



**Office of the Commissioner**  
for Voluntary Organisations

---

# Protecting your Voluntary Organisation from Abuse

---

A Supporting Toolkit

---

August 2018

---

## Table of Contents

Welcome.....	6
Introduction.....	7
Why is this guidance relevant to the VO sector? .....	7
How might VOs be vulnerable? .....	7
Chapter 1:    VOs and Terrorism.....	9
What does the OCVO mean by “must” and “should”? .....	9
Technical terms used.....	10
Role of the OCVO in counter terrorism strategies.....	10
OCVO’s Approach.....	12
How might a VO be abused for terrorist purposes? .....	14
Money laundering and Counter-terrorism Legislation.....	17
Terrorist Financing.....	21
What is terrorist financing?.....	21
How might terrorist financing affect VOs? .....	21
Practical advice.....	22
Reporting Requirements.....	23
When should administrators make a report to the Police? .....	23
What to report .....	24
International Terrorist Organisations .....	25
Chapter 2:    VO’s due diligence, monitoring and verifying the end use of charitable funds.....	28
Administrators’ responsibilities.....	28
A risk based approach.....	30
What do administrators have to do for due diligence?.....	31
What do administrators have to do for monitoring and verifying the end use of funds? ...	34
Key points for administrators to remember.....	35
Tool 1: Risk Assessment.....	37
The risk assessment cycle .....	37
.....	37
Risk assessment tools.....	39
Tool 2: Risk Management.....	40
Strengths, weaknesses, opportunities and threats (SWOT) analysis.....	40

Tool 3: Risk Management.....	41
PESTLE analysis .....	41
Tool 4: Risk Management.....	42
Risk Matrix .....	42
Tool 5: Risk Management.....	45
Risk Assessment Checklist – things to talk about .....	45
Tool 6: Know your donor .....	48
Know your donor - key questions .....	48
Tool 7: Know your donor .....	51
Suspicious donations log.....	51
Tool 8: Know your partner.....	52
Know your partner – key issues to think about .....	52
Tool 9: Know your partner.....	54
Proposed partner form .....	54
Tool 10: Know your partner.....	57
Outline partnership agreement .....	57
Tool 11: Monitoring.....	63
Grant monitoring report – declaration by partner organisations .....	63
Tool 12: Monitoring.....	67
Monitoring visit checklist.....	67
Tool 13: Monitoring.....	68
Options for on-site inspections .....	68
Tool 14: Monitoring.....	69
Monitoring visit log .....	69
Tool 15: Monitoring.....	73
Project monitoring checklist.....	73
Tool 16: Due diligence.....	74
Due diligence – core principles.....	74
Chapter 3: Fraud and financial crime .....	75
What are administrators’ duties and responsibilities? .....	75
What is the purpose of this Chapter? .....	75
Why might VOs be vulnerable to fraud and financial crime? .....	76

How might VOs be vulnerable to fraud and financial crime?.....	77
What are administrators' legal duties and responsibilities? .....	79
What is the CVO's role? .....	79
How can administrators manage the risks from criminal financial abuse?.....	80
Can administrators apply a risk based approach to their duties? .....	81
What financial crimes do administrators need to be aware of?.....	83
What are 'fraud' and 'theft'?.....	83
What is 'money laundering'?.....	84
What is terrorist financing? .....	84
What other types of financial crime are there? .....	84
What are the various types of fraud, and how can administrators prevent them happening? .....	84
Income-related fraud .....	84
Expenditure fraud .....	86
Key financial controls: .....	86
Property and investment fraud.....	87
Key financial controls: .....	87
Procurement fraud .....	88
Fraudulent fundraising in the VO's name.....	88
Fraudulent invoicing and grant applications .....	89
Identity fraud/theft.....	89
Banking fraud .....	90
E-Crime.....	90
Mass market fraud.....	92
What are the Warning Signs for Fraud? .....	92
Changes in behaviour of administrators or staff who handle the accounts.....	94
What practical steps can administrators take to deal with fraud? .....	94
Implementing robust financial controls.....	96
Human resources and recruitment.....	98
Financial control policies and their implementation:.....	98
Fraud policy .....	99
Developing anti-fraud measures .....	99

Whistle-blowing policy .....	100
Practical advice on dealing with money laundering .....	100
How can VOs reduce the risk of money laundering? .....	100
What are the warning signs for money laundering?.....	102
What is a Risk-based approach?.....	102
Fraud action and response plan .....	103
Why should a VO have a fraud action and response plan? .....	103
Reporting fraud and money laundering.....	103
When should a report be made to the police?.....	103
Chapter 4: Holding, moving and receiving funds safely.....	104
Practical advice on operating bank accounts .....	104
Checklist of issues to consider when the VO receives donations from abroad .....	105
The use of intermediaries - checklist of some key risk management questions - .....	106
Checklist of some key financial controls when using intermediaries .....	107
Checklists of some key controls when making physical cash transfers.....	107
Cash Courier agreement form .....	109
Cash payments record form.....	110
Checklist of issues for administrators to consider when using other VOs or NGOs to transfer funds abroad.....	111
Chapter 5: Protecting VOs from abuse for extremist purposes .....	112
What are administrators' duties and responsibilities? .....	112
What do administrators need to do? .....	113
Conclusion .....	115

## Welcome

Dear Reader,

This toolkit is designed to help you safeguard your voluntary organisation from abuse, namely, money laundering, financing of terrorism and fraud.

One might wonder whether this type of abuse is real or apparent. We know for sure that the threat is real, locally and internationally. We cannot be sure that this is not already happening. Thus the best form of defence is offence! This toolkit and the accompanying training sessions and awareness building, is our response to the threat of abuse.

All Voluntary Organisations need to keep in mind that their existence depends on their commitment towards the cause and, more importantly, public trust. Public trust is very difficult to build but incredibly easy to lose! One case of abuse will not only impact that particular organisation, but, the whole sector. The public, on whose generous donations, your organisations depend, want you to show that funds are used responsibly and reach their end cause. If you demonstrate this, then, public support will continue and the sector will flourish.

As Commissioner for Voluntary Organisations, I urge you to take this issue seriously. Your Voluntary Organisation is precious to you and your members. Most of all it is precious to the beneficiaries whose lives are touched by your selfless giving.

Keep up the good work!

Dr Anthony J. Abela Medici

Commissioner for Voluntary Organisations

## Introduction

This document is based on the Compliance Toolkit produced by the Charity Commission for England and Wales.

It is designed to give VOs the knowledge and tools needed to manage risks and protect them from harm and abuse.

The aim is to help VOs put in place good standards of governance and accountability in place to safeguard themselves from terrorism, fraud and other forms of abuse.

The Office of the Commissioner for Voluntary Organisations (OCVO) aims to build awareness within the sector about money laundering, financing of terrorism and other illegal activities.

## Why is this guidance relevant to the VO sector?

Terrorism is a serious and continuing threat to society everywhere. This threat applies to the VO sector as much as any other sector.

Experience in other countries show that the number of cases in which there is evidence to prove that the sector has been involved in supporting terrorist activity, whether directly, indirectly, deliberately or unwittingly is very small in comparison to the size of the sector.

However, such abuse is completely unacceptable and the impact of even one proven case involving a VO is potentially significant for public trust and confidence in that organisation and the sector in general.

The risk of links or association to terrorist activity or of terrorist abuse does not apply equally across the sector and there is no 'one size fits all' approach.

## How might VOs be vulnerable?

The abuse of VOs for terrorist purposes may take a variety of different forms, including exploiting VO funding, abusing VO assets, misusing a VO name and status and setting up a VO for an illegal or improper purpose.

It may also include inappropriate expressions of support by an administrator for a proscribed organisation<sup>1</sup> or designated person or entity.

Terrorism risks may arise when funds are raised and donations received, where grant funding is disbursed, and in the provision of services and other VO activity.

---

<sup>1</sup> A proscribed organisation is one that commits or participates in acts of terrorism; prepares for terrorism; promotes or encourages terrorism (including the unlawful glorification of terrorism); or is otherwise concerned in terrorism (as per UK legislation).

Whatever the VO, its size, activities and areas of operation, those with strong governance arrangements, financial controls and risk management policies and procedures that fit their needs will be better safeguarded against a range of potential abuse, including terrorist abuse.



## Chapter 1: VOs and Terrorism

This chapter is designed to help VO administrators familiarise themselves with the legal framework which aims to protect Malta from terrorist abuse and understand how this affects VOs. It provides advice on what you should do if you discover that your VO may be working with or connected to people or organisations on terrorist lists.

The Maltese legislation concerned with these issues include Prevention of Money Laundering Chapter 373 (1994) and subsidiary legislation Prevention of Money Laundering and Funding of Terrorism Regulations Chapter 373.01 (2018).

### What does the OCVO mean by “must” and “should”?

In this guidance:

- ‘must’ means something is a legal or regulatory requirement or duty that administrators must comply with
- ‘should’ means something is good practice that the OCVO expects administrators to follow and apply to their VO.

Following the good practice specified in this guide will help you to run your VO effectively, avoid difficulties and comply with your legal duties. VOs vary in terms of their size and activities. Consider and decide how best to apply this good practice to your circumstances.

OCVO expects you to be able to explain and justify your approach, particularly if you decide not to follow good practice in this guide. In some cases you will be unable to comply with your legal duties if you don’t follow the good practice. For example:

Your legal duty:	It’s vital that you:
Act in your VO’s best interests	Implement realistic and reasonable risk management strategies to identify and mitigate risks to the VO’s funds, assets and reputation.
Manage your VO’s resources responsibly	Implement robust and effective financial controls, including undertaking appropriate due diligence on partner organisations.
Act with reasonable care and skill	Take appropriate professional advice on matters where there may be material risk to the VO (eg. before entering into a high risk activity such as funding a project in a country where terrorists are known to operate).

## Technical terms used

Some technical terms are used in this guidance. This list explains what they mean:

- Beneficiary: A person who receives benefit, financial or otherwise, from a VO.
- Statute: A legal document setting out the VO's purposes and, usually, how it's to be administered.
- Property: Includes not only land and buildings, but also investments, cash and other assets.
- Serious incident: An incident that has taken place in a VO is considered as serious if it has resulted or could result in a significant loss of funds or a significant risk to the VO's property, work, beneficiaries or reputation.
- Terrorist financing: The raising, moving, storing and using of financial resources for the purposes of terrorism.
- Administrators: VO administrators are the people who serve on the governing body of a VO. They may be known variously as directors, board members, governors or committee members. VO administrators are responsible for the general control, management and administration of a VO.

## Role of the OCVO in counter terrorism strategies

The OCVO outlines a 4 strand approach for tackling the threat of terrorist abuse in the sector:

1. Awareness - raising awareness in the sector to build on VOs' existing safeguards.
2. Oversight and supervision - proactive monitoring of the sector, analysing trends and profiling risks and vulnerabilities.
3. Co-operation - strengthening partnerships with government regulators and enforcement agencies.
4. Intervention - dealing effectively and robustly when abuse, or the risk of abuse, is apparent.

This document forms the main part of the 'awareness' strand of the strategy. A wider goal is to encourage administrators to adopt a risk-based approach to better identify and minimise potential threats, and so to reduce the potential for harm in the sector from terrorist-related abuse.

OCVO also aims to encourage and support VOs to improve their performance by working in partnership with each other and with umbrella groups (platforms), helping them to promote good practice and high standards of governance and accountability, and sharing this knowledge widely.

The Financial Action Task Force's (FATF) is the global standard setting body for anti-money laundering and counter terrorist financing. It has developed a series of recommendations for countries to implement. Collectively these represent the global standard that every country is expected to meet. FATF Recommendation 8 (R8) focuses on non-profit organisations (NPOs) and the implementation of measures so that they cannot be abused for the financing of terrorism. It tasks member countries (which does not include Malta<sup>2</sup>) to review domestic laws and regulations that relate to non-profit organisations. It proposes that countries should ensure these organisations cannot be misused:

- by terrorist organisations posing as legitimate entities
- by exploitation of legitimate entities as channels for terrorist financing including for the purpose of escaping asset-freezing measures
- to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations. The United Nations (UN) adopted Security Council Resolution 1373 (UNSCR 1373) which places barriers on the movement, organisation and fund-raising activities of terrorist groups. It requires member countries to act against terrorist financing. The UN Security Council's Counter-Terrorism Committee monitors to see if countries meet their obligations under the resolution. Malta has defined a National AML/CFT Strategy<sup>3</sup> to further mitigate the ML/TF risks it is exposed to and to address shortcomings in its AML/CFT framework. The Strategy is based on the National Risk Assessment (NRA) and a thorough gap assessment of Malta's AML/CFT framework. The Strategy comprises seven key initiatives:
  1. Establish a national coordination mechanism responsible for defining the overall AML/CFT strategy and overseeing its implementation;
  2. Strengthen and clarify the supervisory framework by extending the breadth and depth of supervision and increasing resources;

---

<sup>2</sup> Malta is a member of MoneyVal. MoneyVal is part of the Council of Europe. It is a Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. For more information please go to <https://www.coe.int/en/web/moneyval/home>

<sup>3</sup> The full document is available here <https://mfin.gov.mt/en/Library/Documents/National%20AML-CFT%20Strategy/National%20AML-CFT%20Strategy.pdf>

3. Enhance internal capabilities of the financial intelligence unit, especially in terms of staff number and training, access to additional databases and use of analytical tools;
4. Enhance investigation and prosecution capabilities with increased resources, specialisation and tools, in order to improve the number of investigations and their translation into legal enforcement;
5. Establish an effective asset recovery unit with a well-equipped agency dedicated to tracing, confiscating and managing assets;
6. Increase transparency of legal entities and arrangements, in particular with regards to their beneficial ownership;
7. Build on the existing international cooperation setup, in particular to improve the effective implementation of targeted financial sanctions and to raise the role of Malta's supervisors in international fora.

The strategic initiatives will be completed by the end of 2020.

## OCVO's Approach

OCVO as the independent and autonomous regulator of the sector is uniquely placed to protect VOs and deal with instances of terrorism or extremism related abuse in VOs. It's not a prosecuting authority and doesn't conduct criminal investigations. Where there are concerns about suspected terrorist abuse connected to a VO, it will always liaise with and work closely with the police and the Security Services as terrorist activity is a criminal offence. Its role and approach in tackling this kind of abuse is to supplement both the criminal, financial sanctions and terrorist asset freezing regimes through regulatory oversight. It may take independent regulatory action to prevent, disrupt and investigate abuse, collaborates with other regulators and sector bodies and supports administrators themselves to strengthen safeguards to minimise the risk of such abuse in their VOs.

It's the responsibility of the administrators to manage risk and safeguard their VO and its activities from all abuse, including terrorist and extremist abuse. OCVO will support you to do this, and will ensure that VOs are able to carry out their valued, legitimate and vital humanitarian and other work, within the law.

If there are concerns, suspicions or evidence that a VO is, or has been, abused for terrorist and/or extremist purposes, 3 key principles underpin OCVO's handling in these instances:

1. OCVO will not enrol an organisation that has support of terrorism explicitly or implicitly as one of its purposes.
2. The use of a VO's assets for support of terrorist or extremist activity is not a proper use of those assets and is illegal.

3. Links between a VO and terrorist activity corrode public confidence in the integrity of the VO. These links include, but are not limited to, fundraising, financial support or provision of facilities, formal or informal links to proscribed organisations and the promotion or support of extremist ideas that are conducive to terrorism and are also part of terrorist ideology. The conduct of, or views expressed by an individual connected to the VO (such as an administrator) in relation to terrorist purposes, regardless of whether those views are held or expressed in a personal capacity, may be taken into account.

OCVO's approach when looking at concerns, suspicions or evidence about VOs and links to terrorism is:

- it will deal this as an immediate priority
- where allegations are made, OCVO will liaise closely with the relevant law enforcement agencies to ensure a proper investigation of the allegations or suspicions and will co-operate fully
- the Commissioner's regulatory interest relates to the lawful exercise by VO administrators of their legal duties and responsibilities and ensuring legitimate relief continues properly to reach those in need.

OCVO will:

- take a balanced approach which is evidence-based and risk-based, targeted and proportionate
- work in partnership and collaborate with government, government entities and the VO sector itself
- maintain its independence in line with the VOA
- ensure the way it tackles the risk of terrorist abuse of VOs is within its existing approach to regulation
- encourage administrators to implement strong and effective governance arrangements, financial management and partnership management - VOs which implement good general risk management policies and procedures will be better safeguarded against all types of abuse
- make clear the responsibilities of administrators to safeguard their VO from terrorist abuse or from being used as a platform to promote inappropriate or extremist views
- as a matter of priority, deal proactively, robustly and effectively with concerns where there is evidence or suspicion of terrorist abuse of or links to VOs using our legal powers where necessary
- where necessary and proportionate, take targeted regulatory action in the VO, where its assets, services, beneficiaries or reputation are at risk of abuse or harm
- where proportionate, work with entities, providing corrective regulatory advice and guidance to ensure compliance with legal requirements to prevent problems and abuse occurring in the first place.

This is relevant to ALL Voluntary Organisations.

### How might a VO be abused for terrorist purposes?

VOs exist to create better societies. The sector is diverse and far-reaching, spanning many different types, aims, activities, sizes and places. They are however, united by a commitment to improve society, giving people a voice and improving quality of life. Many VOs tackle potential causes of alienation in communities. Some concentrate on promoting and upholding human rights. Others provide aid or supply essential services. The sector's impact is both domestic and international.

VOs extend to sections of communities that sometimes governments find hard to reach, working to deliver in extreme or adverse conditions. Their awareness and understanding of local issues is often greater than that of public or private bodies because of their closeness to the people themselves. VOs, like other parts of society, condemn terrorist acts and indeed do much to alleviate conditions that may lead people to turn to extremism or terrorism. International terrorism is motivated by an extremist ideology and exploits modern travel and communications to spread through global networks. It is ever-evolving, as terrorists continue to develop new methods and make use of new technologies.

Proven instances of terrorist involvement in the sector are rare in comparison to the size of the sector, but are completely unacceptable. However, VOs are vulnerable to terrorist and other criminal abuse for a number of reasons.

