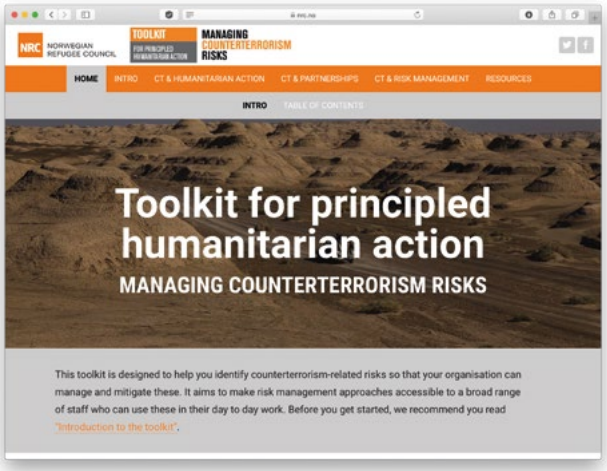
TOOLKIT FOR PRINCIPLED HUMANITARIAN ACTION

MANAGING COUNTERTERRORISM RISKS

NRC NORWEGIAN REFUGEE COUNCIL

TOOLKIT FOR PRINCIPLED HUMANITARIAN ACTION

MANAGING COUNTERTERRORISM RISKS



This material is taken from NRC's online toolkit for principled humanitarian action: managing counterterrorism risks, which you can access at:

https://www.nrc.no/toolkit/principled-humanitarian-action-managing-counterterrorism-risks

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

NRC NORWEGIAN REFUGEE COUNCIL

ACKNOWLEDGEMENTS

This toolkit was produced with the financial assistance of the Swiss Federal Department of Foreign Affairs (FDFA). The toolkit benefits from the contributions of staff from various international non-governmental organisations (INGOs) and other international organisations, UN agencies, and donor governments. NRC would like to thank those who contributed their time and expertise to this work.

The Norwegian Refugee Council is an independent humanitarian organisation helping people forced to flee. For further information, please contact nrcgeneva.policy@nrc.no

Cover photo: © NRC/Jim Huylebroek

Layout & design: BakOS DESIGN

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AML Anti-Money Laundering

CaLP The Cash Learning Partnership

CHS Core Humanitarian Standard on Quality and Accountability

CTF Counter Terrorism Financing

CVA Cash Voucher Assistance

DFID Department for International Development

DTG Designated Terrorist Group

EU European Union

FATF Financial Action Task Force

FSP Financial Service Providers

IHL International Humanitarian Law

INGO International Non-Governmental Organisation

M&E Monitoring and Evaluation

NGO Non-Governmental Organisation

NPA Norwegian People's Aid

NPO Non-profit Organisation

NRC Norwegian Refugee Council

NSAG Non-state Armed group

OCHA Office for the Coordination of Humanitarian Affairs

OFAC Office of Foreign Assets Control

OFSI Office of Financial Sanctions Implementation

PCM Project Cycle Management

PSEA Preventing Sexual Exploitation and Abuse

PVS Partner Vetting System

SOP Standard Operating Procedures

SCP Sanctions Compliance Program

UK United Kingdom

UN United Nations

UNSC United Nations Security Council

US United States

USAID United States Agency for International Development

KEY TERMS AND DEFINITIONS

A single globally accepted definition does not necessarily exist for each of the terms below, and organisations use some of them differently. The definitions given here are for the purpose of this toolkit only.

Access
Humanitarian organisations' ability to reach affected populations, provide humanitarian assistance and the ability of affected populations to access assistance.

Anti-diversion policies and practices
Measures to ensure that humanitarian assistance reaches the intended beneficiaries.

Code of conduct
A set of principles adopted by an organisation designed to maintain standards of behaviour.

Counterterrorism measures
International, regional, national and donor instruments and policies related to counterterrorism

DTG
A group or organisation that has been listed as terrorist by a government pursuant to its national law or by an international body pursuant to international law.

Due diligence
The implementation of an organisational policy and controls designed to assess and track how an organisation's activities and relationships affect its humanitarian work throughout the project cycle.

Evaluation
A learning process intended to systematically assess the efficiency, effectiveness, relevance, sustainability and impact of an activity, project or programme. Evaluations focus on assessing outcomes rather than outputs.

Fraud
A deception practised to secure unfair or unlawful gain.

Monitoring
The continuous and systematic oversight of the implementation of an activity, which is used to measure the achievement of objectives using allocated funds.

Residual risk
The risk that remains after efforts to manage or mitigate risks.

Risk
The effect of uncertainty on an organisation's objectives.

Risk management
The coordinated activities to direct and control an organisation with regard to risk.

Risk transfer
The shifting of risk from one organisation or group onto another. Risk transfer can occur between donors and humanitarian organisations, between international organisations and local implementing partners, and between headquarters and field-based staff.

Sanctions
Restrictions imposed by one or more countries upon another country for political reasons. They may take many forms, including economic and targeted sanctions.

Vetting
The action conducted by an organisation to check whether prospective partners, contractors or staff members appear on designated terrorist lists such as those maintained by donor governments, host governments or bodies such as the UN or EU.

1 INTRODUCTION TO THE TOOLKIT AND RISK MANAGEMENT

The four principles of humanity, impartiality, neutrality, and independence are the foundations of humanitarian action. Guided by these principles,[1] humanitarian organisations work to ensure that assistance and protection go to those most in need. As well as forming the basis of their work, the principles enable humanitarian organisations to gain and maintain acceptance from communities and parties to conflicts, helping ensure the safety of staff.

However, as broad counterterrorism measures become increasingly common at international and national levels, humanitarian organisations are concerned about the impact of these measures on their ability to maintain a principled approach. While humanitarian organisations are, usually, not the target of these measures, they nevertheless pose real risks to operations, staff and beneficiaries. Compounding these risks is the prevalence of "zero tolerance"[2] approaches to risk from some donor governments.

The Toolkit for Principled Humanitarian Action: Managing Counterterrorism Risks updates the information contained in the 2015 Risk Management Toolkit in Relation to Counterterrorism Measures[3] to reflect recent developments. It aims to raise awareness of counterterrorism-related risks so that organisations can identify and mitigate these, and to make risk management approaches accessible to a broad range of staff who can use these in their day to day work.

1.1 WHO IS THE TOOLKIT FOR?

This toolkit is designed for use by a wide variety of staff in headquarters and field locations, ranging from those responsible for programme implementation or partnerships with donors, to those with operational, risk management or policy responsibilities. The toolkit has three objectives:

- To provide an overview of current counterterrorism measures and their potential impact on principled humanitarian action.
- To highlight counterterrorism-related risks that humanitarian organisations may need to manage and mitigate, and to provide a collation of some risk management practices employed in the sector.
- To encourage organisations to mainstream consideration of counterterrorism-related risks throughout the project management cycle.

This toolkit is not exhaustive or prescriptive, nor is it intended to serve as legal or professional guidance.

---

1 International Committee of the Red Cross, Code of conduct for IRC&RCM and NGOs in disaster relief, https://www.icrc.org/en/doc/assets/files/publications/icrc-002-1067.pdf

2 International Council of Voluntary Agencies, Risk and humanitarian culture: An ICVA briefing paper, https://www.icvanetwork.org/system/files/versions/Risk%20and%20Humanitarian%20Culture_briefing%20paper.pdf

3 Norwegian Refugee Council, Risk management toolkit in relation to counterterrorism measures, https://www.nrc.no/globalassets/pdf/reports/nrc-risk-management-tooolkit-2015.pdf

1.2 METHODOLOGY

The development of this toolkit was informed by extensive engagement with donors and staff of non-governmental organisations (NGOs) , international non-governmental oganisations (INGOs) and United Nations (UN) agencies, including during the course of workshops and roundtables in Afghanistan, Kenya, Nigeria, Palestine, Senegal, and Somalia in 2019, as well as desk research and feedback from a steering committee made up of relevant Norwegian Refugee Council (NRC) staff.

