the commission of terrorist acts pursuant to Resolution 1373 (2001). A targeted financial sanction involves the freezing of funds, other financial assets or economic resources of persons or entities on this Consolidated List. It is an offence under Australian law to use or deal with an asset owned or controlled by, or to make an asset available to, a person or entity included on this list.

The Attorney-General’s Department maintains a ‘List of Terrorist Organisations’ which have been proscribed by the Government as terrorist organisations under Division 102 of the *Criminal Code Act 1995* (the Criminal Code). It is an offence under Australian law to:

- direct the activities of the organisation
- be a member of the organisation
- recruit persons to the organisation
- receive training from or provide training to the organisation
- receive funds from or make available funds to the organisation
- provide support or resources to the organisation, or
- associate with the organisation.

While there are similarities between the two lists, there are important differences, which are outlined in Table 1 on pages 12-13. Because of the legal differences between the two lists, the inclusion of an entity on one list does not automatically require the inclusion of an entity on the other list. However, all terrorist organisations on the List of Terrorist Organisations are covered by the Consolidated List.

Both lists are available online at www.nationalsecurity.gov.au/npo.

⁵ NPOs should also be aware that other countries maintain their own lists of individuals and organisations suspected of or associated with terrorism.

D.3 Non-listed organisations can still be considered ‘Terrorist Organisations’

It should be noted that, for the purposes of the terrorist organisation offences in Division 102 of the Criminal Code, a court can determine that an organisation is a terrorist organisation – even if that organisation is not included on the List of Terrorist Organisations – if the prosecution can prove beyond reasonable doubt to a court that the organisation is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (regardless of whether or not a terrorist act occurs).⁶

Therefore, NPOs should avoid providing funds or making assets available to an organisation which it suspects as being a terrorist organisation (or having links with a terrorist organisation), even if it does not appear as a listed individual or organisation.

D.4 Access to the Lists

Both lists are available on the internet (accessible via www.nationalsecurity.gov.au/npo). The Department of Foreign Affairs and Trade (DFAT) also offers two services in relation to the Consolidated List.

- Notifications via email: Any person who is engaged in the business of holding, dealing in, or facilitating dealing in assets, may apply to DFAT for notice of updates to the Consolidated List.
- LinkMatchLite – This software is designed to assist asset holders in finding possible matches between their clients and names on the DFAT Consolidated List.⁷

To find out more, or to apply for either service, email asset.freezing@dfat.gov.au.

It is an offence under Australian law to use or deal with an asset owned or controlled by, or to make an asset available to, a proscribed person or entity. Under the Charter of the UN Regulations, individuals and organisations may request the assistance of the Australian Federal Police (AFP) to determine whether or not the asset is in fact owned or controlled by a proscribed person or entity. To facilitate this process, a referral process has been agreed between DFAT, the AFP and asset holders represented by the Australian Bankers’ Association and the major banks. The relevant referral form (available from: www.dfat.gov.au/icat/Referral_Form_to_AFP.doc) should be sent to the AFP at the following address:

AFP Operations Coordination Centre (AOCC)
e-mail: AOCC-Liaison-Ops-Support@afp.gov.au
Fax: (02) 6126 7900
Phone: (02) 6126 7555

⁶ In addition, the prosecution would have to prove that the person or organisation charged with a terrorist organisation offence (for example, making funds available to a terrorist organisation) either knew that the organisation is a terrorist organisation or was aware there is a substantial risk that the organisation is involved in terrorist activity.

⁷ Before using this software, users should note: the important licence information in the manual; that this is only one method and will miss some variations; that it requires input data in a specific format; that the internal lists are only valid until superseded; and that users must agree to the conditions of use.

TABLE 1
Differences between the Consolidated List and List of Terrorist Organisations