Voluntary Organisations:

- enjoy high levels of public trust and confidence, which is crucial to their success
- often rely on goodwill and voluntary support in one form or another
- are diverse in nature, providing a broad range of activities and reaching all parts of society; because of this reach, large numbers of people come into close contact with VOs, including those who may abuse them, through their services, the use of their property and through their administrators and volunteers
- are relatively easy to set up
- may depend on one or two individuals who play a key, and often unsupervised, role, particularly with smaller VOs
- some VOs work internationally, including in conflict areas and/or where there is little infrastructure, and may move money, goods and people to these areas
- often have complex financial operations including donors, possibly investments, often receiving and using cash, having to account for high volumes of small scale transactions and using informal money transfers

- may have complex programmes of operation and may pass funds through intermediary partner organisations to deliver their services, as well as operating directly themselves
- may have unpredictable and unusual income and expenditure streams, so suspicious transactions may be harder to identify
- may have branches and/or projects that are not under the direct supervision or regular control of administrator management
- may be subject to different and, in some cases, weaker levels of regulation in different parts of the world
- are powerful vehicles for bringing people together for a common purpose and collective action, and may inadvertently provide a ready-made social network and platform of legitimacy for terrorists or terrorist sentiments

Additionally, there may be factors that increase the vulnerability of some VOs; for example, those which operate in certain international areas or engage in a particular type of work. However, it is clear from the enormous diversity of the sector that the risks will vary in each case. As avenues for terrorists to exploit, particular sectors of society, such as the financial sector, are closed off, there is an increasing risk of attention focusing on others, including the VO sector. It is the purpose of this guidance to raise awareness and help VOs to develop their own risk measures and procedures. The abuse of VOs for terrorist purposes may take a variety of different forms, especially given the diverse nature of the sector. The reputation of a VO, the international reach of many VOs - including into hard to access or vulnerable communities - and their financial systems, can all provide openings for terrorists. While the risks of abuse may increase if a VO works in unstable or high risk countries abroad, the risks can be present for VOs working in the Malta as well.

VO funds, facilities and name are precious assets and vulnerable to exploitation for terrorist purposes. People who seek to abuse VOs may see them as a vulnerable target because of the high level of public trust and confidence there is in the sector.

Abuse might occur in the following ways:

- VO funding  
Funds may be raised in the name of a VO for charitable purposes, which are then used by the fundraisers for supporting terrorist purposes, with or without the knowledge of the VO. Where a VO's funds are being moved from one place to another, including internationally, they could be diverted before reaching their intended recipients. A VO might be used to launder money or be used as a legitimate front for transporting cash or other financial support from one place to

another. This risk is increased if the VO's financial controls are weak. The recipients themselves could misuse the funds, a risk that increases if proper due diligence checks are not carried out first on the recipient.

- Use of VO assets

VO vehicles might be used to transport people, cash, weapons or terrorist propaganda, or VO premises used to store them or arrange distribution. Individuals supporting terrorist activity may claim to work for a VO and trade on its good name and legitimacy in order to gain access to a region or community. They may use the VO and/or its name as a seemingly legitimate cover to travel to difficult to reach places to take part in inappropriate activities such as attending terrorist training camps. The communications network of a VO could be exploited to allow terrorists to contact or meet each other. Sometimes the VO may simply provide the opportunity for terrorists to meet. These activities may well take place without the knowledge of the VO or its administrators.

- Use of a VO's name and status

Terrorist activities may be hidden by or take place alongside additional, and otherwise legitimate, VO activities. A VO may give financial or other support to an organisation or partner that provides legitimate aid and relief. However, that organisation or partner may also support or carry out terrorist activities. A school that teaches terrorist ideology or trains terrorist recruits alongside proper classes may be able to provide full receipts for the school books bought with VO funds. Its terrorist activities would make it completely unacceptable for a VO to support that organisation. If an alternative purpose of an organisation which distributes food is to support terrorism, this is not a legitimate activity. If the organisation has relief purposes, but chooses to provide relief only to the families of terrorists or a particular terrorist organisation, this is also not legitimate activity. While each family may be in need, the unstated purpose becomes to help the terrorist or terrorist organisation's work.

- Abuse from within a VO

Although it is less likely than abuse by third parties, those within a VO may also abuse their position within the organisation and the name of VO itself for terrorist purposes. This might include 'skimming' off money in fund raising activities and sending or using the funds to support terrorist activities. People within a VO may arrange for or allow the VO premises to be used to promote terrorist activity. Administrators themselves may also be held accountable for engaging in



behaviour or making inappropriate comments for a similar purpose. VOs may invite speakers or use volunteers they know to be likely to promote terrorism to influence their work. They may abuse the VO by allowing those involved in terrorist activity to visit or work with them.

- VOs set up for illegal or improper purposes

In extreme cases, terrorists may try to set up an organisation as a sham, promoted as a voluntary organisation but whose sole purpose is really to raise funds or use its facilities or name to promote or coordinate inappropriate and unlawful activities.

## Money laundering and Counter-terrorism Legislation

The appropriate legislation referring to money laundering and counter-terrorism are as follows:

### **Chapter 373 – Prevention of Money Laundering Act**

#### **Subsidiary Legislation 373.01 – Prevention of Money Laundering and Funding of Terrorism Regulations**

### **Chapter 328A – Of Acts of Terrorism, Funding of Terrorism and Ancillary Acts**

An important document published in 2018 by the Ministry for Finance is the **National Anti-Money Laundering and Counter Financing of Terrorism Strategy**

Furthermore, one can also refer to the legislations underneath:

### **Chapter 331 – Trusts and Trustees**

Directions from the Authority (MFSA).

38C. Without prejudice to any other obligations arising under any other law, a trustee may apply to the Authority (MFSA) for directions concerning the manner in which he may or should act in connection with any matter concerning the trust or its property when such matter relates to the fulfilment of his obligations relating to the prevention of money laundering. Any bona fide communication or disclosure made in terms of this article shall not be treated as a breach of the duty of professional secrecy or any other restriction, whether imposed by statute or otherwise, upon the disclosure of information and any information disclosed in terms of this article shall be used only in connection with investigations of money laundering.

Requirements for authorisation of trustees.

43. (9) (b) The qualified person (notaries authorised to act as qualified persons) shall ensure due compliance with all fiscal, prevention of money laundering and other legal obligations in connection with relevant property and shall notify the Authority in the event that he resigns, has his engagement terminated or is otherwise hindered in performing his duties hereunder.

## **Chapter 370 – Investment Services Act**

Confidentiality.

26. (4) Where an officer or an employee of a licence holder has reason to believe that a transaction or a proposed transaction could involve money laundering or the funding of terrorism, he shall act in compliance with the reporting and other obligations set out in the regulations made under article 12 of the Prevention of Money Laundering Act and any procedures and guidance issued thereunder, and such disclosure shall not constitute a breach of confidentiality.

## **Chapter 371 – Banking Act**

Confidentiality

34. (3) Where an officer of a credit institution has reason to believe that a transaction or a proposed transaction could involve money laundering or the funding of terrorism, he shall act in compliance with the reporting and other obligations set out in the regulations made under article 12 of the Prevention of Money Laundering Act and any procedures and guidance issued thereunder, and such disclosure shall not constitute a breach of confidentiality.

(6) Notwithstanding the provisions of the Professional Secrecy Act and of article 257 of the Criminal Code, a credit institution may, where necessary for the proper carrying out of its activities or for the fulfilment of its obligations, communicate any information which is in its possession and which is related to the affairs of a customer or of a connected person to:

...(b) any auditor or expert engaged by the credit institution to carry out a compliance assessment, monitoring, auditing or a similar review in relation to any of the activities or risk management processes of the credit institution or of the group of companies of which it forms part in order to assess the credit institution's

compliance with any statutory obligations relating to the prevention of money laundering and the funding of terrorism;...

### **Chapter 403 – Insurance Business Act**

Confidentiality.

59. (5) When an officer or an employee of an authorised insurance or reinsurance undertaking has reason to believe that a transaction or a proposed transaction could involve money laundering or the funding of terrorism, he shall act in compliance with the reporting and other obligations set out in the regulations made under article 12 of the Prevention of Money Laundering Act and any procedures and guidance issued thereunder, and such disclosure shall not constitute a breach of confidentiality.

### **Chapter 487 – Insurance Distribution Act**

Confidentiality.

46. (6) When an officer or an employee of an enrolled company, or a person registered or enrolled, or an officer or an employee of such person, has reason to believe that an activity or proposed activity could involve money laundering, he shall act in compliance with the reporting and other obligations set out in the regulations made under article 12 of the Prevention of Money Laundering Act and any procedures and guidance issued thereunder, and such disclosure shall not constitute a breach of confidentiality.

All the above provisions with the exception of those found under the Trusts and Trustees Act, concern only provisions regarding disclosure of information vis-à-vis the principle of confidentiality, in so far as money laundering and funding of terrorism activities are concerned.

Then:

### **Chapter 529 – Company Service Providers Act**

1. (2) The purpose of this Act is to implement Article 36 of Directive 2005/60/EC of the European Parliament and of the Council of 29 October 2005 (attached for your consideration) on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, in so far as the said article applies to company service providers.

Requirement of registration for company service providers.

3. (1) Any person operating in or from Malta who acts as a company service provider by way of business, shall apply for registration with the Authority (MFSA) in terms of this Act:

Provided that the following persons shall not be required to be registered with the Authority (MFSA) in terms of this Act:

(a) a person in possession of a warrant, or equivalent, to carry out the profession of advocate, notary public, legal procurator or certified public accountant; and

(b) a person authorised to act as a trustee or to provide other fiduciary duties in terms of the Trusts and Trustees Act.

(2) A person in possession of another licence, authorisation or recognition in terms of the Investment Services Act who intends providing company services by way of business shall apply for registration and, in such case, the Authority shall consider any due diligence process already carried out by it.

(3) The persons referred to in sub-article (1) (a) and (b) shall notify the Financial Intelligence Analysis Unit established under the Prevention of Money Laundering Act, that they are acting as company service providers by way of business and that they are not required to register with the Authority under this Act.

Other than the above Acts, there is also Subsidiary Legislation 373.02 regarding the National Coordinating Committee on Combating Money Laundering and Funding of Terrorism Regulations. This legal notice falls under the Prevention of Money Laundering Act.

Although, these laws and regulations do not concern VOs, except as explained below, it is important to have a basic awareness:

(i) trusts which fall under the definition of “charitable purpose” and therefore qualify as voluntary organisations as regulated in terms of the Second Schedule to the Civil Code (Cap. 16 Laws of Malta);

(ii) the new provisions found under the amendments made to the Voluntary Organisations Act (Cap. 492 of the Laws of Malta) and which make reference to the Prevention of Money Laundering Act; and

(iii) the regulations governing the Registration of Beneficial Owners (Foundations and Associations) which transpose Directive 2005/849/EC (both regulations including

the amendments carried out this year and EU Directive are also attached for your consideration).

## **Terrorist Financing**

Money underpins all terrorist activity - without it there can be no training, recruitment, facilitation or support for terrorist groups. VOs play an important role in ensuring that the funds they collect are not diverted to terrorist organisations.

### **What is terrorist financing?**

Terrorist financing is the raising, moving, storing and using of financial resources for the purposes of terrorism.

Over the years, links have been discovered between money laundering and terrorist financing. Money laundering is the process of concealing the illegal origin of profits from crime. In the case of money laundering, the funds are always of illicit origin, whereas in the case of terrorist financing, funds can originate from both legal and illegal sources. The primary goal of those involved in terrorist financing is therefore usually not to conceal the sources of the money, but to conceal both the funding activity and the financial channels. Terrorist organisations may engage in generating income from legitimate businesses which could be in a different geographic location altogether, making detection more difficult. Also, terrorist attacks can be carried out by small groups, with a relatively small amount of money, and sometimes with only limited involvement in the financial system. These small financial amounts may be the very ones that are frequently considered to be of minimal risk, but are in fact open to terrorist financing and money laundering.

### **How might terrorist financing affect VOs?**

The financial abuse of VOs by terrorists may take different potential forms:

- raising funds in public collections in the name of a VO generally, or for a causes such as a humanitarian relief campaign or following a natural disaster - these funds are then diverted away from the VO and used for criminal and terrorism purposes - this may happen without the knowledge of the VO;
- establishing a VO for the purpose of providing cover for channelling funds for the purposes of terrorism, directly or indirectly;
- where VO funds are being moved from one place to another, or in different forms, for example, through international currencies or through cash transfers, in particular internationally, that may be diverted before reaching the intended recipients;
- a VO may be used to launder money;
- cash may be transported in a way that looks legitimate under the name of the VO, so its transportation may be less likely to be questioned or challenged;
- recipients of VO funds, whether partners or individuals, may misuse the money they have been given for terrorism purposes.

These risks increase if the VO's financial, due diligence and monitoring controls are weak. It is the administrators' responsibility to assess and manage risks to ensure that a VO is protected from them. Administrators must take all reasonable steps to minimise the risk that their VO's activities could be misinterpreted as promoting or supporting terrorism including by ensuring they are transparent about their work and rationale behind decisions.

There are no universally recognised criteria for assessing and determining risk in particular countries or geographic regions. However, regions that may pose a higher risk to VOs in ensuring they discharge their legal duties and responsibilities may include:

- countries that are subject to sanctions or embargoes, for example issued by the UN;
- countries identified by credible sources, such as FATF or the World Bank, as lacking appropriate anti-money laundering or counter-terrorism laws and regulations;
- regions where it is known that terrorist organisations operate;
- regions identified as having significant levels of corruption, criminal activity and poor infrastructures, possibly due to internal conflict or military action.

VOs working internationally must ensure their risk assessments take into account any relevant circumstances arising in their particular country or region of operation. Specific risks could arise from, for example, any internal conflict or other military action in a country or region, any known terrorist or criminal activity in the area, or working in a remote or sparsely populated area with limited infrastructure. At the extreme, where the risks are considered too high, the appropriate decision may be to stop working in that region, either temporarily or permanently.

### Practical advice

Factors that may affect the risk a VO is exposed to could include the following:

- political environment;
- legal protection and local laws;
- economic structure;
- cultural factors;
- location/concentration of suspected criminal activity;
- amount of illicit money generally known to be generated in a particular region or country;
- size and nature of the financial service industry and infrastructures;
- the nature and reliability of financial institutions;
- wider government and state control of a country;
- main channels used for finance, including methods of transfer and banking facilities;

- geographical location of the VO's operations;
- types of products and services offered by the VO;
- irregular economic activity and informal money transfers.

These factors, and other considerations, may differ dramatically when working in different countries.

## Reporting Requirements

### When should administrators make a report to the Police?

Administrators, VO employees or volunteers must report suspicions or beliefs about terrorist financing offences as soon as is possible to the police.

If you are concerned about an imminent threat to life and property you must contact the police immediately.

Administrators, employees and volunteers are legally bound to report any belief or suspicion of terrorist financing offences to the police. If they don't, they may commit a criminal offence.

VOs must always remain vigilant.

Article 328B (3) states that:

Whosoever promotes, constitutes, organises, directs, supplies information or materials to, or by any means, directly or indirectly, collects, receives, provides or invites another person to provide money or other property for, or otherwise finances a terrorist group knowing that such participation, involvement or financing will contribute towards the activities, whether criminal or otherwise, of the terrorist group shall be liable -

- (a) where the said participation or involvement consists in directing the terrorist group, to the punishment of imprisonment not exceeding thirty years;

Provided that where the activity of the terrorist group consists only of the acts mentioned in article 328A (2)(j) the punishment shall be that of imprisonment for a period not exceeding eight years;

- (b) in any other case, to the punishment of imprisonment not exceeding eight years.

As a matter of good practice, all VOs, regardless of size or income, should report serious incidents to the Commissioner promptly.

### **What to report**

Given the serious and significant risk to the VO concerns about links to terrorism raise, to discharge your duties, you and your co-administrators should report these concerns immediately.

Incidents which should be reported include:

- your VO (including administrators, members of staff, volunteers or anyone connected with the VO) has known or has alleged links to a proscribed organisation or other terrorist/ unlawful activity;
- someone within or closely connected to your VO, or one of your partners, is placed on an international terrorist list;
- VO funds or assets have been used to pay bribes, protection money or ransoms;
- VO funds or assets have been used/ diverted (perhaps via a partner) to support a terrorist group or terrorist activity;
- your VO has been used to circumvent asset freezing measures;
- VO personnel have been harmed by terrorist groups, including if overseas on VO work/ operations
- your VO has been a victim of fraud and/ or money laundering

You should also report to the Commissioner:

- where your VO's banking facilities are at risk of being withdrawn, perhaps because of its presence on overseas terrorist lists
- where your VO may have come into close contact with a proscribed organisation and is at risk of having committed a criminal offence
- where you're made aware of an allegation about links with terrorist or criminal activities, even if the VO considers these are unfounded

Administrators should also be aware of the risks to the VO being abused for extremist purposes; for example, when carrying out activities and events involving guest speakers or when promoting literature and educational materials, perhaps via the VO's website and on social media.

You should report to the Commissioner if:



- you know or suspect that your VO's premises or activities have been misused as a platform for the expression or promotion of extremist views, or the distribution of extremist materials;
- you become aware of media reports alleging that your VO has been misused for such purposes, particularly if you believe these could damage your VO's reputation

By reporting serious incidents promptly you help show that you're discharging your duties and acting responsibly.

### International Terrorist Organisations

The table below shows a list of terrorist organisations according to the US Department of State.