Information contained in the toolkit is anonymised except where the information is readily publicly available.

1.3 COUNTERTERRORISM MEASURES AND PRINCIPLED HUMANITARIAN ACTION: WHAT ARE THE RISKS?

Humanitarian organisations are committed to ensuring that assistance reaches its intended beneficiaries. To support or endorse any armed group's political or security aims, including through the provision of aid, contravenes the humanitarian principles of impartiality, neutrality and independence. Humanitarian actors have well developed policies and procedures covering security, human resources, finance and administration to prevent this from happening. Sector wide standards to help humanitarian actors to strengthen adherence to the humanitarian principles and enhance risk management include the Sphere Humanitarian Charter and Minimum Standards[4] in Humanitarian Response and the Core Humanitarian Standard on Quality and Accountability (CHS).[5]

Despite these efforts, it is impossible to entirely eliminate risks in the complex environments in which humanitarians work. This toolkit focuses on helping organisations identify, manage and mitigate counterterrorism-related risks while recognising that residual risks will remain. Once mitigation measures are in place, organisations can use programme criticality considerations to assess whether the residual risks are outweighed by the expected humanitarian outcomes of the proposed activity. See Tool 1: Risk categories and operational impacts

1.4 RISK CATEGORIES AND OPERATIONAL IMPACTS

Risk category	Operational impact
Criminal	**Prosecution over the provision of support to designated terrorist groups (DTGs):** The broad definition of support for terrorism that some states have adopted makes this a risk for humanitarian organisations and their staff if they are deemed to have provided support for DTGs by carrying out certain activities. For example, the US Supreme Court ruled in 2010 that training DTG members in international humanitarian law (IHL) was classed as material support and so prohibited. **Criminalisation of staff:** Criminal laws designed to counter terrorism have the potential to criminalise humanitarian workers. Local staff members may be particularly exposed to risks under the host country's counterterrorism legislation. Potential offences that could involve criminal responsibility include presence in an area of designated terrorist activity, the indirect financing of terrorism and broad forms of association with proscribed groups.

[4] Sphere, Humanitarian charter and minimum standards in humanitarian response, https://spherestandards.org/wp-content/uploads/Sphere-Handbook-2018-EN.pdf

[5] Core Humanitarian Standard, The Standard, https://corehumanitarianstandard.org/the-standard

Security	**Insecurity:** Engaging with non-state armed groups (NSAGs), regardless of whether they are DTGs, is a key element of gaining and maintaining secure access to people in need. Engagement also helps to establish consent and acceptance for humanitarian organisations' activities, which is vital to ensure staff safety. Counterterrorism measures can create uncertainty for organisations about whether contact with NSAGs that are also DTGs is permissible. Some organisations refrain from engaging with these groups as a result. Organisations that fail to engage with NSAGs because of counterterrorism concerns risk negative perceptions of partiality and non-neutrality, which in turn puts staff at risk. Other organisations do engage with these groups, but do not provide staff with support and guidance about how to do this. This can create a "don't ask, don't tell" approach whereby field-based staff engage without the knowledge of senior management, and feel unable to openly discuss dilemmas and risks.
Contractual	**Delay:** The inclusion of counterterrorism clauses in grant agreements can delay the implementation of humanitarian initiatives while organisations work with donors to try to negotiate changes or seek clarity about vague wording. The fact that donors do not always inform organisations when they introduce a new counterterrorism clause or change the wording of existing clauses only increases the likelihood of delays. Some requirements, including screening and/or vetting procedures, may also delay the provision of assistance. Delays can also occur as a result of bank derisking, which happens when banks refuse, or take longer than expected to provide transfers to locations perceived as high risk in order to minimise their own exposure to accusations of facilitating terrorist financing.
	Lower quality of response: Compliance with donor counterterrorism requirements may reduce the quality of an organisation's response by causing it to choose modalities perceived as lower risk even if they are less appropriate and effective for a particular context.
	Risk transfer to staff: Counterterrorism-related wording in grant agreements can be vague and difficult to interpret. It is not uncommon for humanitarian organisations to accept these clauses without fully understanding the requirements involved. Staff tasked with implementing a project under a grant agreement may not have been involved in negotiating it, but they shoulder the burden of complying with the requirements, and organisations often do not provide the necessary guidance or support on how to do so.
	Risk transfer to local partners: International NGOs often pass on donor counterterrorism requirements to local partners in the form of "flow-down clauses" without ensuring they understand what signing the clause entails, or that they have the resources and capacity to comply. Local partners may accept requirements that are impossible for them to adhere to or that endanger their staff as a result.
	Establishing a precedent: This can occur when one organisation accepts a counterterrorism clause that others deem unacceptable. Some organisations may choose to negotiate more favourable terms, but their leverage and ability to do so is weakened if others have already accepted the requirements.
	Loss of funding: Some organisations have refused donor funding as a result of uncertainty about, or unwillingness to accept the terms of counterterrorism clause required of them. Expenditure may also be disallowed under a contract if an organisation does not comply with all donor regulations
Humanitarian principles	**Compromised impartiality:** In order to minimise exposure to counterterrorism risks, organisations may choose not to provide assistance in areas controlled by NSAGs that are also DTGs, regardless of the humanitarian needs there. This compromises the impartiality of their response and leaves affected populations without the assistance they need simply because of their location. If an organisation is not perceived as impartial, it can also put staff safety at risk.

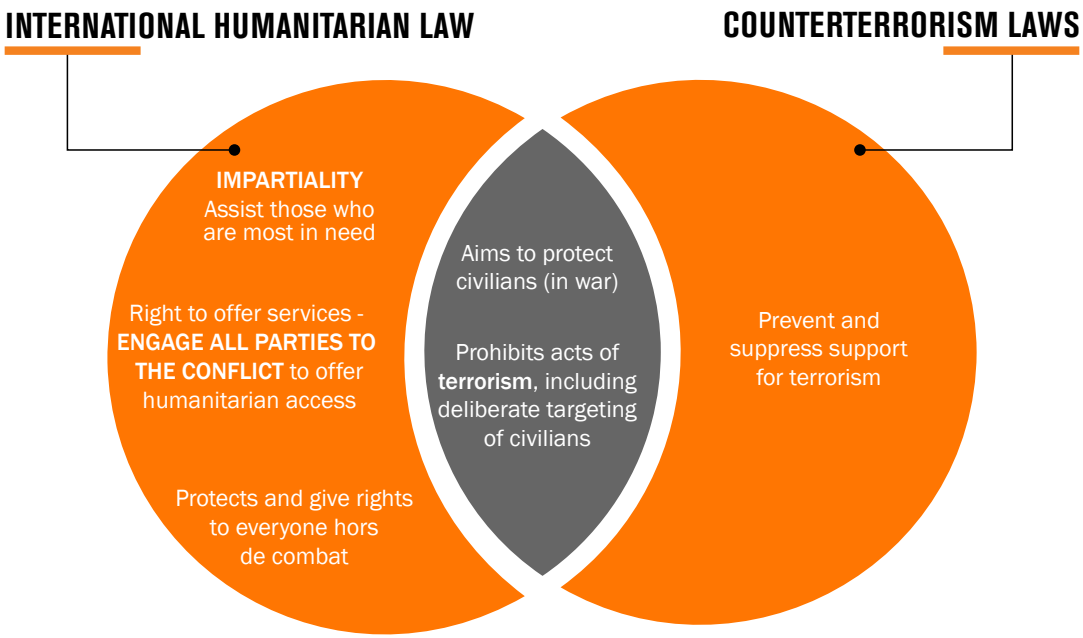
2 COUNTERTERRORISM MEASURES AND PRINCIPLED HUMANITARIAN ACTION

This section is designed to help develop your understanding of counterterrorism measures and how they can affect principled humanitarian action. By the end of it, you should be able to identify the sources of the counterterrorism measures that affect your organisation's work, and some of the impacts on its operations.