	Consolidated List	List of Terrorist Organisations
Respective Legislation	<i>Charter of the United Nations Act 1945 (Cth)</i>	<i>Criminal Code Act 1995 (Cth)</i>
Administered by	Department of Foreign Affairs and Trade	Attorney-General's Department
Purpose	Lists persons and entities which are subject to a targeted financial sanction imposed by a resolution of the United Nations Security Council. This list is therefore not limited to terrorist organisations, but does include all persons and entities designated by the United Nations Security Council's Al-Qa'ida and Taliban Committee pursuant to Resolution 1267 (1999) and all persons and entities designated by the Minister for Foreign Affairs for their association with the commission of terrorist acts pursuant to Resolution 1373 (2001).	Lists those organisations which have been proscribed by the Government as 'terrorist organisations' because they advocate the doing of a terrorist act (regardless of whether or not a terrorist act occurs), or because they are directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (regardless of whether or not a terrorist act occurs).
Number of entities listed	1115 individuals and organisations. ⁸	17 organisations. ⁹
How is an entity listed?	<p>An organisation can be listed:</p> <ul style="list-style-type: none"> • if it is designated by the UN Security Council itself, under country specific sanctions regimes; or • it is designated by the Minister for Foreign Affairs pursuant to UNSCR 1373 (on counter terrorism) 	<p>An organisation can be listed:</p> <ul style="list-style-type: none"> • in Regulations, because the Attorney-General is satisfied on 'reasonable grounds' that the organisation advocates the doing of a terrorist act (regardless of whether or not a terrorist act occurs) or is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (regardless of whether or not a terrorist act occurs). <p>However, it is important to note that a person may commit a terrorist organisation offence even if the Government has not listed the organisation, as long as that organisation is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (regardless of whether or not a terrorist act occurs) (See Section D).</p>

⁸ As of 25 May 2009. Subject to change.

⁹ As of 25 May 2009. Subject to change.

	Consolidated List	List of Terrorist Organisations
Exemptions	The owner or holder of an asset may apply in writing to the Minister for permission to make the asset available to a proscribed person or entity specified in the application.	None.
Offence	It is an offence under Australian law to use or deal with an asset owned or controlled by, or to make an asset available to, a proscribed person or entity.	It is an offence under Australian law to direct the activities of the organisation; be a member of the organisation; recruit persons to the organisation; receive training from or provide training to the organisation; receive funds from or make available funds to the organisation; provide support or resources to the organisation; or associate with the organisation.
Burden of proof	Strict liability offence applies for bodies corporate (meaning it is not necessary to prove that the body corporate intended to commit the offence). However, it is a recognised defence if the body corporate can prove that it took 'reasonable precautions', and exercised 'due diligence'.	For some of the terrorist organisation offences in Division 102 of the Criminal Code, it is not necessary to prove 'intent', but that a person acted 'recklessly'. 'Recklessness' is defined in the Criminal Code as being aware that there is a substantial risk that a particular circumstance exists, or a result will occur; and that having regard to the known circumstances, it would be unjustifiable to take that risk.
Penalties	For individuals: maximum 10 years imprisonment and/or a fine the greater of \$275 000 or three times the transaction value. For bodies corporate: a fine the greater of \$1.1 million or three times the transaction value.	The terrorist organisation offences in Division 102 of the Criminal Code carry penalties ranging from three years to 25 years imprisonment.
Web address	http://www.dfat.gov.au/icat/UNSC_financial_sanctions.html	http://www.nationalsecurity.gov.au and click on 'Terrorist Organisations' under the Quick Links scroll down menu

SECTION E

Legal obligations

E.1 Overview

Like all Australian legal and natural persons, Australian NPOs must comply with Australian laws.

While a NPO is not expected to have specialised legal knowledge, it is responsible for ensuring it complies with the law, and should therefore have some familiarity with relevant legal obligations.

NPOs should seek legal advice if they are uncertain of their obligations under law.

NPOs should contact their relevant State or Territory authority to determine the applicable State or Territory legislation.

SECTION F

Due diligence

F.1 Overview

A NPO may face criminal penalties if it provides funding to a third party, who then passes the funding onto a terrorist organisation.

Penalties apply under both the Charter of the UN Act and the Criminal Code for individuals and organisations which, directly or indirectly, provide funding or make assets available to a terrorist organisation.

NPOs are encouraged to take necessary steps to reduce the risk of funds being misdirected to terrorist activity via a third party. This includes:

- making best efforts to confirm the identity, credentials and good standing of third parties (see **Section F.2**) and beneficiaries (see **Section F.3**), and
- requiring assurances from the third party (as a precondition of funding) that it will not provide funding or make assets available to a terrorist organisation.

F.2 Know your third parties

Where practical, NPOs should use best endeavours to collect the following information about third parties. This could include directly requesting the information from the third party, or conducting independent searches (e.g. using web-based search engines).