Date Designated	Name
10/8/1997	Abu Sayyaf Group (ASG)
10/8/1997	Aum Shinrikyo (AUM)
10/8/1997	Basque Fatherland and Liberty (ETA)
10/8/1997	Gama'a al-Islamiyya (Islamic Group - IG)
10/8/1997	HAMAS
10/8/1997	Harakat ul-Mujahidin (HUM)
10/8/1997	Hizballah
10/8/1997	Kahane Chai (Kach)
10/8/1997	Kurdistan Workers Party (PKK, aka Kongra-Gel)
10/8/1997	Liberation Tigers of Tamil Eelam (LTTE)
10/8/1997	National Liberation Army (ELN)
10/8/1997	Palestine Liberation Front (PLF)
10/8/1997	Palestine Islamic Jihad (PIJ)
10/8/1997	Popular Front for the Liberation of Palestine (PFLP)
10/8/1997	PFLP-General Command (PFLP-GC)
10/8/1997	Revolutionary Armed Forces of Colombia (FARC)
10/8/1997	Revolutionary People's Liberation Party/Front (DHKP/C)
10/8/1997	Shining Path (SL)
10/8/1999	al-Qa'ida (AQ)
9/25/2000	Islamic Movement of Uzbekistan (IMU)
5/16/2001	Real Irish Republican Army (RIRA)
12/26/2001	Jaish-e-Mohammed (JEM)
12/26/2001	Lashkar-e Tayyiba (LeT)
3/27/2002	Al-Aqsa Martyrs Brigade (AAMB)

3/27/2002	Asbat al-Ansar (AAA)
3/27/2002	al-Qaida in the Islamic Maghreb (AQIM)
8/9/2002	Communist Party of the Philippines/New People's Army (CPP/NPA)
10/23/2002	Jemaah Islamiya (JI)
1/30/2003	Lashkar i Jhangvi (LJ)
3/22/2004	Ansar al-Islam (AAI)
7/13/2004	Continuity Irish Republican Army (CIRA)
12/17/2004	Islamic State of Iraq and the Levant (formerly al-Qa'ida in Iraq)
6/17/2005	Islamic Jihad Union (IJU)
3/5/2008	Harakat ul-Jihad-i-Islami/Bangladesh (HUJI-B)
3/18/2008	al-Shabaab
5/18/2009	Revolutionary Struggle (RS)
7/2/2009	Kata'ib Hizballah (KH)
1/19/2010	al-Qa'ida in the Arabian Peninsula (AQAP)
8/6/2010	Harakat ul-Jihad-i-Islami (HUJI)
9/1/2010	Tehrik-e Taliban Pakistan (TTP)
11/4/2010	Jundallah
5/23/2011	Army of Islam (AOI)
9/19/2011	Indian Mujahedeen (IM)
3/13/2012	Jemaah Anshorut Tauhid (JAT)
5/30/2012	Abdallah Azzam Brigades (AAB)
9/19/2012	Haqqani Network (HQN)
3/22/2013	Ansar al-Dine (AAD)
11/14/2013	Boko Haram
11/14/2013	Ansaru
12/19/2013	al-Mulathamun Battalion (AMB)
1/13/2014	Ansar al-Shari'a in Benghazi
1/13/2014	Ansar al-Shari'a in Darnah
1/13/2014	Ansar al-Shari'a in Tunisia
4/10/2014	ISIL Sinai Province (formerly Ansar Bayt al-Maqdis)
5/15/2014	al-Nusra Front
8/20/2014	Mujahidin Shura Council in the Environs of Jerusalem (MSC)
9/30/2015	Jaysh Rijal al-Tariq al Naqshabandi (JRTN)
1/14/2016	ISIL-Khorasan (ISIL-K)
5/20/2016	Islamic State of Iraq and the Levant's Branch in Libya (ISIL-Libya)
7/1/2016	Al-Qa'ida in the Indian Subcontinent
8/17/2017	Hizbul Mujahideen (HM)
2/28/2018	ISIS-Bangladesh

2/28/2018	ISIS-Philippines
2/28/2018	ISIS-West Africa
5/23/2018	ISIS-Greater Sahara
7/11/2018	al-Ashtar Brigades (AAB)

## **Chapter 2: VO's due diligence, monitoring and verifying the end use of charitable funds**

### **Administrators' responsibilities**

The public and those donating to a VO should have confidence that money donated is used for legitimate purposes and is reaching its intended beneficiaries.

Administrators are the custodians of their VOs. They are publicly accountable, and have legal duties and responsibilities under VO law to safeguard their VO, its funds and property.

The best way that administrators can ensure a VO's funds are not abused in the first place is by putting in place good governance and ensuring there is strong financial management, including having robust internal and financial controls and risk management procedures. A significant aspect of an administrator's legal duty to protect VO assets and to do so with care means carrying out proper due diligence on those individuals and organisations that give money to, receive money from or work closely with the VO.

Where VOs give money to partners and beneficiaries, especially large amounts of money or in high risk situations, making sure that adequate monitoring takes place is crucial. This means verifying that VO funds or property reach their proper destinations and are used as the VO intended. What an individual VO and its administrators must or should do in their VO and what is a proportionate approach to adopt will depend on a range of factors. These will include various aspects of the VO's work and the associated risks, how much money is involved, whether the VO works with partners and whether those partners or the VO's funds are overseas, and if so, where.

The aim of this chapter is to make all VO administrators aware of their duties and responsibilities in carrying out due diligence checks and monitoring in relation to the VO's involvement with external bodies and individuals.

This chapter is primarily intended for administrators and others in their VO, but will be of interest to donors and organisations which give grants to VOs to deliver project work in Malta and abroad, so they understand administrators' responsibilities under VO law. The 'tools' are particularly aimed at smaller and medium sized VOs. The guidance will also assist partner organisations and other delivery agents which VOs engage to carry out their work and help them to understand why a VO may have certain reporting requirements or need certain information from them.

What are the risks of not having effective due diligence and monitoring?

Most of the time VOs have good relations with their donors, partner organisations and beneficiaries who give to or work with VOs in good faith. However, practical risks do exist and VOs can be abused in a number of ways, for example:

### **Donors**

1. Money laundering: donors can make loans to VOs as a means of laundering money through a VO or they can make donations with specific restrictions as to which partner or project is to be funded as a means of transferring funds overseas and disguising the origin of the funds.
2. Proceeds of crime: anonymous cash donations or donations through suspect third parties may be a means of disposing of the proceeds of crime.
3. Tax avoidance/evasion: donors may seek tax relief on their donation while at the same time seeking private benefit as a result of their donation or insist that the VO purchase services from an associated company as a condition of the donation, thereby obtaining tax relief on the donation and securing business at the same time.

Administrators should be aware of any funding relationship which involves a return of part or whole of the cash donated to the donor or where the donor benefits in any substantial way as a result of making the donation. Third parties making donations on behalf of a donor who wishes to remain anonymous may also be a cause of suspicion unless the third party is reputable or allows administrators to know the name of the donor with the proviso that this is not made public.

### **Beneficiaries**

Knowing who a VO's beneficiaries are is particularly important if the VO makes grants of cash or other financial support directly to individual beneficiaries; or if distribution of cash or support is through a third party. Without due diligence and sound procedures, payments may be made to individuals who do not qualify as beneficiaries and who are seeking to abuse the VO.

### **Partners**

Partners who are funded to implement a project or deliver aid are in a position to abuse these funds unless:

- the VO is sure they are bona fide organisations

- the VO has evidence that the partner can implement the programme in the way expected
- the partner's internal management and financial control systems enable them to identify and report losses or abuses back to the VO

Overseas partners may be subject to control by or have affiliations with proscribed organisations or designated entities, or have weak internal controls which means that their funds are potentially open to fraudulent claims or theft by others.

In the light of these types of threat, it is vital that administrators take a risk based approach in their relations with their donors, beneficiaries, and partners.

### **A risk based approach**

Administrators' legal duties and responsibilities apply to all VOs and all administrators, whatever the VO, its size and activities. What this means in practice, however, depends on the circumstances. The extent, form and detail of the required project and partner due diligence checks and monitoring, and how this should extend to donors and beneficiaries, will depend on the nature of the risks in the particular circumstances, the activities the VO carries out, and how and where they are undertaken. This is why a risk-based and proportionate approach is important and more appropriate than a 'one-size-fits-all' approach.

Administrators cannot apply a risk based approach randomly. The legal duties apply to all administrators of all VOs subject to the law of Malta, whatever their income, and whether or not they are based, operate or work internationally. However, what action is reasonable or proportionate to take to ensure administrators comply with these duties will vary from one VO to another. VOs can apply a risk based approach to this.

The starting point is the greater the risks, the more VO administrators need to do.

All VOs must have, as a minimum:

- some form of appropriate internal and financial controls in place to ensure that all their funds are fully accounted for and are spent in a manner that is consistent with the purpose of the VO; what those controls and measures are and what is appropriate will depend on the risks and the VO;
- proper and adequate financial records for both the receipt and use of all funds together with audit trails of decisions made; records of both domestic and international transactions must be sufficiently detailed to verify that funds

have been spent properly as intended and in a manner consistent with the purpose and objectives of the organisation;

- given careful consideration to what due diligence, monitoring and verification of use of funds they need to carry out to meet their legal duties;
- taken reasonable and appropriate steps to know who their beneficiaries are, at least in broad terms, carried out appropriate checks where the risks are high and have clear beneficiary selection criteria which are consistently applied

### What do administrators have to do for due diligence?

Due diligence is the range of practical steps that need to be taken by administrators so that they are reasonably assured of the provenance of the funds given to the VO; confident that they know the people and organisations the VO works with; and able to identify and manage associated risks.

What administrators need to apply to undertake due diligence can be described as the 'Know your' principles:

- know your donor;
- know your beneficiaries; and
- know your partner

These are the principles that administrators should follow to ensure that they meet their legal duties under VO law when they are selecting donors, partners and beneficiaries.

The core elements of due diligence across each of the 'Know your' principles involve administrators taking reasonable steps to ensure they:

- **identify** – know who they are dealing with
- **verify** – where reasonable and the risks are high, verify this
- **know what the organisation's or individual's business** is and can be assured this is appropriate for the VO to be involved with
- **know what their specific business is with the VO** and have confidence they will deliver what the VO wants them to
- **watch out** for unusual or suspicious activities, conduct or requests

### Know your donor

VO administrators need to put effective processes in place to provide adequate assurances about the identity of donors, particularly substantial donors, and to verify this where it is reasonable and necessary to do so (identify and verify).

Most VOs should know, at least in broad terms, where the money they are being given comes from (such as grants or cash donations). It does not mean VOs must question every donation or ask for personal details about every donor.

Administrators are likely to need to carry out further due diligence and take steps to identify and verify the identity of more significant donors so they can assess any risks. If there is a significant donor which is an organisation, the VO should know what their business is and be assured that the organisation is appropriate for the VO to be involved or associated with.

Administrators should also be reasonably assured about the provenance of funds and the conditions attached to them (administrators should know what their specific business is with the VO). If there are particular risks, for example where an unfamiliar donor operates a business or is perhaps from a country outside of Malta, about which public concerns have been raised, then the administrators should take more steps to verify the provenance of the funds.

The Know your donor principle does not mean VOs cannot accept anonymous donations. This is perfectly acceptable providing VOs look out for suspicious circumstances and put adequate safeguards in place.

A VO's responsibility is not to work out if a donation is illegal or if it is being asked to use a donation for illegal purposes. However, administrators should carry out good due diligence and report concerns and suspicious activities.

### **Know your beneficiaries**

A common sense approach to the Know your beneficiaries' principle is required. Administrators have a duty to ensure that their VO's funds are used for its beneficiaries, so it is important that administrators are clear, in a general sense at least, about who the beneficiaries are. The amount of detailed knowledge at an individual level will depend upon the activities of the VO and the number of beneficiaries.

For example, a VO providing a recreation ground does not choose its beneficiaries as such and clearly, there is no need to check and verify the identity of members of the public who walk across or use the ground. The principle is more likely to apply to VOs which restrict access to services or activities to a certain number of beneficiaries.

Administrators need to be alert to the risk that some people abuse VOs by making false applications to the VO for grant funding or for individual assistance, including creating beneficiaries that do not exist.



Again, a VO's responsibility is not to investigate or determine criminality. Administrators should carry out good due diligence and take enough reasonable steps to satisfy themselves their beneficiaries are genuine. If they suspect a crime has been committed, or the VO's money or help is being used for illegal purposes by a beneficiary, they must report their concerns and suspicious activities to the appropriate authorities.

Where decisions are made regularly about selecting which particular individual receives services or support from a VO, administrators need to take reasonable and appropriate steps to ensure that:

- they know who those individuals are
- where the risks are high, appropriate checks are carried out
- it is appropriate for the VO to provide assistance to them, both in terms of them meeting any eligibility criteria, and there being no concerns that the VO's assistance will not be used as intended

### **Know your partner**

Administrators must carry out appropriate and proper due diligence on individuals and organisations that the VO gives grants to or uses to carry out charitable projects and help deliver its work. This involves the administrators assessing the risks to ensure that those partners are suitable and appropriate for them to work with. Due diligence steps are likely to include obtaining the key details about who the partner is, where it is based and who the VO will be involved with. These details are likely to be required in practice anyway to arrange for payment of any funds to the partner. Where the risks are high, or the more significant or substantial the work or partnership is, administrators will need to carry out more extensive due diligence, taking steps to identify and verify the identity of the partner and further assess the risks.

Administrators should have reasonable confidence that they know enough about what the partner's business is and they are an appropriate partner for the VO to be involved with, as well as being clear what they intend to deliver for the VO, when and how (administrators should know what their business is with the VO).

It is for administrators to decide the level of due diligence and the type of checks they need to carry out. The nature and extent of due diligence checks should be proportionate to the risks involved in the project and from entering into a new relationship or extending an existing one.

Administrators need to be alert to signs that the VO's funds will not be properly or legitimately used by partners.

### **What do administrators have to do for monitoring and verifying the end use of funds?**

Administrators must be able to demonstrate that funds have been used for the proper purposes for which they were intended. Monitoring is an important way for administrators to ensure they are able to account for the proper use of the VO's funds and that they maintain donor confidence. This includes taking appropriate and reasonable steps to verify the proper end use of funds where the funds are provided to partners.

Monitoring may take a variety of forms depending on the nature of the VO's work, the particular project and amount of funds involved. It will almost always include steps to verify the proper end use of funds.

Drawing up robust monitoring processes, and recording and implementing them will help administrators ensure that funds are adequately protected from abuse, misuse or other loss, and are being put to their most effective use.

Monitoring will usually involve steps aimed at ensuring:

- the VO's funds can be accounted for
- there is an audit trail showing the expenditure of funds by the partner
- the funds were received by the partner and if the partner forwarded those funds on, there is an audit trail to show this
- the partner has actually delivered the project
- the VO's funds have been used for the purposes for which they were intended and the beneficiaries identified by the VO have benefitted
- any concerns that need to be dealt with are identified

The risk based approach recognises that not all partners and financial transactions need to be monitored in exactly the same way. However, if monitoring reveals suspicious circumstances or that non-compliance may have taken place, then there will be much less flexibility in how administrators deal with this.

Verifying the end use of funds is one aspect of monitoring. It is the process of ensuring money has both physically reached the partner and that it has been spent properly and as the VO intended.

## Key points for administrators to remember

### Due Diligence

- 1) Look out for suspicious circumstances and exceptional features.
- 2) Have clear policies and procedures in place to ensure you as administrators, your staff and volunteers know what to do if they identify something suspicious or which poses particularly high risks.
- 3) Where there is a cause for concern carry out further checks.
- 4) Make sure you report suspicious activities to the relevant authorities, including the police, if you think a crime has been committed.
- 5) Carefully consider and record any decisions to refuse donations or accept donations which may present particularly high risks.
- 6) Be alert to the risk that some people abuse VOs by making false applications to the VO for grant funding or for individual assistance, including creating beneficiaries that do not exist; people who may appear to be legitimate beneficiaries may make requests for support they do not qualify for or need.
- 7) Be alert to signs that the VO's funds will not be properly or legitimately used by partners.
- 8) Keep a written record of due diligence processes and the results which informed your decision making.
- 9) Have reasonable assurance that any partner your VO is going to work with can deliver the activities or services required.
- 10) If you suspect that a partner may be bogus or you are suspicious about them or their work, consider not taking forward the proposed project with the partner.
- 11) It is good practice to protect the VO's position with a partnership agreement.
- 12) Seek professional advice where appropriate.

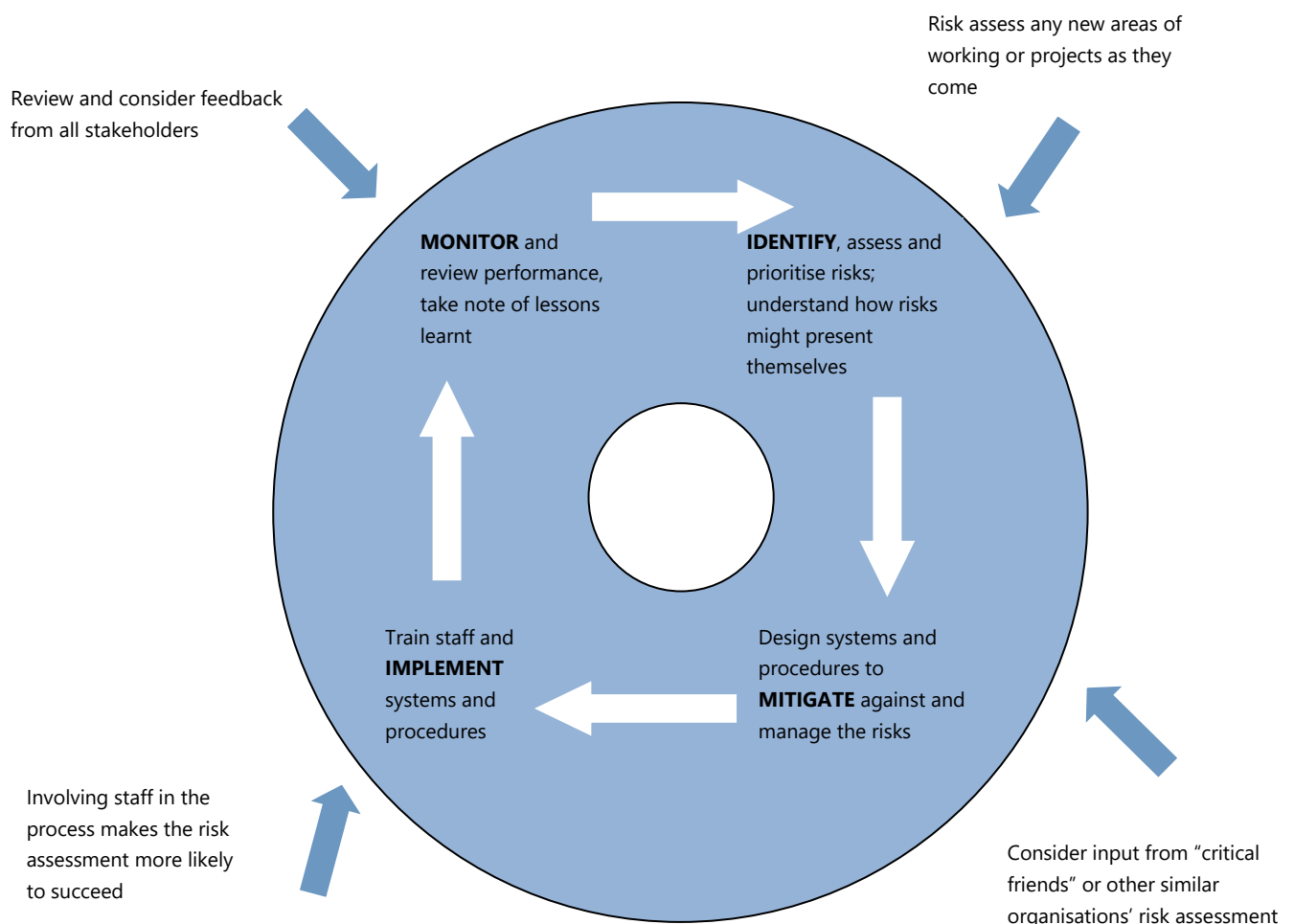
### Monitoring

- 1) Consider which monitoring tools work best for you and your VO's work.
- 2) Make sure the monitoring you carry out is effective and credible.
- 3) Ensure your staff and agents are competent to undertake monitoring and any conflicts of interest are dealt with properly.
- 4) Make sure you keep an audit trail for the movement of funds from your VO to your partners.
- 5) Make sure you keep an audit trail and proper records (such as receipts and invoices) that show the partner has spent the funds as intended and for proper purposes.