2.1 WHAT IS TERRORISM?

There is no universally agreed definition of terrorism. The United Nations Security Council (UNSC) provides one in resolution 1566[6] from 2004 which refers to terrorism as "criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organisation to do or to abstain from doing any act".

There can be some crossover[7] between counterterrorism measures and IHL, with both prohibiting acts of terror and aiming to protect civilians in situations of conflict. However, there are also significant differences.



6 United Nations, Security Council resolution 1566 (2004) https://www.un.org/ruleoflaw/blog/document/security-council-resolution-1566-2004-on-threats-to-international-peace-and-security-caused-by-terrorist-acts/

7 International Committee of the Red Cross, Terrorism, https://www.icrc.org/en/war-and-law/contemporary-challenges-for-ihl/terrorism

2.2 WHERE DO COUNTERTERRORISM MEASURES COME FROM?

Counterterrorism measures are introduced through:

- UNSC resolutions and other international instruments.
- Regulations introduced by regional bodies such as the European Union (EU).
- States' domestic laws.

Once introduced, these measures are often reflected in donor grant agreements.

2.3 INTERNATIONAL LEVEL: UN SECURITY COUNCIL

UNSC resolutions are the main instrument for introducing counterterrorism resolutions at the international level.

The first legal instruments to combat terrorism were established before the 11 September 2001 attacks, but much more extensive measures have emerged since. UNSC resolutions such as 1267[8] from 1999 and 1390[9] from 2002 were aimed at al-Qaeda and the Taliban. They were the first to introduce sanctions against individuals and groups who were designated as terrorist, and to oblige UN member states to freeze their funds and assets.

Not all sanctions introduced by the UNSC or others are counterterrorism-related. Sanctions can also form part of efforts to reverse territorial aggression, restore democratically elected leaders, promote human rights, and promote disarmament. The motivation behind their imposition may vary, but the negative impacts of sanctions on humanitarian action are often similar.

Subsequent UNSC resolutions have required UN member states to adopt laws and measures to prevent and suppress the financing of terrorist acts, and to prevent and suppress the recruitment and financing of foreign terrorist fighters. These resolutions are binding on all member states, which must adopt or adapt national laws and regulations accordingly.

The UNSC has made only limited efforts to minimise the impact of its counterterrorism and sanctions resolutions on humanitarian action. Only one sanctions[10] regime, relating to Somalia, includes an exemption for humanitarian assistance. This was adopted in 2010 during a famine to ensure aid agencies would still reach areas controlled by al-Shabaab, a group subject to an asset freeze under the sanctions, without fear of violating the regime. No other such exemptions have been adopted by the UNSC.

Several UNSC resolutions specify that counterterrorism measures must be in line with member states' international legal obligations, including IHL. Resolutions 2462[11] and 2482,[12] adopted in 2019, go further than this in urging states "to take into account the potential effects of counterterrorism measures on exclusively humanitarian activities, including medical activities, that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law". States are not, however, given guidance on how to do this, nor is their adherence to such requirements publicly reported on. This shortfall and the absence of a universally accepted definition of terrorism means there is a growing tendency among member states to introduce broad counterterrorism measures that may impede humanitarian action.

---

8 United Nations, Security Council resolution 1267 (1999), https://undocs.org/S/RES/1267(1999)

9 United Nations, Security Council resolution 1390 (2002), https://www.undocs.org/S/RES/1390%20(2002)

10 United Nations, Security Council resolution 2498 (2019), https://undocs.org/en/S/RES/2498(2019)

11 United Nations, Security Council resolution 2462 (2019), https://undocs.org/S/RES/2462(2019)

12 United Nations, Security Council resolution 2482 (2019), https://undocs.org/S/RES/2482(2019)

WHAT IS A HUMANITARIAN EXEMPTION?

The term generally refers to language that excludes humanitarian organisations and their staff from the requirement to comply with elements of sanctions regimes and counterterrorism measures that may obstruct their work. Humanitarian exemptions carve out a space for principled humanitarian action, allowing organisations to deliver their services without the risk of contravening such regimes.

The humanitarian exemption in the Somalia sanctions regime, for example, reads:[13] "... without prejudice to humanitarian assistance programmes conducted elsewhere, the measures imposed by paragraph 3 of its resolution 1844 (2008) shall not apply to the payment of funds, other financial assets or economic resources necessary to ensure the timely delivery of urgently needed humanitarian assistance in Somalia, by the UN its specialised agencies or programmes, humanitarian organisations having observer status with the United Nations General Assembly that provide humanitarian assistance, and their implementing partners including bilaterally or multilaterally funded non-governmental organisations participating in the United Nations Humanitarian Response Plan for Somalia''.

Another examples is the EU Directive on Combating Terrorism (2017/541), which states:[14] "The provision of humanitarian activities by impartial humanitarian organisations recognised by international law, including international humanitarian law, do not fall within the scope of this Directive, while taking into account the case-law of the Court of Justice of the European Union'.

Read more on humanitarian exemptions here.[15]

[13] United Nations, Security Council resolution 2498 (2019), https://undocs.org/S/RES/2498(2019)

[14] EU-Lex, Directive (EU) 2017/541, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541

[15] Harvard Law School, Understanding humanitarian exemptions: U.N. Security Council sanctions and principled humanitarian action http://blogs.harvard.edu/pilac/files/2016/04/Understanding_Humanitarian_Exemptions_April_2016.pdf

2.4 INTERNATIONAL LEVEL: FINANCIAL ACTION TASK FORCE

A second key source of international counterterrorism measures is the Financial Action Task Force (FATF), an inter-governmental body responsible for setting standards and promoting the implementation of legal, regulatory and operational measures to combat terrorist financing.

FATF has developed a series of recommendations that member states are expected to implement to counter the financing of terrorism. The recommendations relate to how states should regulate the banking and other sectors to mitigate terrorist financing risks. FATF monitors states' progress in implementing its recommendations and demands reforms if deemed necessary.

FATF recommendations are in theory non-binding, but non-compliance may result in blacklisting, which could impede a state's access to international financial markets. This gives governments a very strong incentive to comply. The FATF standards do not always provide clear guidance for implementation, which creates space for misinterpretation, misuse or overcompliance by states and banks. Humanitarian organisations face difficulties in accessing financial services, including bank transfers, as a result of bank derisking. Bank derisking occurs when banks refuse to offer services, such as accounts or transfers, to organisations or locations perceived as high risk in order to minimise their own exposure to accusations of facilitating terrorist financing, which could result in fines or other repercussions.

FATF AND BANK DERISKING

In 2001, FATF issued recommendation eight, which identified NPOs (non-profit organisations – the umbrella term FATF uses to refer to civil society, development and humanitarian organisations) as "particularly vulnerable" to exploitation for terrorist financing purposes, and called on countries to ensure that NPOs cannot be misused by terrorist organisations. Governments translated the recommendation into domestic banking regulations, banks became increasingly cautious in their dealings with NPOs and the phenomenon of bank derisking emerged.