If the third party is an individual, NPOs should seek the following information, where available:

- a) name (including any aliases used), date of birth and contact details (e.g. phone numbers, postal address, email and URL addresses)
- b) nationality and country of residence
- c) the name and contact details of organisations which they operate
- d) a statement of the principal purpose
- e) details of other projects/operations/initiatives/commitments, either being undertaken or already conducted by the third party – including information on the beneficiaries of these actions, and
- f) any other reasonably available information that assures the NPO of the third party's identity and integrity.

If the third party is an organisation, NPOs should seek the following information where available:

- g) the name and available contact details (e.g. phone numbers, postal address, email and URL addresses)
- h) the jurisdiction in which the organisation is incorporated or formed
- i) any other names that the organisation operates under
- j) a statement of the principal purpose
- k) corporate documents, such as:
 - i) copies of incorporating or other governing instruments,
 - ii) information on the individuals who formed and operate the organisation, and
 - iii) information relating to the beneficiary's operating history.
- l) details of other projects/operations/initiatives/commitments, either being undertaken or already conducted by the third party – including information on the beneficiaries of these actions, and
- m) any reasonably available information that assures the NPO of the third party's identity and integrity.

F.3 Know your beneficiary

The Guidance recognises that identifying beneficiaries at the individual level will often not be practical due to the number of people being assisted. However, NPOs should ensure that they have an understanding of the particular group being assisted (e.g. community, village, town, region) and be satisfied that any assistance provided to the beneficiary will not be misdirected for the purpose of terrorism financing. This could include finding out whether terrorist organisations operate in the area.

NPOs should also undertake best efforts to document the identity of their significant donors while respecting donor confidentiality.

F.4 Privacy Obligations

Where personal information is obtained from individuals for the purposes of this Guidance, it should be collected, used, disclosed and stored in a manner which is consistent with the NPO's obligations under the *Privacy Act 1988* (Cth), and any similar laws in the countries which the NPO operates in. More information about complying with the Privacy Act in Australia can be found on the Office of the Privacy Commissioner's website at: <www.privacy.gov.au>.

F.5 Emergency relief situations

It is recognised that certain aid situations, such as emergency responses to natural disasters, may present challenges to gathering information on third parties and/or beneficiaries. However, NPOs should carefully consider the risks of the particular situation (including whether terrorist individuals or organisations are known to operate in the particular region) and, within the context of this risk assessment, make all reasonable efforts to establish the identity and integrity of third parties and beneficiaries.

SECTION G

Transparency and accountability

Many NPOs already have internal controls in place to ensure funds are fully accounted for and spent in a manner consistent with the stated purpose.

Some common controls may include:

- developing and keeping records of program budgets that account for all program expenses. These budgets should indicate the identity of who will receive funding (i.e. details of third parties and/or beneficiaries) and how the money is to be used.
- protecting the administrative budget from diversion through oversight, reporting, and safeguards.
- producing annual financial statements that provide detailed breakdowns of incomes and expenditures. In many cases, NPOs will be required by law to report financial information to members and regulatory authorities.
- conducting independent financial auditing to provide an assurance that an organisation's accounts accurately reflect the reality of its finances. Many NPOs undergo audits in compliance with requirements of the *Corporations Act 2001* or relevant State or Territory legislation (such as incorporated associations legislation or charitable collections legislation and regulations). Audits may also enhance donor confidence. It should be noted that such financial auditing is not a guarantee that program funds are actually reaching the intended beneficiaries.

Where practical, NPOs should conduct direct field audits of programs (e.g. sending staff to those regions where assistance is being directed) to confirm that funding has reached the intended recipient(s) and the expected output(s) have been delivered.

NPOs should also employ the following practices:

1. Keep funds in bank accounts and use formal financial channels to transfer funding. The use of 'cash' or alternative remittance services to transfer funding should only be used as a last resort.
2. Maintain and make available to appropriate authorities, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation/program/project. Records should be maintained for at least five years, if not longer if required by law.¹⁰
3. Document and maintain information on:
 - a) the purpose and objectives of the NPO's stated activities
 - b) the identity of all employees and their current and previous involvements in other NPOs and commercial entities, and
 - c) the identity of the person(s) who own, control or direct the NPO's activities, including senior officers, board members and trustees.

This information should be publicly available either directly from the NPO or through appropriate authorities.

¹⁰ NPOs should comply with record keeping obligations required under relevant Commonwealth or State legislation.