- 6) Look out for signs of suspicious activities or signs that audit trails and other records may not be in order.
- 7) Consider asking for progress reports from partners.
- 8) If you carry out joint monitoring, ensure you put safeguards in place and are clear about who is doing what.
- 9) Consider some form of reporting back of significant project work to donors and supporters of the VO.
- 10) Where there is a cause for concern carry out further checks.
- 11) Make sure you report suspicious activities to the relevant authorities, including the police, if you think a crime has been committed.
- 12) Make sure your VO's culture is that abuse and misconduct are not acceptable and your administrators, staff and volunteers know this.

## Tool 1: Risk Assessment

### The risk assessment cycle



### Guidance on how a risk assessment cycle usually works

#### **Stage 1:** carry out a risk assessment

No matter what size they are, VOs which consider risk and its management in a structured way and make a clear risk management statement in their annual report are likely to benefit in many ways. This includes enhancing VOs' effectiveness and accountability, and strengthening their reputations among beneficiaries, partners, donors, supporters and the public.

There are various frameworks available for identifying the risks and carrying out a risk assessment that may be suitable for a VO to consider when planning programme operations.

Once the various risks have been identified their likelihood and impact need to be evaluated. In practice it may be reasonable to exclude risks where both impact and likelihood are assessed as low and to focus attention and valuable resources on areas of risk with the highest impact.

**Stage 2:** use processes and procedures and take action to mitigate and manage risks. Once the risks are identified and evaluated, administrators can draw up a plan for the steps that they consider need to be taken to address or mitigate significant or major risks.

There are 4 basic strategies that can be applied to manage a recognised risk. These strategies can be identified as the 4 Ts:

- 1) **Transfer** the financial consequences to third parties or share it. In this context, for example, through the terms or conditions of a partnership agreement or grant that enable the VO to claw back the grant or payment in certain situations.
- 2) **Terminate** the activity giving rise to the risk completely. In this context, for example by refusing the grant or not accepting the project or stopping a particular activity or service.
- 3) **Treat** the risk through effective management. In the context of giving grants or supporting projects, the best way to manage risk is to carry out proper due diligence and act on its results, ensuring there is suitable and regular reporting. Other ways of managing specific risk include making grants in smaller amounts conditional on certain events happening, or satisfactory reporting and auditing, or making an initial grant first and making it easy to terminate this.
- 4) **Tolerate** the risk as one that cannot be avoided if the activity is to continue. An example of this might be where administrators take out an insurance policy that carries a higher level of voluntary excess or where the administrators recognise that in an emergency situation the main concern is to get aid to those who need it. Not all risks can be avoided entirely. The general approach is that the greater the risk the more that administrators need to do to be able to demonstrate that they have discharged their duty to manage it.

The cost of managing a risk should usually be proportionate to the potential impact. A balance will need to be struck between the cost of further action to manage the risk and the potential impact of the residual risk. However, a short term or one-off

cost must be assessed against the long term benefits, assurances required and donor and public expectations.

Some common risks that will need to be considered in the context of due diligence and monitoring are noted.

### **Stage 3: training staff and implementing systems**

Procedures and processes only work if they are properly implemented. VO staff, volunteers and other personnel need to know what those procedures are and how they work. They will need adequate training to ensure they are familiar with the systems and procedures. It is very important that they know what action to take if they suspect misconduct and criminal financial abuse. By understanding their own and others' roles and responsibilities, individuals are more likely to be able to identify and report wrongdoing.

There should be clear reporting systems in place for staff and others working with the VO if they become aware of any activity that causes them concern. Staff and volunteers should know how to report their concerns, including concerns about the conduct of administrators or senior managers as well as about systems and individual events. If administrators know, suspect or have cause for concern that an individual is misusing the VO for their own purposes or misappropriating funds, they must take immediate and appropriate action to investigate and resolve the issue.

Sometimes causes for concern will be identified by the VO's beneficiaries or members of the public. It is therefore important that systems are in place for them to raise their concerns with the VO.

### **Stage 4: monitor and review performance**

Risk management extends beyond simply setting out systems and procedures. The controls identified to mitigate the risks must be capable of implementation, and the implementation (and its effectiveness) should be appropriately monitored.

Risk management procedures need to be sufficiently flexible and responsive to ensure that new risks are addressed as they arise. They should also involve periodic checks in order to identify new risks proactively and ensure that the approach to risk management remains fit for purpose. Risk management is not a one off event and should be seen as an ongoing process that will arise out of monitoring and assessment.

### **Risk assessment tools**

The following tools are not intended to replace the risk assessment processes that VOs are already using. Their suitability will depend on the particular structure and activities of each VO and the risks to which it is exposed. Large VOs are likely to have sophisticated risk assessment processes in place. The examples of tools that follow

are designed to help smaller VOs, with fewer employees, which do not have access to professional advice and support.

The risk assessment tools comprise:

- SWOT analysis (tool 2)
- PESTLE analysis (tool 3)
- Risk matrix (tool 4)

## Tool 2: Risk Management

### Strengths, weaknesses, opportunities and threats (SWOT) analysis

This example shows how a SWOT analysis can be used by administrators to help identify and assess the risks associated with entering into a new partnership with another organisation to carry out the VO's purposes.

<b>Strengths:</b> attributes of the partner, project or activity that will help to achieve the objective or improve the outcome.	<b>Weaknesses:</b> attributes of the partner, project or activity that might cause problems, be harmful to the quality of the outcome, or potentially prevent the objectives from being achieved.
<b>Opportunities:</b> conditions or resources which could be used to help achieve the objectives, or which could help to improve the outcome.	<b>Threats:</b> events or conditions which could restrict the achievability of the objectives, or which could damage the quality of the outcome.



### Tool 3: Risk Management

#### PESTLE analysis

Political	Factors may be altered by the government's influence on a country's infrastructure. This may include tax policy, employment laws, environmental regulations, trade restrictions, tariffs, reform and political stability. VOs may need to consider where a government does not want services or goods to be provided.
Economic	Factors include economic growth, interest rates, exchange rates, inflation, wage rates, working hours and cost of living. These factors may have major impacts on how VOs operate and make decision.
Social	Factors include cultural aspects, health and safety consciousness, population growth rate and various demographics.
Technological	Factors include ecological and environmental aspects and available products and services. VOs may need to innovate, having considered the compatibility with their own technologies and whether they are transferable internationally.
Legal	Factors include any law which may impact on the VOs' operations, including NGO regulation and criminal and terrorist legislation which will differ from country to country.
Environmental	Factors include an awareness of climate change or seasonal or terrain variations which may affect VOs' service delivery methods.

## Tool 4: Risk Management

### Risk Matrix

A Risk matrix is another common method for assessing risk, which can be used in conjunction with the SWOT and PESTLE analyses. Administrators may find this method useful when assessing areas of risk, for example when planning a new project to be carried out with a new partner organisation. The identification of appropriate risks may be best undertaken by involving those with a detailed understanding of the VO's operations and work and/or detailed knowledge of the particular operating environment or the nature of particular projects.

The level of risk should be measured by both the likelihood of something occurring and the severity of impact if it were to happen. The risk matrix can subsequently be used as a risk register for ongoing monitoring and review of risk throughout the life of a project. The following is an example of a section of a risk matrix.

Areas	Risk	Likelihood	Impact	Controls
Reputation	A real or perceived link or association between the VO and terrorist activity damages the VO's reputation.	LOW	HIGH	<ul style="list-style-type: none"><li>• draw up detailed partnership agreements</li><li>• review partner's governance structures</li><li>• review project audit and monitoring, including field visits</li><li>• include an impact and risk assessment for all projects</li><li>• take references and contact other affiliates of the partner for recommendations</li><li>• request standard documentation and invoices</li></ul>

				<ul style="list-style-type: none"> <li>• check the consolidated list of designated individuals and entities</li> </ul>
Financial/ Criminal	Financial loss, fraud, money laundering, terrorist financing.	MEDIUM	HIGH	<ul style="list-style-type: none"> <li>• clear responsibilities and segregation of duties</li> <li>• scheme of delegation</li> </ul>
	Failure to comply with regulations.	HIGH	MEDIUM	<ul style="list-style-type: none"> <li>• developing and implementing a fraud policy</li> </ul>
	Exchange rate losses or gains.	MEDIUM	MEDIUM	<ul style="list-style-type: none"> <li>• purchases and tender controls, reconciliations of cash book to petty cash and bank, expenses procedures and authorisation limits</li> </ul>
	Funds or assets provided are not used for the intended project or misappropriated.	LOW	MEDIUM	<ul style="list-style-type: none"> <li>• monitor exchange rate losses or gains and review impact on expenditure and income</li> <li>• use bank accounts and procedures</li> <li>• quarterly project financial reviews and project reports</li> <li>• documented financial procedures</li> </ul>

				<ul style="list-style-type: none"> <li>• regular budget monitoring and forecasting and grant management</li> </ul>
Security	<p>Risk to staff and / or beneficiaries</p> <p>Obstacles to the effective delivery of services</p> <p>Areas of conflict, political instability, hostile government</p>	HIGH	HIGH	<ul style="list-style-type: none"> <li>• country specific security risk assessment</li> <li>• crisis management policy and procedure</li> <li>• health and safety security training</li> </ul>

## Tool 5: Risk Management

### Risk Assessment Checklist – things to talk about

#### The activity/project

- Is the activity clearly within the VO's objects?
- Are proper policies and procedures in place to prevent beneficiaries being put at risk?
- Are partners/staff/volunteers sufficiently trained to be able to carry out the work?
- What lessons has the VO learnt from its own previous experience, or that of other organisations working in the same area and/or type of activity?

Comments

#### Legal

- Are there any specific laws and requirements to be aware of in carrying out the activity?
- Are there any local or EU sanctions in force?

Comments

#### Finance

- What is the VO's financial position and is there enough money available to support the proposed activity?
- Will there be an impact on tax (for example, VAT implications)?

- How will the money get to the project site? Will it go through bank accounts direct to the recipient?
- Will cash couriers be required?

Comments

### Partners

- Are partners involved?
- What risks does this pose?
- Have these partners been involved before?
- Will a written agreement be in place?
- What are the risks of the partner not delivering?
- Can money be recovered if necessary?
- What problems might there be?

Comments

### External Factors

- What factors are outside the administrators' direct control?
- VOs working internationally should ensure their risk assessment takes account of any relevant circumstances arising in their particular country or region of operation. Specific risks could arise from working in an area where there may be:
  - internal conflict or other violent or military action
  - known terrorist or criminal activity

- poor infrastructure in remote or sparsely populated areas
- changes in government/political environment
- lack of banking facilities
- high levels of bribery and corruption

## Tool 6: Know your donor

### Know your donor - key questions

These questions are not intended to be asked in respect of each donor. However, administrators may need to consider them depending on the risk, including the size and nature of the donation, and whether it appears to have any suspicious characteristics.

#### General information

- Who are the donors?
- What is known about them?
- Does the VO have a well-established relationship with them?
- Do any additional identity checks need to be made? Full use should be made of internet websites, particularly to check whether a donor organisation is registered with another regulator. Registration may provide access to the organisation's accounts and governing document
- Are the donors Malta taxpayers?
- In what form is the money being received? Cash, cheque, bank transfer?
- Have any public concerns been raised about the donors or their activities? If so, what was the nature of the concerns and how long ago were they raised?
- Did the police or a regulator investigate the concerns? What was the outcome?
- Would any adverse publicity about the donor have a damaging effect on the VO?

Comments
----------

#### The nature of the donation and any conditions

- How big is the donation?
- Is it a single donation, or one of a number of regular donations, or the first of multiple future donations?
- Is the donation one of a series of interest-free loans from sources that cannot be identified or checked by the VO?
- Are there unusual or substantial one-off donations?



- Does the donation come with any conditions attached? What are they? Are they reasonable?
- Is there a condition that funds are only to be retained by the VO for a period and then returned to the donor, with the VO retaining the interest?
- Is the donation conditional on particular organisations or individuals being used to apply the funds?
- Is the donation conditional on being applied to benefit particular individuals either directly or indirectly?
- Is there a suggestion that the VO is being used as a conduit for funds to a third party?
- Is the donation in sterling or another currency, perhaps with a requirement that the donation be returned in a different currency?
- Are any of the donors based, or does the money originate, outside Malta? If so, from which country?
- Does this country/ area pose any specific risks?
- Are donations received from unknown bodies or international sources where financial regulation or the legal framework is not rigorous?
- Is the donation received from a known donor but through an unknown party or an unusual payment mechanism where this would not be a typical method of payment?
- Is anything else unusual or strange about the donation?

Comments

What administrators should do if they are suspicious?

- If due diligence checks reveal evidence of crime, administrators must report the matter to the police and/or other appropriate authorities.
- If the administrators have reasonable cause to suspect that a donation is related to money laundering and/or terrorist financing, they are to report the matter to the police.
- Such issues should be reported to the CVO, especially if significant sums of money or other property are donated to the VO from an unknown or

unverified source. This could include an unusually large one-off donation or a series of smaller donations from a source you cannot identify or check.

- Check the donor against the lists of financial sanctions targets and proscribed organisations.
- Consider whether to refuse the donation

Comments

## Tool 7: Know your donor

### Suspicious donations log

Name of donor			
Amount of donation		Date received	
Form of donation (cash, cheque, bank transfer)			
Name of Bank			
Account Number / Name			
Swift Code		IBAN	
Name of cheque signatory			
Currency used			
Nature of suspicion / reason for query			
Any previous donations from this source?			
Any conditions attached to the donation?			
Action to be taken (indicate all that apply)	Report to police		
	Report to CVO		
	Refuse donation		
	Other action		

## Tool 8: Know your partner

### Know your partner – key issues to think about

Key partner details	<p>Are you satisfied with the partner's status and governance? Consider checking:</p> <ul style="list-style-type: none"><li>• its governing document</li><li>• the proscribed organisation list</li><li>• the designated entity list</li><li>• the consolidated list of financial sanctions target</li></ul> <p>Carry out internet searches and review local media to identify if, for example, the organisation has any links with political activity.</p>
Representatives and structures	<p>Who are the key senior personnel?</p> <p>Are the organisation's size, management and operational structure fit for purpose?</p> <p>Can you be reasonably sure the organisation is able to deliver the services required?</p> <p>How easy is it to contact the organisation's senior representatives and other key staff?</p>
Practical working relationship	<p>What do you know about the partner? Have you worked with them before?</p> <p>Does your experience of working with the partner in the past raise any concerns?</p> <p>Are its aims and values compatible with those of your VO?</p> <p>Are there likely to be any language, communication or cultural problems? How can these be overcome?</p> <p>Is the partner already working with other organisations? Will this present any problems?</p>

	<p>Are there arrangements in place to enable you to monitor the services provided? Are you confident about any third parties involved in monitoring and feedback?</p>
Accounting and internal financial controls	<p>Are the partner's financial controls generally adequate and reliable?</p> <p>Are its financial policies and procedures documented?</p> <p>What recording and audit systems are in place, and are these suitable for the type of work being undertaken and the scale of funding involved?</p> <p>Will the VO be able to inspect the partner's financial records?</p> <p>Are there any concerns about banking local arrangements and the movement of funds? If so, have these been addressed satisfactorily?</p> <p>Does the partner have adequately trained and qualified staff to manage funds, maintain accounts and report back to the VO?</p> <p>How closely do the partner's senior staff monitor its more junior staff?</p>
External risk factors	<p>What special risk factors apply to the area in which the partner organisation will operate? Will the organisation be able to deal with these? For example:</p> <ul style="list-style-type: none"> <li>• what is the political, economic and social environment?</li> <li>• is there any potential or actual instability, unrest or conflict?</li> <li>• are there health and safety concerns for VO representatives?</li> <li>• would external factors affect your ability to monitor the VO effectively?</li> </ul>

## Tool 9: Know your partner

### Proposed partner form

Basic Information	
Name of partner	
Working name (if applicable)	
Principal address	
Website	
Main Contact	
Name	
Telephone & Email	
Administrators	
Name	
Address	
Name	
Address	
Name	
Address	
Senior Management Staff	
Name	
Address	
Name	
Address	
Name	
Position	
Name	
Position	
Legal status formation of partner organisation	
Legal status	
Type of governing document (attach copy)	
Date established	
Country	
VO registration (if applicable)	
Relevant policy documents (attach)	
Working languages	

Brief description of partner's objectives and activities			
Bank details			
Name of bank			
Swift Code		Account Number	
Partnership with other organisations (if any)			
Proposed partnership work			
Outline of project			
Technical and other skills necessary			
Estimated overall cost			
Estimated time scale			
External and other risks identified			
Assurance			
Summary of other due diligence checks carried out			
Confirmation of partner complying with regulatory requirements			
Partner's accounts examined – last 3 years (if applicable)			
Year ending			
Comments			
Year ending			
Comments			
Year ending			
Comments			
Partnership agreement signed (attached)			
Date signed			
Position of partner signatory			
References taken up (attached)			
Other "open source" checks (details attached)			
Overall conclusion as to suitability, including			

assessment of capacity to deliver project	
Board Approval	
Date and Signature	



## Tool 10: Know your partner

### Outline partnership agreement

#### Important

This is not intended to be a definitive model agreement, but a guide and check-list. Every project and partnership will be different, and the content of the agreement will vary according to the particular situation. Legal advice in preparing the agreement, or reviewing it, is highly recommended, particularly where there is a significant level of funding, or where reputational risk is at stake.

Where the VO is entering into the partnership to enable the delivery of services which the VO is contracted to deliver by another body or donor, or where the funds have been supplied by a donor with particular conditions or restrictions attached, the terms of the partnership agreement should set the same or higher standards and obligations on the partner, to ensure that the VO does not inadvertently default on its head contract or funding agreement.

Key items that the partnership agreement is likely to need are set out below.

#### **1. Date of agreement**

#### **2. Title of agreement/project**

#### **3. Parties' names and addresses**

#### **4. Brief overview of nature and duration of agreement**

For example, "The VO and the partner agree to work together for the implementation of the project during the period 1 January 2019 to 31 December 2020 in accordance with the terms set out in this partnership agreement dated 15 December 2010 'the agreement'".

Brief summary of the purpose and aims of the project and the key deliverables. (Further detail is provided in the project Implementation document annexed to the agreement.)