The NPO Coalition on FATF, a group of civil society organisations formed to advocate with FATF and represent NPOs' interests, conducted a focused campaign to encourage an end to the trend of derisking through changes to recommendation eight. FATF revised the recommendation in 2016 as a result, directing governments to take a more nuanced and risk-based—rather than risk-averse—approach when developing counterterrorism financing measures to avoid the disruption of "legitimate non-profit activities".

The revision has not, however, had the desired effect, partly because regulators have not issued new guidance to banks instructing them to take a risk-based approach in their dealings with NPOs. According to the revised recommendation, member states are required to carry out and update counterterrorist financing risk assessments[16] of different sectors, including NPOs.

Based on the assessment findings, countries should adopt measures proportionately targeting only those NPOs at risk. However, FATF does not provide guidance to states regarding how risk assessments should be carried out, resulting in widely varying approaches. Often NPOs are not consulted during risk assessments of the sector.

In the absence of both guidance from governments emphasising the need for a risk-based approach, as well as accurate, nuanced risk assessments of the NPO sector, banks continue to take risk-avoidance approaches in their dealings with humanitarian organisations. Rather than assessing the risks involved in a particular transaction, taking into account NPOs' risk mitigation measures, banks tend to perceive any transaction to an area where DTGs are present as inherently high risk. Banks are concerned about fines for non-compliance with counterterrorist financing rules and have very little incentive to carry out potentially risky transactions.[17] As a result, derisking has become a major operational constraint[18] for organisations trying to transfer money to countries where sanctions have been imposed or DTGs are present.

More information on derisking and on the NPO Coalition on FATF can be found here.[19]

---

16 Global NPO Coalition on FATF, The ABCs for Risk Assessment of the Nonprofit Sector in Your Country, http://fatfplatform.org/wp-content/uploads/2018/10/HANDOUT-Risk-Assessment.pdf

17 Human Security Collective, Derisking and civil society: drivers, impact and solutions, https://www.hscollective.org/news/timeline/article-derisking-and-civil-society-drivers-impact-and-solutions/

18 Charity & Security Network, C&SN report on financial access for U.S. nonprofits reveals broad scope of problem https://charityandsecurity.org/csn-reports/finaccessreport/

19 Financial Action Task Force, The Global NPO Coalition on FATF, http://fatfplatform.org/about/

2.5 REGIONAL LEVEL

Measures adopted by the EU are an additional source of obligation for relevant member states.[20] UNSC sanctions are given effect in EU regulations and the bloc may also adopt its own sanctions, as it has done for Syria and Ukraine. The EU's approach to humanitarian exemptions is not uniform. If it is implementing sanctions, it follows the UNSC's approach. The EU will not insert an exemption if the UNSC does not. When it imposes its own sanctions, it sometimes includes exemptions and at other times allows member states to issue licenses for certain activities. The purchase of fuel in Syria, for example, is prohibited by sanctions, but an exemption for projects funded by the EU and its member states allows it to be bought for use in providing humanitarian assistance.

The EU has created a number of tools to help improve understanding of its sanctions regimes, including a sanctions map[21] and FAQs[22] on its Syria measures. It does not, however, instruct member states on how to fulfil their responsibility for implementing sanctions or granting licenses. Approaches tend to vary considerably from one member state to another, adding to an already confusing operating environment for humanitarian organisations.

2.6 DOMESTIC LEVEL

States are obliged to reflect global and, where relevant, regional instruments in their national laws, but the absence of an internationally recognised definition of terrorism allows them very broad scope in doing so, including the ability to factor in their own political, security and military objectives.

States can also develop their own counterterrorism measures. Some, such as the United States (US) and the United Kingdom (UK), have their own lists of DTGs and designated individuals in addition to those maintained by the UNSC.

States criminalise support for terrorist groups in different ways. In the aftermath of 11 September 2001, the US government introduced legislation that criminalised the provision of "material support" to DTGs. Four types of support are included: training, expert advice or assistance, service and personnel. US law on material support has broad scope and extraterritorial jurisdiction. This means it can be applied to organisations and individuals regardless of where the alleged crime was committed, the nationality of the perpetrator or the source of the funds involved. This differs from the situation in the UK, where material support crimes are framed not in terms of support to listed groups but to terrorist acts. The UK asserts extra-territorial jurisdiction over these offences only when committed by its own nationals.

Governments are also increasingly introducing broad counterterrorism legislation in response to the issue of returning "foreign fighters",[23] those who travelled abroad to support or take part in "terrorist acts" or "the providing or receiving of terrorist training" but have since returned to their home country. Most states have legislation in place that makes it a crime to travel abroad to commit a terrorist offence, but in order to make it easier to prosecute "foreign fighters", some are introducing broader legislation, making it a criminal offence simply to travel to certain areas.

---

20 Chatham House, Recommendations for reducing tensions in the interplay between sanctions, counterterrorism measures and humanitarian action, https://www.chathamhouse.org/sites/default/files/publications/research/2017-08-23-sanctions-counterterrorism-humanitarian-action-gillard-final.pdf

21 European Union sanctions map, https://www.sanctionsmap.eu/#/main

22 European Commission, EU restrictive measures in Syria – FAQs, https://ec.europa.eu/fpi/what-we-do/sanctions/eu-restrictive-measures-syria-%E2%80%93-faqs_en

23 United Nations, Security Council resolution 2178 (2014), https://www.un.org/sc/ctc/wp-content/uploads/2015/06/SCR-2178_2014_EN.pdf

2.7 CASE STUDY: UK COUNTER-TERRORISM AND BORDER SECURITY ACT

The UK government adopted new legislation in 2019 that gives the government power to make it an offence for UK nationals and residents to enter or remain in a designated country or part of a country. The new legislation is designed to make it easier for the government to prosecute foreign fighters who have returned to the UK, and the act does not contain an exemption for humanitarian workers who may need to enter designated areas.

The designated areas clause as originally proposed exposed staff of humanitarian organisations who enter those areas to the risk of arrest and criminal charges upon their return to the UK. Such legal proceedings against an aid worker engaged in legitimate activity could have a major impact on an organisation, given the resources, cost and possible reputational damage involved.

Several organisations advocated for a humanitarian exemption to provide the legal clarity to protect aid workers who travel to designated areas from arrest. The government initially resisted but ultimately it changed its position. The bill was passed with an exemption[24] for those "providing aid of a humanitarian nature".

Shortly after it passed, the Dutch government tabled a similar bill, again without a humanitarian exemption. Humanitarian organisations expect this issue to keep arising as governments introduce increasingly broad counterterrorism legislation designed to make the prosecution of returned foreign fighters easier.

Read more about advocacy efforts in the UK here[25] and here,[26] and see a joint press release from INGOs on the issue here.[27]

HOST COUNTRY COUNTERTERRORISM MEASURES

Much of the focus on how counterterrorism measures impact humanitarian action tends to be on measures imposed by donor governments. It should also be recognised, however, that measures imposed by host governments can have a significant impact on the staff and operations[28] of humanitarian organisations. Local staff may be particularly exposed to these risks.

Typical offences under local laws that could impact humanitarian work and humanitarian workers may include the prohibition of indirect financing of terrorism, material support laws and the prohibition of broad forms of association with designated groups. These offences can lead to the potential criminal responsibility of staff.