#### **5. The VO's responsibilities and obligations.**

For example:

- to provide ongoing assistance to the partner in implementing the project within the limitations of resources and funding at its disposal for these purposes
- to advance funds in accordance with the agreed budget (annexed to the agreement) to the partner in a timely manner to a bank account nominated by the partner
- to carry out monitoring visits on dates as set out in the visit and reporting schedule (annexed to the agreement) or where the VO otherwise considers such a visit is reasonably required, and has given the partner reasonable notice in advance of the visit
- to make available to the partner assistance from appropriate and qualified personnel to provide expert technical advice on the project, whose fees will be funded by the partner in accordance with the budget
- to give reasonable consideration and a prompt response to requests from the partner for adjustments to the budget

## **6. The partner's obligations**

For example:

- to implement the project in accordance with the agreement, using its best endeavours to complete the activities and deliverables listed in the project implementation document (annexed to the agreement), within the budget and to target timescales
- to co-ordinate and co-operate with the VO, and to make available to the VO information relating to the project, including the submission of financial and narrative reports required by the visit and reporting schedule (annexed to the agreement) or such other material as the VO may reasonably request
- to comply with the financial reporting requirements (annexed to the agreement), and to request the funds required to implement the project in accordance with the budget (annexed to the agreement)
- to monitor regularly the project's progress, and to adapt activities where necessary and with the VO's prior agreement so as to ensure that the project is fully implemented within the total amount of the budget

- to manage the project in accordance with the VO's policies (annexed to the agreement)
- to facilitate visits to the project, in accordance with the visit and reporting schedule (annexed to the agreement)
- to use its best endeavours to ensure that no funds provided under the agreement are used for any purpose other than the project, or for any improper purposes, or purposes unlawful in Malta or the partner's country of operation, including money laundering, supporting terrorist activity, inappropriate private benefit, or for political purposes; nor to assist or be in contact with any person suspected of such activities; and to report any such suspicions to the VO as a matter of urgency
- in the event of the partner sub-contracting any aspect of the project to local partners, the partner must:
  - before selecting a local partner, conduct appropriate due diligence to ensure that the partner has compatible values, and the capacity and expertise to perform the sub-contract
  - put in place a binding written agreement with the local partner containing terms and conditions that reflect those in the agreement
  - regularly monitor and review the local partner's implementation of the project

## **7. Standard clauses**

For example:

- how disputes will be dealt with and by whom – internal and/or external to the VO and the partner (alternative dispute resolution, jurisdiction?)
- how the agreement can be terminated
- the conditions under which the VO can withhold funds
- force majeure clause (what will happen in the event of any exceptional and insurmountable situation beyond the control of the parties, which affects the parties' ability to fulfil their obligations under the agreement?)
- who are the appropriate contact persons for each party to the agreement?

- confidentiality clauses?
- intellectual property considerations?

## **8. Signature by authorised officers on behalf of each party to the agreement**

## **9. Annexes**

For example:

- **Project implementation document**

Clearly setting out the details of the project:

- specific activities to be undertaken or other milestones
- where it should be delivered
- the nature of the beneficiaries
- the timeframe
- SMART objectives and deliverables (qualitative and quantitative), that is, **S**pecific (simple, sensible, significant), **M**easurable (meaningful, motivating), **A**chievable (agreed, attainable), **R**elevant (reasonable, realistic and resourced, results-based), and **T**imely (time-based, time limited, time/cost limited, timely, time-sensitive).

- **Budget**

Setting out different heads of expenditure and amounts allocated to each. For example:

- staff costs (recruitment, salary, pension, other benefits, training)
- travel costs (travel tickets, subsistence, insurance)
- external costs (procurement of project items, legal fees, auditors, consultancy, bank charges, meeting/event costs, grants to other organisations/individuals)
- office costs (rent, telephone, internet, postage, stationery, printing, artwork/design, office equipment, photocopying)

- **Financial reporting requirements**

Setting out minimum financial standards the partner should follow. For example:

- maintenance of proper records for a specified period
- auditing requirements
- accounting requirements (keeping funds ring-fenced, accounting in such a way as to enable monthly monitoring of expenditure)
- how financial transactions should be conducted/authorised
- budget monitoring and forecasting requirements
- treatment and permitted levels of under spend or overspend
- treatment of exchange rate gains or losses
- how funds are drawn down (tied in with reporting)
- currency and exchange rate to be used for financial reporting
- **Visit and reporting schedule**
  - dates for submission of reports (monthly/quarterly/annually/on project milestone dates/project end)
  - periods which reports should cover
  - format of reports (financial and narrative)
  - dates for site visits
  - format for site visits
  - responsibilities of the partner for site visits
  - responsibilities of the VO for site visits
- **Relevant policies**

Where a partner agency does not have its own policies in place, or its policies do not meet the standards to which the VO wishes it to adhere, the VO should explore whether the partner is willing and to adopt the VO's own policies, for the purposes of the partnership work.

Such policies may include:

- child protection
- staff security
- procurement
- staff handbook
- health and safety
- serious incident reporting

- insurance
- finance

## Tool 11: Monitoring

### Grant monitoring report – declaration by partner organisations

Basic Information				
Partner name				
Address				
Principal contact				
Name				
Telephone				
Email				
Project for which grant being made				
Project duration				
Start Date		Estimated end date		
Reporting period				
From		To		
Report due date		Submitted on		
Report Type	Monthly <input type="checkbox"/>	Quarterly <input type="checkbox"/>	Six-monthly <input type="checkbox"/>	Annually <input type="checkbox"/>
Amount of grant in Euro and local currency				
Whether single grant or stage payment				
Single grant (tick)	<input type="checkbox"/>	Stage Payment	<input type="checkbox"/>	
Frequency of Payment	Monthly <input type="checkbox"/>	Quarterly <input type="checkbox"/>	Six-monthly <input type="checkbox"/>	Annually <input type="checkbox"/>
Payment Number	Payment [ ] of [ ] payments			
Period for which grant is being made				
From		To		
Total amount of grants to date (including this one)				
Next request for funding expected on				
Project Objectives and deliverables				
Summarise planned key stages and deliverables				
Describe progress achieved so far and whether				

progress is on time				
State reason for any significant variation from plan and action required.				
Narrative report submitted				
Yes <input type="checkbox"/> (attach)	No <input type="checkbox"/>	State why and attach evidence		
Summary of achievements and deliverables met (if any)				
Any delays in project implementation. If yes, explain why.				
Summary of main risks, challenges or significant issues.				
Significant changes to project plans and / or activities				
Financial reporting				
Budget utilisation report	Yes <input type="checkbox"/> No <input type="checkbox"/>			
Type of documentation received	Invoices/Bills <input type="checkbox"/>	Bank statement <input type="checkbox"/>	Management Accounts <input type="checkbox"/>	Audit reports <input type="checkbox"/>
	Other			
Budget monitoring report	Yes <input type="checkbox"/> No <input type="checkbox"/>			
Date and amount of funds last received				
Amount requested for next funding period				
Summary of overall budget and expenditure year to date, including variance				
Overall budget				
Disbursed				
Variance Amount	%	€		
Summary of action required				



to correct variance	
Specify any new funding received	
Source	
Amount	
Purpose	
Duration	
Specify any key changes in personnel	
Summary of arrangements for periodic financial reports to be made	
Beneficiary / Impact	
Details of services provided through the project, including number and distribution of beneficiaries (if applicable)	
Any proposed changes to agreed selection criteria	
Any proposed changes to agreed identified beneficiaries	
Do beneficiaries know their entitlements?	
Have reports been given to beneficiaries and other stakeholders?	

Feedback received (attach or summarise as appropriate)	Government Agencies <input type="checkbox"/> Beneficiaries <input type="checkbox"/>	NGOs <input type="checkbox"/> Other <input type="checkbox"/>
Declaration		
The information provided on this form, and attached supporting documents, are a true and accurate report of project activities and use of funds provided by the VO.		
Signed		
Date		
Position		

## Tool 12: Monitoring

### Monitoring visit checklist

Here is a checklist of some questions and factors that may be useful when considering how best to carry out a monitoring visit:

- how much control do you have over the inspection and questions that will be asked?
- will you be able to influence the scope of the visit?
- are there any health or safety concerns about visiting the project or area in which it is being carried out?
- are there any restrictions as to who can visit the project or location?
- what knowledge and expertise does the person carrying out the monitoring visit have, for example, will they be able to assess whether items have been purchased at a reasonable price or if the standards being met are suitable for the region?
- do you need to verify independently the feedback you receive?
- are there language and/or communication issues?
- how will these be addressed?
- what form does the inspection/visit report need to take?
- is it a one-off visit?
- if not, how often will they take place?
- are there any timing issues?
- are there any the local laws which affect record keeping?
- are the records likely to be readily available?
- are there any local customs that might impact the information required or evidence, for example, is it unusual in the location to receive a receipt as proof of purchase?
- are there any conflicts of interest issues?
- if problems are identified, how will this be reported back to the administrators (or funders) and how quickly will this be done?

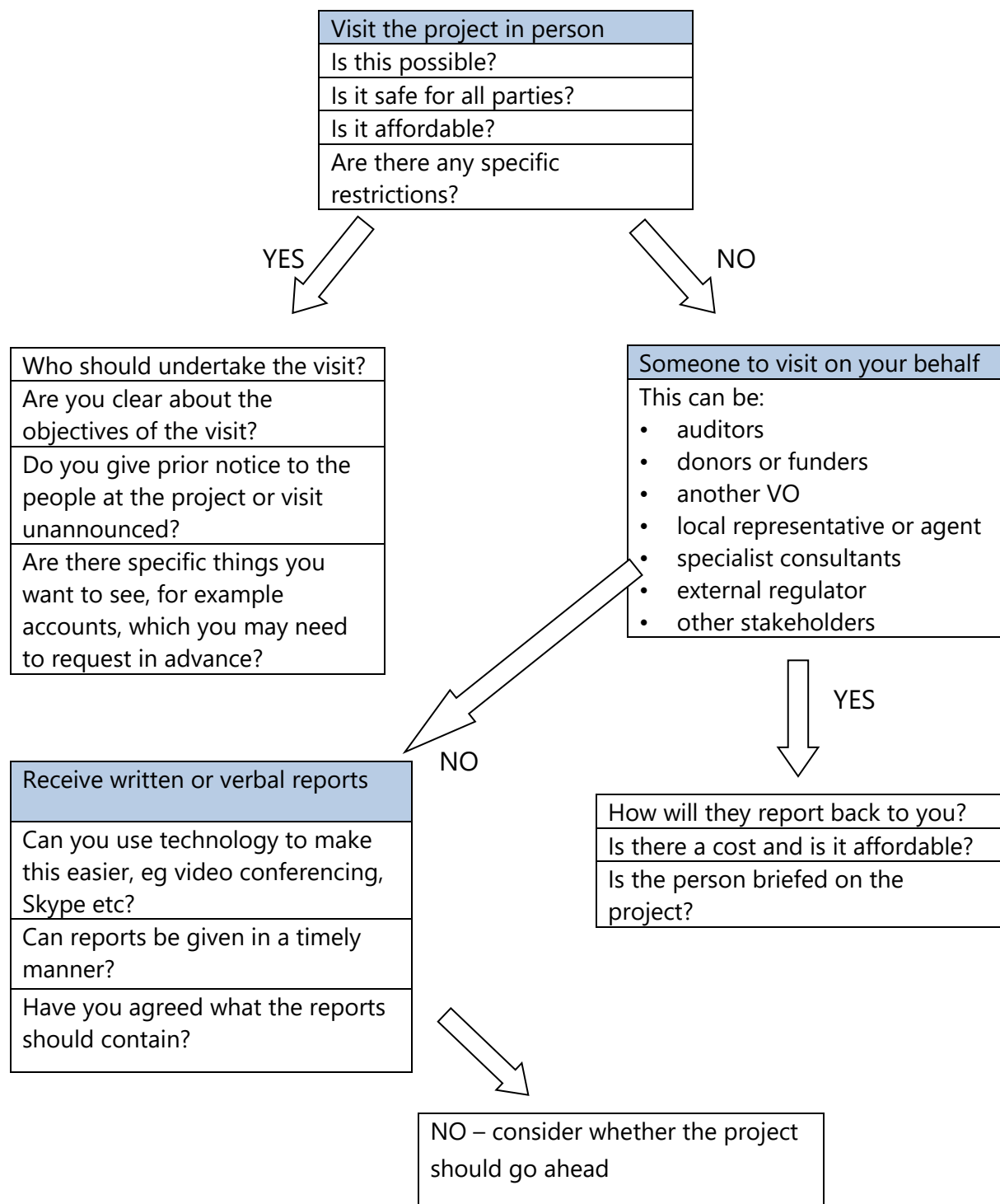
Comments

--

## Tool 13: Monitoring

### Options for on-site inspections

Some form of monitoring is essential to ensure that the VO's funds are being used for proper purposes. In some cases on-site inspections are the only reliable method, but it is not always practicable for administrators to carry out the inspections. This flowchart may help in assessing the different options and their merits.



## Tool 14: Monitoring

### Monitoring visit log

Basic Information			
Partner Name			
Project address & principal contact on site			
Address			
Contact name and position			
Duration of the project			
Start date		Estimated end date	
Date of visit			
List of staff / representatives met			
Name			
Representing		Position	
Name			
Representing		Position	
Name			
Representing		Position	
Project objectives and milestones			
Outline of key project milestones / stages (if appropriate)			
Milestone/stage			
Progress to date, including significant delays, changes and costs			
Milestone/stage			
Progress to date, including significant delays, changes and costs			
Milestone/stage			
Progress to date, including significant delays, changes and costs			
Description and assessment of partner's own			

records of progress and monitoring; whether consistent with inspection	
Financial records	
Records and audit trails covering:	
<ul style="list-style-type: none"> <li>Income / receipts</li> </ul>	
Whether record-keeping system is adequate and in accordance with agreement	
Evidence of Income retained	
Income approved at correct level	
<ul style="list-style-type: none"> <li>Expenditure</li> </ul>	
Whether record-keeping system is adequate and in accordance with agreement	
Evidence of expenditure retained	
Expenditure approved at correct level	
Budgeting	
Whether record-keeping system is adequate and in accordance with agreement	
Evidence of income /	

expenditure retained	
Income / expenditure approved at correct level	
Areas of concern	
Nature of concern	
Recommended action	
Nature of concern	
Recommended action	
Nature of concern	
Recommended action	
Progress to date	
Assessment and evidence of project delivery to date	
Direct observation of project work/ activity	
Feedback from beneficiaries	
Name (where appropriate)	
Comment	
Name (where appropriate)	
Comment	
Feedback from independent stakeholders and / or observers	
Name & position	
Comment	
Name & position	
Comment	

Photographic/ video/media evidence (attached)			
Future progress			
Current project risks			
Risk			
Rating of risk			
Action to mitigate risk			
Risk			
Rating of risk			
Action to mitigate risk			
Other comments			
Conclusion			
Overall assessment			
Log completed by			
Name			
Position		Date	
Signature			



## Tool 15: Monitoring

### Project monitoring checklist

Robust monitoring processes will help to satisfy administrators that funds are adequately protected from abuse and have been put to proper use. These should also be capable of identifying system weaknesses and breakdowns at an early stage so that action can be taken to put things right. And at the end of the project, good quality monitoring feedback will help administrators to see whether there is anything that can be improved in the planning of future projects.

The following is a checklist of some of the main general questions to ask as part of the monitoring process.

When monitoring a project, the following questions will help administrators to determine whether due diligence checks were adequate and VO funds are being used effectively and appropriately:






- how does performance and delivery link to agreed milestones and targets?
- is the quality of activities/services delivered acceptable?
- can all the money sent be accounted for?
- is there sufficient proof of expenditure?
- are there sufficient financial controls in place?
- have there been any significant changes in personnel?
- has the project actually been carried out?
- have the project activities, services or funds reached the intended identified beneficiaries?
- are all funds, assets and premises accounted for?
- were any significant problems encountered? If so, were these reported promptly to the VO and dealt with effectively?
- are there any lessons that can be learnt to improve future performance and quality?

Comments

--

## Tool 16: Due diligence

### Due diligence – core principles

Identify		know who you are dealing with
Verify		where reasonable, and the risks are high, verify identities
Know what the organisation's or individual's business is		and can be assured this is appropriate for the VO to be involved with
Know what their specific business is with your VO		and have confidence they will deliver what you want them to
Watch out		for unusual or suspicious activities, conduct or requests

## Chapter 3: Fraud and financial crime

### What are administrators' duties and responsibilities?

Administrators have a legal duty and responsibility under VO law to protect the funds and other property of their VO so that it can be applied for its intended beneficiaries. They must also comply with the general law (and overseas law where applicable) including in relation to the prevention of fraud, money laundering and terrorist financing.

Fraud will flourish in an environment of weak governance and poor financial management. So this means that the protection of VO funds begins with having robust financial control systems within a framework of strong and effective governance.

### What is the purpose of this Chapter?

This Chapter aims to highlight some of the types of fraud and financial crime to which VOs are vulnerable and provide some practical advice for administrators on how to tackle it. The VO sector is very diverse, and sometimes highly specialised; not every VO will experience every type of fraud or crime mentioned. However, if administrators have an awareness of fraud and financial crime risks they will be better equipped to recognise them. This guidance will also help administrators to devise and implement measures to manage the risks.

Sound financial management is an increasingly important factor in determining people's trust and confidence in VOs. So it is vital for VOs to reassure the public that the money they donate to the VO is used properly and goes to the causes for which it is intended.

Fraud and financial crime can have a particularly damaging impact on a VO. The loss of funds may only be the beginning; forensic investigation, legal advice and recovery costs can be considerable, and in some cases may exceed the amount lost. There are also indirect consequences: the negative effect on VO administrators and staff morale may adversely influence service delivery, and the impact on the VO's reputation and resources can be irreversible. All of this can seriously threaten the security and very existence of a VO with modest resources.

Clearly, the best approach is to prevent fraud, financial crime or indeed any financial abuse happening in the first place. VO administrators have a legal duty to take all necessary steps to protect their VO's funds and assets from misuse, and to comply with the general law on fraud and financial crime. The starting point is to make sure

that the VO's governance framework includes good, robust financial controls together with effective risk assessment and due diligence. Although good systems will not necessarily prevent fraud and financial crime altogether, they will lessen its likelihood, help to maximise the chances of recovery if it does happen and minimise the opportunities for any recurrence. They will also send strong signals to criminals and those who seek to abuse a VO that they will not get away with it. Sound financial controls and financial management are an essential defence for VOs against fraud and financial crime. They should be a core part of a VO's culture, and practised to the same degree of excellence as a VO's activities.

### **Why might VOs be vulnerable to fraud and financial crime?**

VOs are also heavily reliant on altruism, trust and honesty. They enjoy high levels of public trust and confidence, so appearing to be associated with a VO can give a criminal enterprise a veneer of respectability.

Many VOs in Malta are small or medium sized entities. Such organisations tend to rely on a small number on volunteers, to supervise the funds and assets of the VO and these arrangements may lack the scrutiny and division of duties possible in larger organisations. The reliance of VOs on cash-based fund raising may make the sector attractive to both opportunist and organised fraudsters. And the ethos of VOs, built on voluntarism and pursuit of a common and shared goal, may create a degree of trust amongst individuals and staff which allow the unscrupulous to operate with less suspicion.

VOs can be attractive to fraudsters and financial criminals because they:

- may believe that nobody would abuse a VO, so VO administrators might not think to ensure strong financial controls;
- often rely on goodwill and voluntary support in one form or another, making it less likely that problems are identified or criminals pursued;
- often depend on one or two individuals who can play a key or largely unsupervised role in running the VO;
- form a hugely diverse sector, are involved in a wide range of activities and reach all parts of society, so patterns of financial abuse may be harder to identify and prevention methods need to be adapted to work efficiently
- may have unpredictable and unusual income and expenditure streams that can make suspicious transactions and financial trends harder to identify;

- may have an international presence, sometimes in areas of conflict and/or where there is poor financial infrastructure or operate in cash intensive environments;
- may have complex financial systems involving multiple donors or investments, and high levels of cash income and expenditure;
- may need to use carry out multiple transfer of funds locally and overseas;
- may have partners through which they deliver work and pass funds
- may have branches and/or projects that are not under the direct or regular control or supervision of the VOs' administrators;
- may have insufficient staff to allow for proper segregation of duties;
- can be set up as sham organisations to disguise what are in reality illegal public fundraising and other activities

### **How might VOs be vulnerable to fraud and financial crime?**

Financial abuse may occur within a VO, carried out by someone involved in or connected to it, or the VO may be the victim of crime committed by entirely external individuals or entities.

VOs can be victims of crime in the same way as other sectors and individuals and this risk can never be completely eliminated. Financial abuse of a VO can be committed by individuals outside of a VO or by other organisations. For example, fraudulent fundraising in the name of a VO or VOs generally, or on behalf of defunct, bogus or non-existent VOs. Incidents may be isolated, or they might form part of a systematic plan over a long period of time.

However, sometimes abuse takes place by those close to or connected with the VO, which is particularly serious. Administrators are in a position of trust. VOs depend on trust. The public, donors and those involved in VOs depend on them to protect VO funds and assets. Sadly, sometimes people involved with VOs in positions of trust with specific financial responsibilities abuse that trust.

The risk of financial crime exists at every stage of a VO's activity, from the point at which income is generated and received, through the internal management and decision making and eventually to the end use of funds. Some VOs may face additional or particular risks because of the activities they undertake, but no VO can regard itself as being immune to the risk. All administrators must ensure that they are aware of the risks their VO faces, assess them objectively and take appropriate and proportionate steps to manage them in the context of their particular VOs and what they do.

Fraudsters and criminals are becoming increasingly sophisticated in their methods, adopting new technologies and targeting organisations' vulnerabilities. This emphasises the importance of regularly reviewing and updating financial controls and safeguards against fraud, and highlights the importance for administrators to be aware of what is going on in their VOs. There is a very clear need for VOs to protect themselves by adopting or reinforcing anti-fraud initiatives.

VOs working internationally may face an increased risk of financial abuse from fraud, or theft because of the complexity of working across borders where there may be less control or where local conditions make it hard to apply controls. Administrators of these VOs may need to address particular challenges, for example relying on alternative methods for transmitting funds abroad, or trying to establish clear audit trails when working with partner agencies abroad. (See the 'Due Diligence' and 'Know Your' principles in Chapter 2). Moving funds overseas creates extra opportunities for them to go missing because of, for example, conversion to other currencies, conversion of cash into goods and back again and, in some areas, local corruption, the absence of formal banking systems and unregulated local customs and practices.

Financial crime does not necessarily involve large amounts of money. Depending on the VO's size and the work it undertakes, fraud involving relatively small amounts can still result in significant damage. There is much that VOs can and should do to be fraud-aware.

Criminals may exploit VOs by misappropriating charitable funds through fraud, theft, money laundering or diverting charitable funds from legitimate charitable work. Examples of the types of fraud and financial crime that VOs may be susceptible to include:

- banking system theft and fraud;
- misuse of the VO's bank account;
- fraudulent credit or debit card transactions or charges;
- intercepting postal donations and cheques;
- failing to pass on money from public collections;
- stealing or 'skimming-off' money from cash collections;
- fake fundraising events and requests for donations;
- theft from VO shops and trading activities;
- using the VO's databases or inventories for personal profit or unauthorised private commercial use;
- fake grant applications the creation of false invoices or purchase orders;

- the creation of false employees or inflated expenses, overtime or other claims;
- providing services to beneficiaries who do not exist, and other forms of identity fraud.

### **What are administrators' legal duties and responsibilities?**

This means that administrators must:

- do their best and take reasonable steps to help prevent financial abuse of the VO's funds in the first place;
- make sure that proper robust financial controls and procedures suitable for their VO and its activities are in place;
- ensure they act responsibly when, and in the interests of the VO, dealing with incidents of fraud and crime

### **What is the CVO's role?**

The Commissioner does not investigate or prosecute crime. Our concerns and regulatory interest is about:

- protecting the VO's funds and assets and ensuring public trust and confidence in the VO;
- ensuring administrators comply with their legal duties and responsibilities in the management and administration of the VO.

Our remit does not extend to investigating or prosecuting criminal activity although we do work closely with other agencies. Action taken by the Commissioner will usually be focused on considering whether there has been misconduct or mismanagement in the administration of the VO in how the financial abuse and illegal activity has arisen or been allowed to occur, as well as ensuring going forward the VO's funds are protected and the administrators are taking steps to recover lost funds, where it is reasonable to expect them to do so.

We will pass on information and report information to the police and law enforcement agencies.

We may need to do, or consider, one or more of the following:

- clarifying the extent to which the VO and its personnel are involved in, or responsible for any alleged incident;

- whether the administrators have handled any allegations and concerns properly and responsibly, particularly where they involve an administrator or someone senior with financial responsibility within the VO;
- ensure administrators are taking responsibility for ensuring they have proper financial controls in place and that these are reviewed, where appropriate, after an incident and proper checks are carried out for those employed to have particular responsibility for the VO's money.

The CVO's role is not to be prescriptive about the detailed range and type of financial controls that are appropriate for each VO; that is for the administrators to decide. However, as the VO regulator the CVO has a responsibility to promote public trust in VOs and to ascertain that administrators are fulfilling their legal duty to protect their VOs.

### **How can administrators manage the risks from criminal financial abuse?**

The risk from financial fraud and abuse can never be completely ruled out. However, proper and adequate internal financial controls play an important part in managing this risk. Administrators are responsible for the effective administration of the VO and have a legal duty to safeguard VO assets. Funders, donors, supporters and beneficiaries are entitled to expect proper standards of management and financial control.

If the VO falls victim to financial crime resulting from administrators not putting adequate financial controls in place, then the administrators will have failed to meet their legal duties to the VO.

When reviewing financial controls to ensure they are fit for purpose, administrators should take into account changes in the VO's structure, activities and area of operation that could affect the risks to the VO.

Changes in the types of threat the VO may face also need to be considered, for example new or emerging methods of fraud, to ensure such risks are properly managed. It can be difficult to identify financial abuse as criminals may be adept at presenting their activities as legitimate and lawful. Establishing the identity and legitimacy of any organisation the VO works with can reduce such risks.

Administrators should also consider how the VO will react to different types of financial crime should they occur. There should be procedures for reporting known or suspected crime or abuse and clarity about how reports of concerns will be investigated.



Adequate training should be provided to staff and volunteers to ensure they are familiar with the VO's financial controls and know what actions to take if they suspect criminal financial abuse. Staff and volunteers should know how to report their concerns within the organisation, including concerns about the conduct of administrators or senior managers. If administrators know or suspect an individual is misusing the VO for their own purposes or misappropriating funds they should take immediate and appropriate action to resolve the issue.

VOs often rely on computer systems to receive information and store financial data including the bank or credit card details of donors and financial supporters, staff and suppliers. This data is very valuable and its loss could expose the VO and others to the risk of theft, fraud, identity theft and loss. The administrators should have in place appropriate policies governing access, use and storage of electronic information ensuring compliance with Data Protection legislation. Procedures should also include the use of computers, hard drives, USB and data storage devices and the protection of data.

If it is known or suspected that a VO is a victim of financial crime then this should always be reported to the police and the CVO.

### **Can administrators apply a risk based approach to their duties?**

What a VO and its administrators must or should do in their VO and what is a reasonable and proportionate approach to adopt when taking action to comply with legal duties will depend on a range of factors.

It will, for example, depend on:

- different aspects of a VO's work and the risks which arise;
- how much money is involved;
- whether partners and funds are overseas and what the risk of fraud and corruption is there;
- whether the crime has occurred by someone within or closely connected to the VO;
- how often incidents are taking place

In order to minimise risk, VOs should:

- Have some form of appropriate internal and financial controls in place to ensure that all their funds are fully accounted for and are spent in a manner that is consistent with the purpose of the VO. What those controls and measures are and what is appropriate will depend on the risks and the VO.

- Keep proper and adequate financial records for both the receipt and use of all funds together with audit trails of decisions made. Records of both domestic and international transactions must be sufficiently detailed to verify that funds have been spent properly as intended and in a manner consistent with the purpose and objectives of the organisation.
- Give careful consideration to what other practical measures they may need to consider to ensure they take reasonable steps to protect the VO's funds and the administrators meet their legal duties.
- Deal responsibly with incidents when they occur, including prompt reporting to the relevant authorities and ensuring the VO's funds are secure

In all these cases, the more complex or significant the VO's activities and financial transactions, the more money or the higher the number of transactions involved, the more serious the crime or its circumstances, the more steps that are likely to be required as reasonable to ensure a administrator complies with these duties, even when balancing this with the volume and cost of administration this may involve.

What is appropriate and proportionate therefore depends on the nature of the risk, its potential impact and likelihood of occurring. What is important is for administrators to be able to show that the action they have taken is reasonable in light of those risks and actions.

The existing requirements for independent audit in category 3 VOs may assist administrators, but they should not be relied on as the only way or fail safe way of ensuring no abuse takes place.

Conversely, smaller VOs and those VOs operating where the risk of fraud and abuse is lower, will not have to do as much to protect the VO and ensure the administrators discharge their duties. For example, smaller VOs will not usually be expected to have written fraud policies and specific anti-fraud measures in place.

Whatever a VO's size and circumstances, the administrators need to be able to explain what they did (or did not do) and show that this was reasonable in the particular circumstances.

## What financial crimes do administrators need to be aware of?

The main financial crimes to be aware of are:

- Fraud
- Money Laundering
- Terrorist Financing

### What are 'fraud' and 'theft'?

Fraud is a form of dishonesty, involving either false representation, failing to disclose information or abuse of position, undertaken in order to make a gain or cause loss to another.

Theft is dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it.

Fraud is a criminal offence. In practice there are a wide variety of types of fraud that VOs can experience including fraud connected with VO fundraising, income and expenditure, property and investments, VOs' identities, banking fraud and others. More information on fraud can be found further down. Fraud committed against an organisation has sometimes been portrayed as a 'victimless crime', but it can have a devastating effect upon individuals and communities. For VOs, the impact of fraud can include significant loss of funds, permanent financial or reputational harm and damage to public confidence. Smaller VOs with relatively low incomes may be less capable of coping with the financial and reputational impact of fraud.

There are many different types of fraud and the methods used are constantly evolving. Individuals and organisations may be targeted through emails, phone calls, letters, the internet, or other methods. An operation in which a donor is deceived or tricked into giving money is fraud. VOs themselves can be victims of fraud, but sometimes a VO, or a VO's name, can be used to commit a fraud against individuals – for example, when people are sold items supposedly for VO when the money in fact goes straight to the fraudster.

Fraud can take be committed through:

- false representation
- failing to disclose information
- abuse of position

### **What is 'money laundering'?**

Money laundering is a crime and is usually described as the process of turning the proceeds of crime into property or money that can be accessed legitimately without arousing suspicion. The term 'laundering' is used because criminals turn 'dirty' money into 'clean' funds which can then be integrated into the legitimate economy as though they have been acquired lawfully. VOs, like any other organisation, can be targeted as channels for money laundering, but in practice they may have a greater vulnerability because being associated with a VO tends to give a veneer of public respectability to a non-VO enterprise that is in reality dubious or possibly criminal.

### **What is terrorist financing?**

Terrorist financing is the raising, moving, storing and using of financial resources for the purposes of terrorism. Money underpins all terrorist activity - without it there can be no training, recruitment, facilitation or support for terrorist groups. The disruption of terrorist financing activity is a key element of the Government's overall fight against terrorism.

VOs play an important role in ensuring that the funds they collect are not diverted to terrorist organisations.

### **What other types of financial crime are there?**

There are various other types of crime related to financial abuse. The police are responsible for identifying which crimes apply to a particular set of facts. However, some other crimes which exist include bribery, false accounting, fraudulent trading and intellectual property offences.

### **What are the various types of fraud, and how can administrators prevent them happening?**

There are various frauds to which VOs are potentially vulnerable. Frauds can be identified either as internal (involving only people within the VO) or external (in which at least some element of the fraud is perpetrated outside the VO).

The following sections set out some information about some common types of fraud and provide advice on how administrators might protect their VO from them.

#### **Income-related fraud**

This occurs when people within or connected to a VO attempt to divert funds for personal use or other non-VO purposes.

Examples of income-related fraud include:

- redirected resources from VO shops or trading activities;
- intercepted postal donations and cheques being paid into personal accounts;
- skimming money from fundraising collections;
- impersonating a VO and redirecting the income collected to a fraudulent or bogus body;
- false accounting;
- claiming inappropriate expenses.

### **Prevention:**

A lot of VO work relies upon the goodwill, dedication and hard work of volunteers, staff and supporters, so it is important to maintain a culture of trust and harmony within a VO. However, administrators should not assume that processes and procedures will always be carried out correctly.

Administrators should remember that they are ultimately responsible and they must ensure that their VO's financial control and other systems are adequate and operating correctly so that they can satisfy themselves that funds and resources are properly collected, allocated and spent.

### **Summary of key financial controls:**

**Prevent** – embed good financial controls and sound financial management as a core part of the VO's culture:

- ensure relevant staff and volunteers are trained and understand the VO's financial controls and their responsibilities;
- segregate duties where possible. Don't allow one person to be in charge of all aspects of the VO's financial controls
- rotate staff responsibilities where possible

**Identify and disrupt** – be aware of risks and actively monitor and review:

- regular review of budgeting and cash flows to ascertain expected income levels, review cash received and compare to expectations
- look at comparative figures for previous periods. If there are significant variations, or no variation at all, this should be regarded as grounds for further query
- be open and transparent with donors. Administrators may discover from them that their VO has actually received more than they thought

**Act promptly and properly** to minimise damage and prevent further loss.

### **Expenditure fraud**

Examples:

- claiming non-existent, over-inflated or inappropriate expenses or overtime
- withdrawing cash directly from the VO's bank account for personal use using cheques which have been obtained without authorisation, or by issuing false direct debit/standing order instructions for personal gain
- misusing VO credit and debit cards or internet banking for personal expenditure
- creating false invoices, purchase orders and supplier identities in order to obtain payment from the VO for goods and services that have not been supplied
- submitting, or conspiring to submit, false applications from real or fictional individuals for grants or other benefit - this may involve an employee who knows the system and how to manipulate it. In some cases individual employees may have authority to approve applications themselves
- an administrator or employee awarding a contract, or preferential terms, to a supplier in return for payments, personal discounts, commission or other benefits
- using receipts and records for a completed project to support a further application for funding from another grant-maker
- creating non-existent beneficiaries or employees for directing payments, or use of a beneficiary identity for personal benefit

### **Key financial controls:**

- Segregation of duties where possible.
- Carrying out regular bank reconciliations.
- Requiring multiple signatories for all bank account activity
- Restricting full access to all areas of the accounting system – in particular with regard to the setting up of new payees.
- Regular review of and spot checks on payroll records to ensure that they are consistent with staff movements.
- Reconciliation of supplier statements, invoices and creditor balances.
- Establishment of authority thresholds for the approval of orders and the payment of suppliers.
- Random checks should be carried out to ensure expenditure below key thresholds is legitimate.

- Assess whether there are any employee/administrator connections with suppliers. Any new contracts entered into with suppliers should be thoroughly assessed with regard to value for money, and administrators may wish to consider asking new suppliers to declare whether they have any business, family or other connections with VO personnel.
- Reasonable and necessary expenses may be paid to administrators and employees but there should be proper controls including a full documentary audit trail.

### **Property and investment fraud**

Examples:

- Fraudulent use of VO property - for example personal use of VO vehicles, hiring them out, siphoning off fuel, claiming for overpriced or unnecessary repairs.
- Stealing VO letterheads and personal details of administrators, staff or beneficiaries may be part of an identity theft fraud.
- Using the VO's databases or inventories for personal profit or unauthorised private or commercial use. The theft of donor details or other personal information, for example, might have implications under the Data Protection Act.
- Theft of furniture, computers, plant and other equipment. Administrators may of course allow staff to make moderate and reasonable use of VO equipment such as personal telephone calls and small quantities of stationery.
- Making grant applications on behalf of the VO with the intention to intercept the funds for personal use.
- Transferring VO funds to an organisation with which an administrator or employee is connected – for example, making an 'investment' or interest-free loan of VO funds to a company which is not in the interests of the VO and in which one of the administrators is a director.

### **Key financial controls:**

- A list or register should be maintained of all assets, whether purchased, donated or loaned. It should show the cost (or value) of each asset and provide sufficient detail to enable them to be identified and located. For moveable items such as machinery or equipment serial numbers should be recorded, and it is usually advisable to keep photographs.

- The asset register should be inspected at regular intervals and physically checked against the assets themselves in order to ensure that they are in good repair and being put to appropriate use.
- Bank records should be reconciled with internal accounts at least monthly, and reviewed by a second person. Any discrepancies should be resolved.
- There should be a securely held list of all active bank accounts. The list should be reviewed periodically and dormant accounts should be closed.
- Cheques and other payment instructions should be signed by at least two individuals.
- The opening or closing of accounts should either be authorised by the whole administrative body or, if delegated, the administrators should ensure that they are informed promptly.
- Third party individuals or organisations should not be allowed to open bank accounts in the VO's name, or use the VO's bank account to receive or transfer personal money.
- There should be proper systems to approve and authorise movements between, and payments from, bank accounts.