In addition, several host governments have brought in so-called 'NGO laws', which sometimes invoke national security concerns in order to restrict or control the activities of humanitarian organisations by using counterterrorism and anti-money laundering (AML) measures. These restrictions can include burdensome registration requirements and limitations on foreign funding, and can go as far as to give governments power to approve projects and oversee the selection of suppliers and beneficiaries.[29]

---

24 UK Government Legislation, Counter-terrorism and border security act 2019 http://www.legislation.gov.uk/ukpga/2019/3/section/4/enacted

25 Bond, NGOs academics and journalists to be exempt from Counter-Terrorism and Border Security Bill, https://www.bond.org.uk/press-releases/2019/01/ngos-academics-and-journalists-to-be-exempt-from-counter-terrorism-and-border

26 The Guardian, MPs pass counter-terror bill amendments to protect aid workers, https://www.theguardian.com/global-development/2019/jan/23/mps-pass-counter-terror-bill-amendments-to-protect-aid-workers

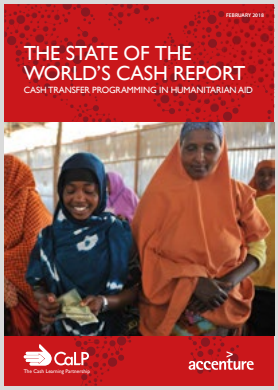
27 Bond, UK's leading NGOs concerned aid workers journalists and development researchers will be caught out by Counter Terrorism and Border Security Bill, https://www.bond.org.uk/press-releases/2018/11/uks-leading-ngos-concerned-aid-workers-journalists-and-development

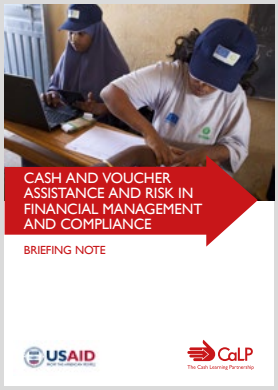
28 The Guardian, Nigerian army orders closure of aid agency for 'aiding terrorism', https://www.theguardian.com/global-development/2019/sep/20/nigerian-army-orders-closure-of-aid-agency-for-aiding-terrorism

29 Freedom House, The spread of anti-NGO measures in Africa: Freedom under threat, https://freedomhouse.org/report/special-report/2019/spread-anti-ngo-measures-africa-freedoms-under-threat

IMPACT OF COUNTERTERRORISM MEASURES ON CVA

Research[30] shows that cash and voucher assistance (CVA) is no riskier than other forms of aid, but donors tend to increase their scrutiny of implementing partners' risk management policies and procedures for this type of assistance, mainly due to concerns about the misappropriation of cash. This tendency toward risk aversion was reflected in the Department for International Development's (DFID) April 2019 decision to pause[31] its support for CVA in north-east Syria as a precautionary measure over concerns about the risk of diversion.





The Cash Learning Partnership (CaLP) commissioned a scoping study[32] on CVA and risk in 2019, which examined three key areas:

1. Transferring funds to countries of operation: identifying competent and willing banking and other financial service providers (FSPs).
2. Identifying in-country FSPs: know-your-customer regulations and financial sector identity checks by in-country providers, including mobile network operators.
3. Beneficiary identification and data security: counterterrorism financing and anti-money laundering regulations and international sanctions applicable to CVA recipients.

The study concluded that the measures reviewed had not explicitly targeted CVA to date, but a trickledown effect was observed on FSPs' ability and willingness to facilitate this type of assistance. It also found a lack of policies or guidance on the measures to ensure CVA remains unencumbered by bureaucratic processes and risk aversion. This may lead to the use of in-kind assistance instead of CVA, even if the latter has been deemed more effective.

There are also concerns about increased scrutiny of the CVA chain of custody between the recipient and where the funds are spent. To mitigate the impact of increasing restrictions on CVA, CaLP aims to:

- Advocate for humanitarian perspectives to be considered in policy making.
- Support the building of an evidence base on the impact of counterterrorism-related restrictions on CVA.
- Continue to provide technical and policy support to the CVA community of practice and cash working groups to develop shared risk registers informed by national regulations and practices.

Read more about this topic from CaLP here.[33]

30 Cash Learning Partnership, State of the worlds cash report, https://www.calpnetwork.org/publication/state-of-the-worlds-cash-report/

31 The New Humanitarian, Fleeing the last days of the Islamic State in Syria, https://www.thenewhumanitarian.org/photo-feature/2019/01/24/islamic-state-syria-fleeing-last-days

32 Cash Learning Partnership, Cash and voucher assistance and risk in financial management and compliance, https://reliefweb.int/sites/reliefweb.int/files/resources/1575312843.CaLP%20CVA%20Financial%20Management%20Compliance%20FINAL.pdf

33 Cash Learning Partnership, Risk, https://www.calpnetwork.org/themes/cash-and-voucher-assistance-and-risk/

2.8 WHAT ARE THE RISKS?

Risk category	Operational impact
Criminal	**Prosecution over the provision of support to designated terrorist groups (DTGs):** The broad definition of support for terrorism that some states have adopted makes this a risk for humanitarian organisations and their staff if they are deemed to have provided support for DTGs by carrying out certain activities. For example, the US Supreme Court ruled in 2010 that training DTG members in IHL was classed as material support and so prohibited. **Criminalisation of staff:** Criminal laws designed to counter terrorism have the potential to criminalise humanitarian workers. Local staff members may be particularly exposed to risks under the host country's counterterrorism legislation. Potential offences that could involve criminal responsibility include presence in an area of designated terrorist activity, the indirect financing of terrorism and broad forms of association with proscribed groups.
Security	**Insecurity:** Engaging with NSAGs, regardless of whether they are DTGs, is a key element of gaining and maintaining secure access to people in need. Engagement also helps to establish consent and acceptance for humanitarian organisations' activities, which is vital to ensure staff safety. Counterterrorism measures can create uncertainty for organisations about whether contact with NSAGs that are also DTGs is permissible. Some organisations refrain from engaging with these groups as a result. Organisations that fail to engage with NSAGs because of counterterrorism concerns risk negative perceptions of partiality and non-neutrality, which in turn puts staff at risk. Other organisations do engage with these groups, but do not provide staff with support and guidance about how to do this. This can create a "don't ask, don't tell" approach whereby field-based staff engage without the knowledge of senior management, and feel unable to openly discuss dilemmas and risks.
Contractual	**Delay:** The inclusion of counterterrorism clauses in grant agreements can delay the implementation of humanitarian initiatives while organisations work with donors to try to negotiate changes or seek clarity about vague wording. The fact that donors do not always inform organisations when they introduce a new counterterrorism clause or change the wording of existing clauses only increases the likelihood of delays. Some requirements, including screening and/or vetting procedures, may also delay the provision of assistance. Delays can also occur as a result of bank derisking, which happens when banks refuse, or take longer than expected to provide transfers to locations perceived as high risk in order to minimise their own exposure to accusations of facilitating terrorist financing.
	Lower quality of response: Compliance with donor counterterrorism requirements may reduce the quality of an organisation's response by causing it to choose modalities perceived as lower risk even if they are less appropriate and effective for a particular context.
	Risk transfer to staff: Counterterrorism-related wording in grant agreements can be vague and difficult to interpret. It is not uncommon for humanitarian organisations to accept these clauses without fully understanding the requirements involved. Staff tasked with implementing a project under a grant agreement may not have been involved in negotiating it, but they shoulder the burden of complying with the requirements, and organisations often do not provide the necessary guidance or support on how to do so.
	Risk transfer to local partners: International NGOs often pass on donor counterterrorism requirements to local partners in the form of "flow-down clauses" without ensuring they understand what signing the clause entails, or that they have the resources and capacity to comply. Local partners may accept requirements that are impossible for them to adhere to or that endanger their staff as a result.
	Establishing a precedent: This can occur when one organisation accepts a counterterrorism clause that others deem unacceptable. Some organisations may choose to negotiate more favourable terms, but their leverage and ability to do so is weakened if others have already accepted the requirements.
	Loss of funding: Some organisations have refused donor funding as a result of uncertainty about, or unwillingness to accept the terms of counterterrorism clause required of them. Expenditure may also be disallowed under a contract if an organisation does not comply with all donor regulations.
Humanitarian principles	**Compromised impartiality:** In order to minimise exposure to counterterrorism risks, organisations may choose not to provide assistance in areas controlled by NSAGs that are also DTGs, regardless of the humanitarian needs there. This compromises the impartiality of their response and leaves affected populations without the assistance they need simply because of their location. If an organisation is not perceived as impartial, it can also put staff safety at risk.