### **Procurement fraud**

Procurement fraud is a generic term describing fraud relating to the purchase of goods and/or the commissioning of services, as opposed to the simple theft of cash. Procurement fraud usually involves collusion between one or more members of the VO's staff and one or more outside suppliers. Practical advice for dealing with it are covered further down.

### **Fraudulent fundraising in the VO's name**

This usually involves misrepresenting to the public or other donors the destination of funds, or the amount going to a named VO. It can occur through:

- fundraising events and/or competitions which claim to be for charitable purposes but from which no VO in fact receives any proceeds
- cash collections either in public places or from house to house which have not been authorised by the VO and/or the relevant local authority
- collecting tins for a named VO which does not exist
- fundraisers raking off funds and handing over only a proportion of what has been collected
- professional fundraisers not being truthful to donors how much of the funds being donated will be used to pay their charges



- creating spurious email appeals or false websites, claiming that money donated through them will be given to VOs which may or may not be genuine

### **Fraudulent invoicing and grant applications**

This is likely to involve:

- making false or inflated applications to a VO to win service contracts or misapplying grant funding in breach of trust and contract
- making grant applications to a VO in respect of bogus or non-existent applicants
- setting up a false VO to obtain grant funding but with no genuine intention to provide services or register with the Commission

### **Identity fraud/theft**

False identities may be created in order to justify fraudulent payments. Corporate Identity Fraud occurs when a bogus company is set up, or a genuine company's details are used without authorisation, to facilitate unlawful activity.

Examples of identity fraud and theft include:

- falsifying, creating or fraudulently using administrator or employee details
- provision of funds or services to non-existent beneficiaries
- using a genuine VO's name or logo in correspondence or on materials for the purpose of deception and fraudulent gain

Administrators should be vigilant against any unauthorised use of their, or their VO's, identities, for example in carrying out cash collections.

### **Practical advice**

If your VO regularly receives payments from beneficiaries for charitable services, the following suggestions could reduce the threat to your confidential client data from identity fraud:

- restrict access to account information on a 'need to know' basis, such as those responsible for processing payments
- carry out proper vetting checks on new staff, and ensure that any agency staff have been adequately checked by the agency
- ensure that your beneficiaries are clear as to what your normal business procedure is on communicating important messages to them, and that your staff follow this

- ensure that you manage your beneficiaries' personal information in line with current Data Protection guidelines.

## Banking fraud

A major risk under bank fraud is fraudulently setting up direct debits and standing orders to transfer funds to the fraudster's own bank account. The steps that administrators can take to reduce the risk of this type of fraud are:

- Prevention:** make it clear in writing to the bank that no further direct debits should be set up without the express approval of specific named personnel. If bank account details are to be made public (for example, on appeal literature) it should be a stand-alone account from which no payments can be made outside the VO.
- Detection:** ensure that regular checks are carried out on your bank statements and that they reconcile with the VO's records. Any unexplained or unusual transactions must be investigated.
- Redress:** under the direct debit guarantee scheme, wrongly paid direct debits can be reclaimed from the bank. It is then the bank's responsibility to recover this money from the person or organisation which has received it.

## E-Crime

### Using VOs to validate stolen or cloned credit cards

Fraudsters may use stolen or cloned credit cards to make small online donations through VO websites. Their purpose in doing this is to check whether a stolen card has been blocked or cancelled. If the 'test' donation works the card will be used for more widespread fraud.

To help prevent this, VO staff may be able to identify some of the following patterns:

- fraudsters typically donate a small, token amount, eg €1. (Note, however, that there might be a large number of relatively small donations during appeals for humanitarian disaster relief or in the approach to Christmas)
- one card may be used a number of times in succession, to check it is still unblocked
- the name of the donor may not match the cardholder's name. Some fraudsters will put random characters into mandatory name and address fields

On identifying this kind of risk it may be possible to take some preventive measures, such as:

- carrying out address checks for large donations
- checking that the CVC number (last 3 digits on the back of the card) tallies with the individual's details
- checking the internet provider address from where the donation is being attempted. Suspicious or problematic internet provider addresses can be blocked and blacklisted
- using systems which require the donor to manually input details
- reporting suspected fraudulent activity to the police and bank immediately
- having an anti-fraud email address in place so that donors can report direct to the VO any suspicious activity and possible scam emails
- ensuring that all emails sent to donors direct them to the VO's website, without using a link if possible

Fraudsters have been known to set up false VO websites, with the appearance of genuine ones, in order to obtain credit card and personal details of unwitting donors. In doing so they frequently infringe trademark, logos and copyright laws in addition to financial crime. It is advisable for VOs to provide the following advice to donors or customers who are proposing to make donations through websites:

- always update your information online by using the process you have used before, or open a new browser window and type in the website address of the legitimate organisation's account maintenance page
- be wary of unfamiliar website addresses, as they may not be genuine. Only use the address that you have used before, or start at your normal homepage. Avoid unfamiliar links or pop-up screens
- always report fraudulent or suspicious emails to your Internet Service Provider (ISP). This will help to ensure that bogus websites are shut down before they can do further harm
- take note of the header address on the website. Spoof sites are more likely to have an excessively long line of characters in the header, with the business name somewhere in the string. Many secure sites have padlock symbols and other secure technology to look out for
- if you have any doubts about an email or website, make a copy of its address and send it to the legitimate business to check whether it is genuine

- if VOs discover, or suspect, that they are victims of this type of scam, it is recommended that they contact the ISP which is hosting the spoof website and request that the site be taken down as quickly as possible

## **Phishing fraud**

'Phishing' is a type of e-crime which involves fraudsters sending emails to many, sometimes thousands, of recipients asking them to disclose sensitive or confidential information. The fraudsters may be based overseas and may be almost impossible for the authorities to trace. Typically, the phishing email is made to look like a genuine email from a bank, and it may ask the recipient to confirm information such as account usernames or passwords because, it claims, there has been a security problem with the bank's computer system. In many cases the phishing email will contain a link to another website into which the recipient is asked to enter the confidential information.

Phishing scams cost fraudsters very little to set up, and they can make a profit if only a few people in every thousand actually provide information that then results in their bank accounts being emptied.

## **Mass market fraud**

This covers a substantial variety of frauds which rely on letters and emails to reach large numbers of people. In some cases fraudsters pose as legitimate businesses and send what appear to be genuine letters from established companies. These can include customer account details and their current payment information.

The letters instruct, say, tenants to amend existing records and send their normal payment to a different bank account, which is actually controlled by the fraudster. This account may be held with the same bank or a different one.

Any VO which has large numbers of beneficiaries who regularly and routinely make electronic payments for services to the VO may be vulnerable to this type of scam.

## **What are the Warning Signs for Fraud?**

There is no definitive list of what to look out for. However, the following set of questions may help administrators and their VOs to recognise the early signs of fraud. It is important to bear in mind that a 'yes' answer to any question – or even more than one – should **not** be regarded as an indication that fraud is taking place. Rather, it should prompt administrators to consider whether their VO's financial control systems and procedures are adequate, and to revise them where appropriate. A high number of 'yes' answers, or repeated occurrences of a small number, should

be investigated appropriately, in the context of the VO's size, activities and financial structure. Administrators should use their judgement and their knowledge of their VO to determine the appropriate extent and depth of investigation.

### **Accounting and transactions**

- Are there unusual discrepancies in accounting records and unexplained items on reconciliations?
- Are many financial documents - such as invoices, credit notes, delivery notes, orders etc – photocopies rather than originals? This might indicate counterfeit documents created to support bogus account entries.
- Do alterations or deletions frequently appear on documents? Again, this might be evidence that documents have been falsified to support bogus account entries.
- Have any documents or account books gone missing?
- Are there high numbers of cancelled cheques?
- Are common names unexpectedly appearing as payees?
- Are there any duplicated payments or cheques?
- Do transactions take place at unusual times with irregular frequency, unusual or 'round' amounts, or to unknown recipients?
- Are suppliers regularly submitting invoices electronically and are these in non-PDF format that can be altered?
- Are there any unexplained variances from agreed budgets or forecasts? Have audits highlighted any inconsistencies or irregularities?
- Are unrestricted reserves being spent without proper prior authorisation?
- Have restricted funds been used for general purposes?
- Is there an asset register or inventory, and does it match up with equipment physically on hand?
- Are payments made to individuals or companies with family or business connections to an administrator, and perhaps authorised by that administrator? This might indicate collusion.
- Is there any indication that income is being under-reported or expenditure being over-reported?
- Is there any incorrect or false purchase and expense items in the accounting system?
- Can cash withdrawals be supported by documents and a full audit trail from approval to expenditure?
- Have any blank cheques been pre-signed?

### **Changes in behaviour of administrators or staff who handle the accounts**

- Are vague responses being given to reasonable and legitimate queries and/or are those queries being left unexplained, or taking a long time to resolve?
- Is there any reluctance by a volunteer, member of staff or administrator involved in handling finances to accept assistance? Does a single member of staff or administrator have control of a financial process from start to finish with no segregation of duties?
- Is any member of finance staff working unsociable hours or working from home without reason? Are there any noticeable changes in behaviour or work patterns, such as a reluctance to take holidays or over-protectiveness of work?
- Has the format of financial information presented to the board or senior managers suddenly changed or become more complicated or difficult to understand?
- Are there inconsistent, vague or implausible responses to questions about the accounts or accounting records?
- Do administrators and members of finance staff always comply with financial policies and procedures?

None of the above warning signs are necessarily indicative of financial abuse on their own, but if one of them is happening frequently or several in combination, further scrutiny may be warranted.

### **What practical steps can administrators take to deal with fraud?**

All VOs are vulnerable to fraud and financial crime and those that have weak internal financial controls are likely to be at even greater risk. Administrators need to consider applying, depending on the size of their VO and the complexity of its operations and administration, an appropriate set of financial controls and, for many VOs, put in place a suitable range of anti-fraud measures to protect their VO's funds. The larger and more complex a VO's operations and administration, the more likely it is the administrators will need to implement a broad set of anti-fraud measures.

Administrators may find some of the following anti-fraud measures are appropriate to use or adapt for their VOs. Such measures will not be necessary or relevant for all VOs but administrators should use their judgement and their knowledge of their VOs to decide which ones are appropriate and proportionate for the context of their VO. Any anti-fraud measures adopted should be flexible enough to cope with change

and regularly reviewed to ensure that they cover all risk areas and remain generally fit for purpose.

#### Anti-fraud measures:

This list of measures ranges from those (at the top) which all VOs should implement through to those (at the bottom) which are probably necessary and proportionate only for larger VOs. The larger the VO, the more complex its operations and financial transactions or higher the risks of fraud or other financial abuse, the more administrators will be expected to do to ensure they protect the VO and meet their legal duties and responsibilities. Administrators should use their judgement and knowledge to decide how far down the list it is appropriate for their VO to go. Remember to review these measures at regular intervals, and especially when the VO expands or changes its activities.

- implementing robust financial controls and governance measures - relevant staff should be made aware of the controls and measures in place
- ensuring there are clear procedures for reporting fraud to the police and to the CVO
- ensuring basic records of all income and expenditure are kept and receipts, invoices and supporting documents are kept
- increasing awareness amongst administrators, staff and volunteers of the fraud risks within their VO
- checking that financial controls are not being overridden, by-passed or ignored, whether by administrators, staff or volunteers - override arrangements such as pre-signing blank cheques can significantly compromise financial controls
- restricting and closely monitoring access to sensitive information
- using tiered authority and signature levels for payments, where possible
- regularly reconciling bank statements and other accounts, carrying out spot-checks on books and records
- periodically auditing processes and procedures
- setting out clearly defined roles for administrators and staff - these should include segregation of duties and delegation of financial responsibilities with appropriate report-back procedures
- recording all instances of suspected and confirmed instances of fraud, which will help your VO spot emerging patterns, identify areas of risk, measure losses and build an evidence base if fraud is confirmed as having occurred

- clearly communicating fraud policies and procedures to all staff, volunteers and administrators through team meetings and as part of an induction programme for new people - training will be needed to keep up to date with new risks and changes in the law
- appointing or designating staff, at appropriately senior levels, to have special responsibility for fraud prevention policies
- introducing a whistle-blowing policy and including fraud as one of the key threats on the VO's risk register
- controlling access to buildings, assets and systems using secure or unique logins and passwords
- introducing an anti-money laundering policy
- aligning Human Resource policies and procedures with fraud and financial crime issues
- developing a fraud risk assessment process that takes into account the types of fraud to which the VO is most exposed, having regard to its structure and activities
- having a clear response plan in case fraud occurs - it should outline how investigations will be conducted and by whom, the people and organisations that need to be notified, and the process for handling internal and external communications

### **Implementing robust financial controls**

Administrators must ensure that their VO has financial and banking procedures in place which are appropriate to their VO and its activities and are fit for purpose. They must also monitor the application of those procedures so as to ensure they remain fit for purpose, and ensure that they obtain and understand financial reports upon which they base their management decisions. Not doing this may be regarded as failing to exercise the reasonable care expected of administrators.

Internal financial controls are essential checks and procedures that help VO administrators to:

- meet their legal duties to safeguard the VO's assets
- administer the VO's finances and assets in a way that identifies and manages risk
- ensure the quality of financial reporting, by keeping adequate accounting records and preparing timely and relevant financial information.



The operation of a system of effective financial controls should be a priority for VOs at all times, but it becomes even more important during periods of financial difficulty for the VO, or for the economy in general. An effective framework provides administrators, VO employees and volunteers with the boundaries within which they should operate and also gives beneficiaries and the public confidence that their VO is operating effectively.

Administrators should ensure that any staff and volunteers working for the VO understand how its financial controls are to be properly implemented. For larger VOs subject to an external audit, the correct operation of internal controls is something about which the auditor will need to gain assurance in order to produce an opinion on the accounts. Some audits simply acknowledge paper trails rather than verifying actual transactions. In these cases, the risk of financial crime or fraudulent activity being missed is greater.

Administrators are individually accountable for the performance of their duties and must collectively make decisions about internal financial controls. In some VOs, administrators may be able to delegate some aspects of financial management to one or more administrators or employees, but they remain collectively responsible and should ensure that the delegated tasks are properly carried out. This will involve setting out a clear description of the work to be done and arrangements for regular and adequate report-back. Administrators should ensure that the decisions they make about financial controls and delegation are fully recorded.

All VO administrators should keep accounting records sufficient to show and explain all of its transactions. Smaller VOs, as a minimum, should maintain simple income and expenditure records supported by invoices, receipts and bank statements. Larger VOs with more complex activities and structures will need to have accounting systems that are appropriate for their purpose.

Every VO needs to operate a bank account of a kind that best meets its individual needs. For some VOs this will mean having more than one account, and possibly accounts in more than one country. As a matter of general principle cash transactions should be kept to the absolute minimum, but all transactions, whether through the bank or in cash, must be properly authorised and authenticated with appropriate supporting documentation.

By defining, implementing, and reviewing a VO's controls, the risk of fraud and financial crime is reduced. However, administrators and managers should be alert to new risks and ensure that their VO's financial controls remain fit for purpose.

## Human resources and recruitment

For those VOs that have staff or volunteers, effective fraud prevention starts with robust HR policies and procedures. For smaller VOs this might mean nothing more than checking references for new staff and ensuring that they are aware of the financial controls in place. For larger VOs with more staff and greater levels of income and expenditure, a more comprehensive recruitment and selection process will be appropriate. Introducing measures to inform decisions made on recruitment and staffing issues will help to limit exposure to fraud and financial crime. The following measures may be helpful when reinforcing HR procedures:

- a self-declaration form for staff to confirm that they do not have an unspent conviction for fraud, theft or other relevant offence (as a minimum for smaller VOs, or a police conduct certificate)
- performing a credit check or screening on employees and volunteers who are handling finances or dealing with cash - prospective and existing employees or volunteers must be informed they will be subject to screening and have signed a consent form and data protection statement
- checking the references of previous employers when recruiting
- setting out the VO's policies and procedures covering anti-money laundering, fraud and reporting requirements (including whistleblowing) as part of a staff and administrator handbook
- assessing staff and administrator awareness of VO policies and procedures as part of the performance appraisal and review process

## Financial control policies and their implementation:

It is crucial that financial control procedures are understood and used by administrators, staff and volunteers, and that they reflect what happens in practice in the VO. Developing a culture in which respect for internal controls as an integral part of the VO's operation is important. Regular communication with staff on financial control policy and procedures will help to embed an organisational culture that focuses on effectively addressing risk and safeguarding the VO. Staff, volunteers and operational partners should be made aware of VO policies and procedures as part of their induction and training processes.

The larger and more complex the VO the more likely it is that it will need to have a documented financial control policy, whereas smaller VOs may rely on their practice and procedure being generally known. Either way, it is important that a VO's policies and procedures are understood and applied.

Amongst the key points to be covered by policies are: who has authority to commit expenditure, and how much; how cash is handled and accounted for; and who is responsible for maintaining the day to day records and producing periodic financial reports.

Policies and procedures introduced to safeguard against fraud and financial crime should be subject to regular reviews, as they can only continue to be effective if they take into account changing internal and external factors which may impact upon the VO. Where appropriate, administrators should ensure that staff receive adequate refresher training when systems are changed or updated.

### **Fraud policy**

Not every VO will need to have a fraud policy. However, the larger the VO or complex its operations the more likely that this will be sensible and/or necessary. If administrators decide it is appropriate to develop and implement a fraud policy for their VO, this can usefully outline the VO's attitude to fraud and set out responsibilities for its prevention and detection. These may include:

- setting out what fraud and theft means within the context of the VO
- how the VO expects to deter fraud and how it will react to different types of potential fraud
- key responsibilities of senior staff and administrators in preventing and detecting fraud and in co-operating with any investigations
- details of any whistleblowing plan, including those to whom VO representatives can report concerns and suspicions confidentially
- the procedures for reporting to the police and CVO suspected incidents of fraud and theft
- how to respond to allegations of fraud
- how the VO assesses its exposure to fraud risk, including details of its fraud recording system, an estimate of how much has been lost as result of fraud in the past, and an opinion of how much could be at risk

### **Developing anti-fraud measures**

Management meetings, at which administrators and staff can share experiences and ideas, are a useful way to encourage the development of good anti-fraud procedures and decision-making. Preparation for and conduct of meetings might include:

- circulating financial reports and related papers in advance to administrators and managers so they have time to consider and, if necessary, check the financial information

- ensuring that all decisions on financial controls and policies are accurately minuted
- allowing sufficient time to discuss finance reports and related decisions on financial controls
- providing training for new and existing administrators on how to understand the VO's accounts and financial reports
- carrying out regular budget comparisons with previous years for benchmarking purposes
- producing statutory accounts as soon as possible after the financial year-end, as this could highlight any deviations in income and expenditure - an early analysis may highlight any unusual and potentially fraudulent activity
- encouraging open discussion and questioning - if something doesn't look or seem right to the administrators then it should be properly investigated

### **Whistle-blowing policy**

A whistle-blowing policy should set out the procedures to be followed where there are concerns about fraud or financial crime. These policies are often wider than just about fraud or financial crime. The policy would normally include:

- confirmation that the VO actively encourages its staff and volunteers to report concerns and suspicions about fraud or financial crime in the VO, and it will take them seriously
- a statement on confidentiality/ anonymity and support
- advice for staff and volunteers on when to speak to a line manager or other senior staff
- details of how to report concerns (eg about an administrator) to the VO's senior staff or board.