2.9 CASE STUDY: RISKS RELATED TO INDIRECT SUPPORT TO A DTG

Global Solidarity is an international humanitarian organisation that runs large-scale programmes in areas affected by conflict. Global Solidarity works in area X, which is controlled by local authorities who have strong links with a DTG. Operations are managed remotely. There are no international staff based in the area because of access and security concerns. Global Solidarity put out a tender for the provision of trucked water for area X. The process was administered by the remote management team per Standard Operation Procedures (SOPs). After the bid process, one of the bidders alleged that contractors had to pay three per cent of the contract value to the local authorities in order to obtain approval to operate in area X.

Global Solidarity's field coordinator based in area X confirmed this was the case. This was the first time the remote management staff had been informed that field staff were aware of such payments or had any confirmation of their existence.

No tender bids for any current or previous contracts had mentioned a requirement to pay percentage fees to the local authorities to operate in area X. The bids were very detailed, so the fees, which amounted to thousands of dollars, appear to have been absorbed within the overall bids in a way that hid them from Global Solidarity. The fees contravened Global Solidarity's policies on facilitation payments, and the local authorities' relationship with a DTG carried further implications.

A report was provided to Global Solidarity's regional anti-corruption adviser, who launched an internal investigation. The remote management team immediately suspended the signing of new contracts until the matter could be fully investigated. Global Solidarity made an initial declaration to associated donors and sought legal advice on anti-corruption and terrorism financing legislation.

Global Solidarity also raised the issue with Office for the Coordination of Humanitarian Affairs (OCHA), requesting that it intercede with the local authorities to seek a waiver that would exempt NGOs from paying fees imposed on services that contributed to the provision of humanitarian relief. The engagement, which was undertaken with other affected humanitarian organisations, was successful and a waiver was granted.

Global Solidarity engaged the donor that funded the trucked water project in discussions about risk sharing. The donor agreed the payments in question did not constitute significant irregularities but chose to classify the costs as non-reimbursable and subject to repayment.

The incident sheds light on the obstacles faced in providing humanitarian aid in areas where DTGs may be active, and the additional challenges associated with managing operations remotely. It also shows that internal checks and balances can help to mitigate issues that may arise from remote management, and that coordination and collaboration among humanitarian organisations and donors is essential to bring about solutions.

3 COUNTERTERRORISM CLAUSES AND PARTNERSHIP AGREEMENTS

Counterterrorism clauses intended to ensure that donors' funds are not used to benefit DTGs are becoming increasingly common in grant agreements. These clauses can, however, present significant challenges for humanitarian organisations. This section is designed to develop your understanding of these clauses. By the end of it, you should be able to identify potentially problematic wording related to counterterrorism that appears in grant agreements, know how to engage with donors to discuss counterterrorism clauses, and develop an internal process for decision making on whether and how to proceed with funding opportunities that pose risks related to counterterrorism measures.

3.1 WHERE ARE COUNTERTERRORISM CLAUSES FOUND?

Counterterrorism clauses may be found in the following types of partnership agreements:

- Agreements between a donor, including states and multilateral agencies, and a humanitarian organisation, in which the former requires the latter to comply with a counterterrorism clause.
- Humanitarian pooled fund agreements.
- Agreements between humanitarian organisations, in which:
  - An organisation is the recipient of bilateral funds from a donor that requires it to include, or 'flow down', counterterrorism clauses in all sub-agreements linked to the funding of the project. In some cases, even if a bilateral agreement does not stipulate that the grantee must include a counterterrorism clause in sub-agreements, the organisation may be responsible if a sub-grantee puts the recipient in breach of its agreement with the donor.
  - An organisation has a policy of including counterterrorism clauses in its sub-agreements, usually reflected in its template for partnership agreements. Some UN agencies, for example, include such clauses in their templates.
- Commercial or service contracts between a donor government or multilateral institution and a humanitarian organisation.

Donors may adopt a standard form of clause inserted into all contracts, or they may adapt their clauses, or include additional requirements, depending on the context, the programme, or the recipient of funds.

Counterterrorism clauses are sometimes inserted in sections of a grant agreement covering anti-bribery, anti-fraud and anti-corruption measures, but they can also appear elsewhere, including in the general conditions of an agreement. Donors do not always inform partners when they change the wording of counterterrorism clauses or when they introduce new clauses.

Signatories to grant agreements are obliged to comply with all clauses and to apply them in good faith. As such, it is vital that an organisation review each agreement thoroughly before signing to ensure it is fully aware of the requirements, regardless of whether it has signed previous agreements with the same donor or not. A thorough review helps to ensure that any problematic language is identified, allowing the organisation time to seek clarity, renegotiate wording if necessary and make a considered decision about whether to sign the agreement.


© NRC/Jim Huylebroek

It should be noted that not all donor-imposed counterterrorism requirements appear in grant agreements. They can also arise in pre-contract negotiations. For example, the United States Agency for International Development's (USAID) Proposal Guidelines for Risk Mitigation in High Risk Environments require agencies to include risk assessments and mitigation strategies for diversion in environments it identifies as high risk 'due to the presence of groups and individuals sanctioned by the U.S. Government'. Another example is USAID's certifications and assurances, which must be signed and submitted with proposals. Documents like these also form part of agreements with donors, and should be considered in decision-making processes.

The table in Tool 2: Examples of counterterrorism clauses provides examples of current counterterrorism clauses used in agreements with donor governments, country-based pooled funds, NGO downstream partnerships and development-donor grants. They show that the content and scope of counterterrorism clauses can vary significantly. These clauses are provided as examples and should not be interpreted as examples of best practice, nor as being compatible with principled humanitarian action.

Furthermore, counterterrorism clauses may include vague or unclear language, making it difficult for organisations to understand what they are agreeing to and their liabilities in case of a breach. Counterterrorism clauses may also include requirements incompatible with a principled humanitarian approach, such as vetting beneficiaries. This can result in risk transfer, in which donors seek to mitigate their own risks by passing them on to grantees.

Find an extensive analysis of counterterrorism clauses from the Harvard Law School here.[34]

[34] Harvard Law School , Counterterrorism and humanitarian engagement project, https://reliefweb.int/sites/reliefweb.int/files/resources/CHE_Project_-_Counterterrorism-related_Humanitarian_Grant_Clauses_May_2014.pdf

3.2 UNDERSTANDING COUNTERTERRORISM CLAUSES

Definitions and scope of terminology

As identified during interviews conducted as part of the research for this toolkit, humanitarian organisations may face challenges in interpreting the meaning and implications of counterterrorism clauses that appear in partnership agreements.

Agreements may use phrases such as:

- "Employ all reasonable efforts to ensure" or "apply the highest reasonable standard of diligence to ensure" that assistance is not diverted to DTGs. This means an organisation may be held liable if its assistance is diverted, and the required standard of due diligence has not been applied. The specific wording used will determine the degree of liability.

- An organisation must "commit to the war against terror". This language raises concerns about neutrality and may undermine operational independence. It could also have security implications because it may influence how DTGs view the organisation.