### **Practical advice on dealing with money laundering**

#### **How can VOs reduce the risk of money laundering?**

Internal financial controls are essential checks and procedures that help to safeguard against money laundering. It can be hard for a VO to detect that it is the innocent victim of money laundering, so an initial assessment of the type of money laundering risks that might affect the VO's activities, and what this would mean to the VO's finances and reputation, should help to determine the level of anti-money laundering procedures that is appropriate.

There have not been any proven instances of money laundering involving a VO. However, it could happen and it is therefore important that administrators take

reasonable steps to prevent the VO being used for money laundering purposes and know what to do if they have any suspicions. This kind of abuse usually involves the receipt of funds which are then paid out, perhaps in different amounts, to different people and in different forms and currencies. To help prevent money laundering, VOs should assess the levels of risk to which they are exposed and adopt appropriate anti-money laundering procedures. These might include:

- due diligence checks on the donor, in accordance with the 'know your' principles in Chapter 2 of the toolkit, taking into account factors such as size of donation, source of funds and donor's location
- further verification checks when the donor is considered higher risk
- ensuring that staff know how to recognise the warning signs of possible money laundering
- robust methods for recording and documenting donations and grants
- protocols for monitoring the effectiveness of the money laundering procedures

In order for the controls to be effective, all relevant staff will need to be adequately trained on the VO's policy on accepting donations and loans. Administrators must ensure that robust methods for recording and documenting donations and grants are in place, and that there are procedures for monitoring the effectiveness of the money laundering controls. Decisions to refuse or accept donations should be recorded in writing. This will be important to show that administrators have acted responsibly, have given due consideration to any risks and can demonstrate the integrity of the decision-making process. If there is any reasonable doubt or suspicion about the source of funds coming into the VO administrators should consider whether to refuse it and inform the relevant authority.

Some donors may seek to attach conditions to their donations. Whilst VOs are free to accept gifts in these circumstances, they should consider whether the condition is compatible with the purposes of the VO as well as their current priorities and planned activities. Donations subject to unusual conditions or unsolicited offers of loans to VOs may be intended to facilitate money laundering or financial crime.

These risk-based measures should be documented and can form part of the VO's general policy on accepting and refusing donations.

### **What are the warning signs for money laundering?**

There is no definite list of common signs. However, the following situations should be considered critically as possible indications of money laundering, especially if more than one of them occurs or they occur regularly.

- large unexpected donations from unknown individuals, organisations or other sources new to the administrators
- donations on condition that particular individuals or organisations, who are unfamiliar to the VO, being engaged to carry out the work
- money being offered as a loan to the VO for a period of time after which it is to be returned or sent elsewhere. Typically, the VO is allowed to retain the interest earned or some other small sum in return for agreeing to take part in the arrangement
- similar 'loan' arrangements in which money is received by the VO in a foreign currency but is to be returned to the donor in Euro
- unexpected or unexplained requests for the repayment of all or part of a donation
- requests for assistance in recovering large sums of money where the VO is offered a percentage of the amount recovered. The VO might be asked to provide its bank account details or allow the donor to use its name or letterheads on the pretext that it is a necessary part of the recovery process
- unsolicited offers of short term loans of large cash amounts, repayable by cheque or bank transfer, perhaps in a different currency
- being asked to allow transactions to pass through the VO's bank account
- offers of goods or services which seem very expensive, unusual or carry high administration and other charges

### **What is a Risk-based approach?**

Adopt a risk-based approach to limit potential for money laundering:

- Identify risks – weigh up money laundering risks; their scale and possible impact on your VO
- Reduce risks – apply the preventive measures set out above
- Monitor risks – collect data, re-assess risks, modify and introduce new systems, criteria and procedures to meet increased or different risks
- Keep records – write down your VO's policies and procedures, and regularly review and update them

## **Fraud action and response plan**

### **Why should a VO have a fraud action and response plan?**

If administrators and staff are aware of what to do if a fraud occurs or is suspected, they have a much better chance of reducing any potential negative impact. A fraud action and response plan can help with this and can also act as a deterrent to fraud in the first place. For very small VOs, such a plan may not be necessary. For others, a fraud action and response plan can be a relatively simple set of procedures; administrators of larger VOs with a wider range of activities or more complex operations are likely to need a plan and for it to be more comprehensive.

As well as the obvious financial impact of fraud it is important not to underestimate the emotional impact of being a victim. If a VO has an action plan in place, which addresses both aspects, administrators and staff will be in a much better position to deal with the full impact and consequences of fraud.

## **Reporting fraud and money laundering**

### **When should a report be made to the police?**

If administrators suspect a crime has been committed or the VO's money or help is being used for illegal purposes, they must report their concerns and the suspicious activities to the police and appropriate authorities as soon as possible.

## Chapter 4: Holding, moving and receiving funds safely

All VOs need money or financial assistance of some kind to carry out their work. They may receive money from donors and sponsors, from fundraising activities, from membership subscriptions or from charging for their services. They spend money in a variety of ways, for example on running the organisation, on projects to help beneficiaries and by giving grants to other VOs and organisations. VOs which work internationally often move money across international borders and spend it in other countries, encountering different financial systems and needing to use different currencies.

Most countries in the world have formal banking systems in place. Using such systems is a prudent and responsible way to ensure that VO funds are safeguarded, and that there are appropriate audit trails of the sort which administrators must keep for the receipt and use of money. This chapter explains the need for VOs to have and use bank accounts; what administrators' duties are when using the banking system; and the particular issues which may arise in connection with exchanging currencies.

This chapter provides a number of practical Tools that administrators can use to help manage the risks and protect their VO's funds from harm.

### Practical advice on operating bank accounts

Administrators should exercise effective general control over their VO's bank accounts and make regular checks to ensure that their VO's bank accounts are operating as intended, and are consistent with the internal financial records.

Administrators should ensure that:

- the opening or closing of accounts should either be authorised by the whole trustee body, or if delegated, the administrators should be informed of changes
- a list of all its bank accounts should be kept and reviewed for dormant accounts which should be closed
- the costs and benefits of the current and deposit accounts held should be regularly reviewed to ensure bank charges and/or rate of interest are competitive, and that the credit rating of the institution is acceptable
- for internet banking, a dual authorisation system should be used
- third parties should not be allowed to open bank accounts in the VO's name, or use the VO's bank account to receive or transfer money



Administrators should make regular checks to ensure that their VO's bank accounts are operating as intended, and are consistent with the internal financial records. The frequency and extent of the checks will vary according to each VO's financial size and complexity and nature of its transactions; some basic checks will work effectively irrespective of the VO's size. These checks may be delegated by administrators to appropriate members of staff acting under the directions of administrators. Examples of basic checks on bank transactions include:

- making regular spot checks, and checks of all transactions above a certain value
- checking that individual daily receipts from the cash book agree with bank paying-in slips and statement credits for that day
- making sure that standing orders and/or direct debit mandates have been stopped for organisations which no longer supply services or goods to the VO
- for a sample of larger transactions, checking that they reconcile with purchase orders, delivery notes and invoices, and that all documents have been authorised at the appropriate level
- checking a sample of smaller transactions, to mitigate the risk of there being a series of low level errors/fraud which can still add up to significant amount
- the preparation of bank reconciliations at least monthly for all accounts, reviewed by a second person, and the resolution of any discrepancies

Remember:

- checks should ideally be made by somebody other than the person who originally authorised or posted the transactions.
- administrators should periodically review the authorised signatory and other bank mandate instructions so that they remain appropriate and proportionate to the level of financial activity and risk.

#### **Checklist of issues to consider when the VO receives donations from abroad**

- Has there been sufficient prudence and care in verifying and recording the source and origin of the donations?
- What donations and payments were expected?
- Do they match against payments received?
- Do administrators need to take additional steps to verify sums received from particular sources or for sums above a certain amount?

- Are particular financial controls needed to receive certain funds, eg do administrators need to open new accounts in particular currencies?
- Is there any suggestion of pressure being put on the administrators to receive or apply the funds in a particular way?
- Are the administrators satisfied that they have full discretion and proper control of the application of the funds for the appropriate purposes?
- Wherever donations are from, the administrators should be satisfied that there are no express or implied conditions attached which are not in the VO's interests.
- If the funds have been received through intermediaries are the administrators satisfied that these transactions have been through properly regulated and registered agents?
- If the funds have been received in cash are the administrators satisfied that the transfer has been done legally?
- Are there any issues in respect of financial sanctions or anti-money laundering regulations that the administrators have not taken into account?
- Are the administrators clear that this is a donation and the VO will not be expected to repay some or all of the payment at a later date?
- Broadly, are the administrators content that there are no concerns regarding the source of the money?

#### **The use of intermediaries - checklist of some key risk management questions -**

- Speed:
  - how urgent is the proposed transaction?
  - would it be acceptable to allow the transaction to go through the formal banking system, possibly taking a little more time, or is there a pressing need to transfer funds through intermediaries?
- Cost:
  - how much are the charges and what are they for?
  - are the costs reasonable?
  - is it possible to negotiate a better rate?
  - is it a one off or a percentage or commission basis?
  - have the costs of other providers or options been considered and a record made to evidence the decision making process?
- Security:
  - are the administrators satisfied with the overall safety and security of the proposed arrangements, and that there have been appropriate due diligence checks on the intermediary?

- is the proposed transaction putting funds or VO employees or volunteers at any undue risk?

### **Checklist of some key financial controls when using intermediaries**

Administrators should consider appropriate financial controls, risk management and assurance procedures, for instance:

- the administrators should be able to demonstrate why using these methods is in the best interests of the VO
- the administrators should be able to demonstrate effective management and conduct when using intermediaries, including proper decision making and the identification and management of any problems
- administrators should document and agree the policy and the circumstances when such methods may be used
- expenditure should be subject to the same authorisation procedures as for bank payments using formal banking
- there is an obligation for VOs to keep proper records, so an audit trail must be kept for each transaction in the chain of transactions
- receipts should be sought from those that business is conducted with and clear accounting records kept of these
- checks should be carried out to confirm that the funds have been received by ultimate recipient and an accounting record kept, such as an email or other notification
- subsequent transfers should, where practical, be avoided until receipt of a previous transfer can be confirmed

### **Checklists of some key controls when making physical cash transfers**

General issues

- Are the administrators able to demonstrate that there are sound reasons for any decisions to make cash transfers or payments?
- Have the administrators formally authorised its staff or agents to carry cash?
- Has there been a proper assessment of risks to personal safety?
- Have the administrators established adequate levels of financial controls?
- Have the administrators considered the risks in using cash couriers for moving funds?

Financial controls

Financial controls in respect of physical cash transfers could include:

- where significant amounts of cash are being transferred, administrators need to ensure that full records are kept of their decision to allow this, making clear why it is in the interest of the VO to do so and what steps will be taken to ensure the money is safely transferred and reaches its destination
- records must be kept of how much cash is being taken - and in which currency - and a detailed breakdown of what it is intended to be used for
- the breakdown should be prepared by someone independent ie not the person or persons actually carrying the cash
- any currency and commission charges should be fully documented
- the cash should be signed for by the person or persons actually carrying the cash
- on arrival the cash should be stored in a safe if possible
- there should be a proportionate policy on what should be done with any spare (unused) cash, to include circumstances where particular currencies cannot be taken out of the country
- on return a detailed breakdown of expenditure should be provided with receipts as far as possible, accompanied by a self-declaration of how funds were expended by the person responsible for taking the cash, or more than one such declaration if more than one person is travelling
- consideration should be given to the provision of emergency funds for the travellers
- where cash couriers are used, as opposed to VO volunteers or staff, the above controls should be used where relevant, although administrators need to consider whether additional controls and precautions should be introduced

### Cash Courier agreement form

This form can be used or adapted for circumstances where VOs need to use Cash Couriers to make transfers of cash, in furtherance of the VO's aims, where it is not practical to remit funds through formal banking. This form should be retained in the VO's accounting records.

Name of VO			
Name of person acting on behalf of VO			
Name of courier agency			
Name of courier			
Tracking reference number			
Date funds passed to courier (dd/mm/yy)		Date funds due with recipient	
Amount of payment		Currency	
Equivalent in Euro (if applicable)			
Purpose of payment			
Recipient organisation (if applicable)			
Recipient			
Specific details as to how funds are to be delivered			
Signed by VO			
Signed by courier			
Confirmation of receipt of funds (record attached)			
Date confirmation received			

### Cash payments record form

This form can be used or adapted for circumstances where VOs need to make cash payments, in furtherance of the VO's aims, to persons or organisations where it is not practical to remit funds through formal banking. The form should be retained in the VO's accounting records.

Name of VO	
Name of person acting on behalf of VO	
Name of Recipient organisation	
Name of person acting on behalf of VO	
Tracking reference number (if applicable)	
Amount of payment	
Equivalent in Euro (if applicable)	
Purpose of payment	
Date of transaction (dd/mm/yy)	
Any other comments	
Signed by VO	
Signed by recipient	

## Checklist of issues for administrators to consider when using other VOs or NGOs to transfer funds abroad

### Basic information:

- name and address of the other VO or NGO ('partner')
- website
- main contact details
- legal status of organisation/registration number as applicable
- governing document
- partner's objectives and activities
- bank details/sort code/account name and number of partner

### Assurance issues to be considered by VO:

- why is such a transfer through a partner necessary: what other means have been considered and is this the most effective way of moving funds?
- have relevant due diligence checks been done?
- is the partner complying with other legal requirements?
- does the partner have the legal power to hold and transfer funds in this way?
- are there any other risk management issues to be considered by the administrators?

### Key elements of any agreement between the VO and the partner:

- key details of the VO and its partner (as above)
- details of proposed holding and transfer of funds by partner
- agreement on when and how funds are to be released to final destination for the project objectives to be met
- evidence of receipt of funds by partner - copy documentation
- evidence of transfer to intended destination once it happens - copy documentation
- declaration by the partner that the funds have been held and transferred in accordance with the agreement

## Chapter 5: Protecting VOs from abuse for extremist purposes

VOs, by the nature of their work and the issues they deal with, will raise issues which some people find emotive or which may be controversial. They are often innovative and can challenge traditional boundaries. Many VOs further their purposes by arranging events and meetings involving speakers, and by distributing literature and other educational materials. In most cases, this causes no problems.

However, there might be occasions when terrorists, and those with extremist views who encourage and support terrorism and terrorist ideology, use VO events to make those views known or use VOs to promote or distribute their literature.

VO administrators and managers need to be aware of, and actively manage, activities which give rise to the risks that speakers or literature may:

- break the law, by, for example, inciting hate speech;
- encourage or glorify terrorism
- incite racial or religious hatred
- incite criminal acts or public order offences
- be outside of the VO's objects
- put the VO's reputation or other assets at risk
- be otherwise inappropriate under VO law,

### What are administrators' duties and responsibilities?

VOs and their administrators must comply with the general law. This means they must not promote or support extremist views or activity that promotes terrorism or terrorist ideology through the VOs' work.

As part of their VO law duties, administrators must always act in the best interests of their VO. They must act reasonably and prudently and they must ensure that the VO's funds, assets and reputation are not placed at undue risk, and that it is complying with the wider legal framework. They must not engage in activities which would lead a reasonable member of the public to conclude the VO supports terrorism.

A VO's activities can only be in pursuit of lawful purposes. Concerns about a VO involved in promoting, supporting or giving a platform to inappropriate radical and extremist views, would call into question whether what it was doing was lawful under both the criminal law and VO law. Those views might include encouraging violence,



encouraging people to adopt a violent ideology or making claims to which violence is subsequently presented as the only solution.

It can also raise the question as to whether the VO is operating in furtherance of its benevolent purposes and in a way which is for the public benefit. Administrators must also ensure they comply with the VO law.

### **What do administrators need to do?**

The risks vary from one organisation to another. The higher the risks the more needs to be done. Administrators need to be vigilant and should put in appropriate measures in place, such as to:

- assess the risks in connection with the proposed event, meeting or publication, including those undertaken by partner organisations
- ensure they know enough about proposed speakers and close partners
- be clear about how speakers, partners, sponsors and publications are selected and approved
- provide clear guidelines for speakers, authors, translators and editors
- take steps to ensure proposed partner organisations and speakers are suitable
- properly manage VO events to prevent inappropriate activities taking place and, if those steps do not work, to deal with them promptly
- satisfy themselves that literature distributed by or made available by the VO does not break the law, is consistent with its purposes and does not place the VO or its assets at undue risk of harm
- take steps to prevent the VO's activities and views from being misinterpreted
- set procedures for responding to complaints and concerns

Where a VO carries out events or provides or promotes literature on a regular basis, administrators should have written policies and clear procedures in place covering these issues.

Where a VO's activities may, or appear to support, condone or encourage terrorist activity and terrorist ideology, the VO's administrators are expected to take immediate steps to deal with this.

What steps will be required will depend on the circumstances, but may include some of the following:

- ceasing the activities immediately; for example, withdrawing further copies of literature
- if a speaker or literature content gives the impression that the VO supports or condones terrorist activity or violence, making clear these are not the VO's views and that it does not condone or support these views
- not using the speaker again
- not promoting literature by that author again
- if the individual speaker or author is an administrator, member of the VO's staff or agent, considering whether further internal action is required or may be appropriate.

It is expected that any person connected with a VO, whether an administrator, employee, volunteer, or beneficiary, to deal responsibly with concerns of the VO's possible links with extremist activity.

## Conclusion

It is up to the each Voluntary Organisation to choose whether to use this toolkit. Money laundering and financing for terrorism might sound as situations farfetched, but, you, administrators, staff and volunteers, must be aware that you may be surrounded by people whose interests and aims are not as noble as they seem.

It is up to you!