- An organisation is prohibited from providing "material support" "directly or indirectly" to DTGs and those "associated with" DTGs. Such prohibitions lead to concerns around the scope and application of the requirement and the potential impact on commitments to an impartial response. Organisations must, for example, interpret whether "associated with" applies to relatives of DTG members or communities where DTGs are active.

Agreements may have references to "knowledge" and "intent":

- If humanitarian assistance is diverted to a DTG, the organisation responsible may not be aware of the diversion and may not have intended it. Counterterrorism clauses may indicate whether "knowledge" and "intent" are relevant and the impact they might have on the organisation's degree of liability in the event of diversion.

Agreements may have flow-down clauses or implications:

- Humanitarian organisations often include counterterrorism clauses in their sub-contracts to ensure implementing or consortium partners comply with their donors' requirements. One donor's counterterrorism clause may "flow down" or "flow across" a large number of organisations and sub-contractors as a result.

Agreements may have references to or implications for vetting:

- To ensure that funds or other assets are not made available to DTGs, counterterrorism clauses sometimes require recipient organisations to ensure their staff, contractors, and the staff of any implementing partner organisations do not appear on relevant lists of these groups. Some donors may require the names of potential beneficiaries to be checked against these lists. For more information, see the info box on vetting staff, partner staff and beneficiaries.

Processes for understanding and addressing counterterrorism clauses

Humanitarian organisations must be aware of their obligations under the proposed terms of a grant agreement before they sign it. Its implications should be understood in advance, and organisations should use a systematic process to identify and try to address any concerns. There is no one "correct" approach to take, but the processes outlined below serve as guidance.

1. Organisations should develop and implement procedures to ensure that all grant agreements are read and understood in full before they are signed. Management, policy, legal personnel and other departments as necessary should review the entirety of the agreement. For more information, see Tool 3: Reviewing counterterrorism clauses on how to review counterterrorism clauses.

2. Internal codes of conduct and anti-corruption, risk management and other relevant policies should be consulted to establish whether the counterterrorism language in a grant agreement is inconsistent with these internal policies.

3. Prior to entering into negotiations with a donor regarding the terms of a partnership agreement, organisations should establish an organisational position regarding which terms of an agreement will be deemed acceptable and which terms will constitute a breach of organisational policies and values.

4. Consult other humanitarian organisations that receive funds from the same donor.

5. Organisations could consider asking the donor for its own interpretation of the clauses and the degree of liability inferred, acknowledging that the donor's interpretation may be as strict as possible.

6. Organisations should consider documenting their own interpretations of the clauses. Organisations should consider whether additional resources would be needed to meet the agreement's obligations, and whether their capacity to provide principled humanitarian assistance would be affected. Organisations should ensure they can provide clear guidance, as well as any necessary resources, to staff responsible for implementation. If additional resources will be required to ensure compliance with the clauses, organisations should consider asking the donor to cover any related costs.

7. Organisations can use Tool 4: Go/No-Go checklist in relation to counterterrorism measures to help decide whether the funding opportunity should be pursued.

8. Organisations should recall that, while in some cases counterterrorism clauses can be negotiated with donors, the laws of the donor state will prevail over the agreed upon terms. Regardless of the text of the partnership agreement, the organisation and those signing it will be subject to the laws of the donor state and should therefore ensure they are aware of the obligations these impose. Depending on the state, these laws may infer different kinds of liability and may have differing territorial limitations.


© NRC/Jim Huylebroek

NPA VS USA

USAID's Office of the Inspector General (OIG) requested Norwegian People's Aid (NPA) assistance in February 2017 "pursuant to an ongoing investigation" related to grants made to the organisation in South Sudan dating back to 2012. NPA cooperated fully with the request and shared all required documentation. After several rounds of submissions, NPA was informed that it was the subject of the investigation, which related to a breach of the False Claims Act[35] involving NPA's activities in support of a democratisation project for young people in Gaza between 2012 and 2016 and a demining project in Iran that ended in 2008.

USAID had not funded either of the projects in question but had funded an NPA project in South Sudan in 2012. In accepting the funding in South Sudan, NPA was required to sign USAID's anti-terrorist certification, which states: "The Recipient, to the best of its current knowledge, did not provide, within the previous ten years, and will take all reasonable steps to ensure that it does not and will not knowingly provide, material support or resources to any individual or entity that commits, attempts to commit, advocates, facilitates, or participates in terrorist acts, or has committed, attempted to commit, facilitated, or participated in terrorist acts."

The US authorities said NPA had not complied with this clause given that it had provided "training and expert advice or assistance" to DTGs in the course of its previous programmes in Gaza and Iran, and its certifications about knowingly providing material support or resources to prohibited parties were false, despite the fact that USAID had not funded these projects.

NPA disagreed with the fairness of the OIG's claim. It had understood the anti-terrorist certification to apply only to activities supported by US funding. However, NPA decided to settle out of court in 2018 to the tune of more than USD 2 million. It took the decision in consultation with its legal team because of the estimated cost, resources and time involved in taking the case to trial. Its decision also considered the worst-case scenario of losing the court case and incurring even greater financial penalties that would jeopardise the organisation's work.

Given that the case hinged on whether USAID's clause had universal jurisdiction or only covered US government funding, NPA decided to end its cooperation with this donor that interprets its terms and conditions as superseding those of others. It took this decision after USAID also made it clear that negotiating the wording of the clause was not an option.

[35] Charity & Security Network, False claim act lawsuits: What nonprofits need to know, https://charityandsecurity.org/issue-briefs/fca-basics-handout/

VETTING STAFF, PARTNER STAFF AND BENEFICIARIES

For the purposes of this toolkit, screening is understood to be the process by which an organisation checks whether prospective staff, staff of partner organisations or contractors appear on lists of designated terrorists identified by the relevant donor or host government.

Screening can be done manually, by cross checking with relevant lists maintained by donor governments and/or institutions, such as the UN or EU, or by using online services that allow names to be checked against several lists at once. Vetting is a more in-depth process of conducting background checks which could include verification of past employment and criminal history checks.

Generally, humanitarian organisations are not required to share personal data from screening or vetting processes with donors, although USAID's Partner Vetting System (PVS) is an exception to this.

To ensure that funds or other assets are not made available to DTGs, counterterrorism clauses sometimes require recipient organisations to ensure their staff, the staff of any implementing partner organisations, contractors and suppliers do not appear on relevant lists of these groups.

Most organisations will perform checks on some staff, depending on their grade, and on contractors and suppliers, depending on the value of the transaction.

In some cases, donors may require organisations to check whether individuals on beneficiary lists are associated with DTGs. This requirement can be explicitly articulated in a grant agreement, or it can be indicated by vague language around the need to ensure that no assistance or funds are made available to those who are associated with DTGs.

Vetting of beneficiaries is a red line for many humanitarian organisations because it could lead to organisations selectively responding to the needs of affected populations, withholding assistance from certain potential beneficiaries rather than providing assistance on the basis of needs alone. It could also negatively impact communities' perception of humanitarian organisations, by giving the impression that organisations that perform vetting are politically aligned with certain donor governments.

The beneficiary selection process for humanitarian programmes is based on needs, vulnerability and selection criteria generally defined by respective clusters and sectors in line with international standards and in consultation with relevant technical authorities and local communities. To ensure an impartial response, affiliation with political, or other groups, does not form part of the selection criteria.

Requirements to vet beneficiaries are particularly common from development donors, which tend to have more stringent counterterrorism measures than humanitarian donors. Sometimes this is because these donors are development banks, which require adherence to AML and counterterrorism funding (CTF) requirements imposed by regulators. It should be noted that where these donors are state agencies, they should not impose conditions that are in tension with the state's IHL obligations. However, negotiating exceptions or the removal of problematic clauses from agreements with development donors on the basis of incompatibility with the humanitarian principles can be difficult because these donors do not have a humanitarian mandate.

Humanitarian organisations should pay close attention to any counterterrorism clauses included in grant agreements with non-humanitarian donors to ensure that accepting financial support does not compromise their adherence to the humanitarian principles.

In practice this is difficult as the lines between humanitarian and development funding are increasingly blurred, partly reflecting moves toward the humanitarian–development nexus.[36] Many

[36] Humanitarian Law and Policy, A humanitarian-development nexus that works, https://blogs.icrc.org/law-and-policy/2018/06/21/humanitarian-development-nexus-that-works/

© NRC/Jim Huylebroek

organisations are now 'dual mandate' and engage in both humanitarian and development work. The situation is further complicated by the fact that some key funds for humanitarian organisations tend to come from development donors, including for resilience and early recovery activities, particularly in contexts where development organisations do not have the necessary presence or access.

Vetting requirements and principled humanitarian action: what are the challenges?

- Designation of an individual or group as terrorist should not deprive those designated from the protection and assistance afforded to them by IHL. Donor requirements to exclude those who are designated as terrorist from beneficiary lists may contravene IHL.

- The humanitarian principles require organisations to act independently from donor governments' political, security and military objectives. If organisations are required to provide information about staff, contractors or beneficiaries to donors, they could be involved in information gathering for donor governments. This may negatively impact the perception of an organisation by a community or NSAG, and it could prove a security risk to staff where the organisation relies on community acceptance to safely access affected populations. It could also pose a security risk to beneficiaries if they are perceived to be associated with a certain donor government.

- If organisations are required to provide the donor government with information about their staff, partners or beneficiaries, it could compromise the right to privacy and may violate data protection and privacy laws.

- Vetting requirements could cause organisations to 'self-censor' and avoid areas controlled by designated groups in order to ensure compliance with donor counterterrorism requirements, rather than providing assistance on the basis of needs alone.

- The bureaucratic procedures sometimes associated with vetting can delay operations and impede the timely delivery of humanitarian assistance.

3.3 CASE STUDY: ADVOCACY AND PRINCIPLED PARTNERSHIP CONDITIONS

Donor Government introduced a revised version of its global partnership agreement with a new counterterrorism clause but did not tell its partner World Response about the new language. World Response discovered it when its internal focal point at headquarters reviewed the agreement and was particularly concerned that the clause could be interpreted as a requirement to vet beneficiaries—a red line under World Response's internal counterterrorism policy.

World Response notified its senior management immediately about the new clause and the need to determine whether to sign the agreement and continue its partnership with Donor Government.

World Response requested an opinion from its legal adviser, who determined that signing the agreement and complying with the new clause would require it to cross its red line on vetting beneficiaries. World Response shared the legal opinion with Donor Government and asked for the wording of the clause to be adjusted to ensure it did not impede its ability to adhere to the humanitarian principles. World Response also contacted other humanitarian organisations to raise awareness of the new clause. The other organisations also raised their concerns with Donor Government.

Donor Government lawyers reviewed the feedback from World Response and the other organisations but did not accommodate the request and stated there was no further room to negotiate.

It suggested that World Response could, if interested, attach a clarifying statement to the agreement to indicate that although it had signed the legally binding document, it did not agree that it was under any obligation to vet beneficiaries.

The statement would not, however, be legally binding and World Response could still be held accountable for not adhering to all clauses in the partnership agreement should any issues arise. Donor Government also noted that other organisations had raised the counterterrorism clause as a concern, but this had not prevented them from signing the agreement.

World Response decided it was not in a position to sign the agreement because doing so would require crossing the red lines in its counterterrorism policy. It also decided to discontinue its partnership with Donor Government on the same basis. It did not consider Donor Government a significant partner and believed it would be able to fill the potential funding gap via other sources.

This example illustrates the difficulties organisations face in advocating against counterterrorism-related language in grant and partnership agreements, particularly if they are unable to negotiate collectively with donors. Individual organisations have less leverage on their own. This case also illustrates the importance of having an internal counterterrorism policy with clearly identified red lines—a vital tool with which to guide decision making when dilemmas arise.

4 COUNTERTERRORISM AND RISK MANAGEMENT FRAMEWORKS

This section explores practical aspects of risk management and steps your organisation can take to strengthen risk management policies and practices, while maintaining a principled approach. It endeavours to make risk management approaches accessible and understandable to a broad range of staff, including those who are field-based and responsible for programme implementation.

4.1 WHAT IS RISK MANAGEMENT?

Risk management is a process to help staff systematically think though what risks may arise in specific contexts and what can be done to mitigate these. It addresses the question of what organisations can do to make sure that as those most in need are assisted as much as possible in a principled manner, despite challenging contexts, by identifying, monitoring and tackling key risk factors.

Definitions:

- **Risk:** Uncertainty, whether positive or negative, that may affect the outcome of an activity or the achievement of an objective.
- **Risk management:** a cycle of identifying and assessing risks, assigning ownership of them, taking action to anticipate and mitigate them, and monitoring and reporting progress.

Why use a risk management framework?

Owing to the nature of the environments they work in, staff of humanitarian organisations constantly manage risk. Where this is done in an ad-hoc manner there may be gaps and inconsistencies in the way risks are identified and managed. In order to prevent this, organisations should consider adopting a framework to establish clear processes for identifying and managing risks. Counterterrorism issues should feature strongly within this framework. The key components of a risk management framework are outlined in this section. Where an organisation does not have a clear risk management approach in place staff and teams can still apply these risk management processes to the contexts they work in to address CT issues.

RISK	DESCRIPTION
Operational	Inability to achieve objectives
Security	Violence or crime
Safety	Accident or illness
Fiduciary	Misuse of resources, including fraud, bribery and theft
Information	Data loss, breaches or misuse
Legal/compliance	Violation of laws and regulations
Reputational	Damage to integrity or credibility
Operational	Inability to achieve objectives
Ethical	Insufficient application of the humanitarian principles and duty of care, lack of adherence to organisational values and mandate

4.2 COMPONENTS OF A RISK MANAGEMENT FRAMEWORK

Risk management has four main components:

1. **Identification**
2. **Assessment**
3. **Monitoring**
4. **Reporting**

❶ Identification

Risks can be grouped into two main categories, external and internal, and many subcategories. SWOT analysis can be used to identify risks, with strengths and weaknesses focusing on internal sources of risk and opportunities and threats focusing on external ones.

Organisations should try to identify all risks, including those associated with counterterrorism measures. Once identified, these should be added to an internal risk register,[37] which should be reviewed and updated regularly to account for any changes in context or environment.

❷ Assessment

Once an organisation has identified and classified its risks in a register, it needs to assess them. This tends to be done by assigning each risk a numerical value, often on a scale of one to five, for its likelihood, impact and sometimes an organisation's vulnerability to it. The values are then combined to establish an overall score for each risk.

There are various ways of assessing risks objectively. The table in Tool 5: Criteria for calculating risk shows some criteria for evaluating risk impact and likelihood values. The overall scores for each risk can then be put into Tool 6: Risk matrix to create a concise visualisation of the risk assessment.

Establishing a score for residual risk allows an organisation to assess whether the risks are outweighed by the expected humanitarian outcomes of the activity involved. This assessment can be made using programme criticality tools, such as this one used by the UN.[38] The outcome of this assessment can vary depending on an organisation's risk appetite, or willingness to accept risk, and its risk tolerance, or capacity to accept risk.[39]

---

37 Humanitarian Outcomes, Risk register tool, https://www.humanitarianoutcomes.org/publications/risk-register-tool

38 United Nations, What is programme criticality? https://programmecriticality.org/Static/index.html

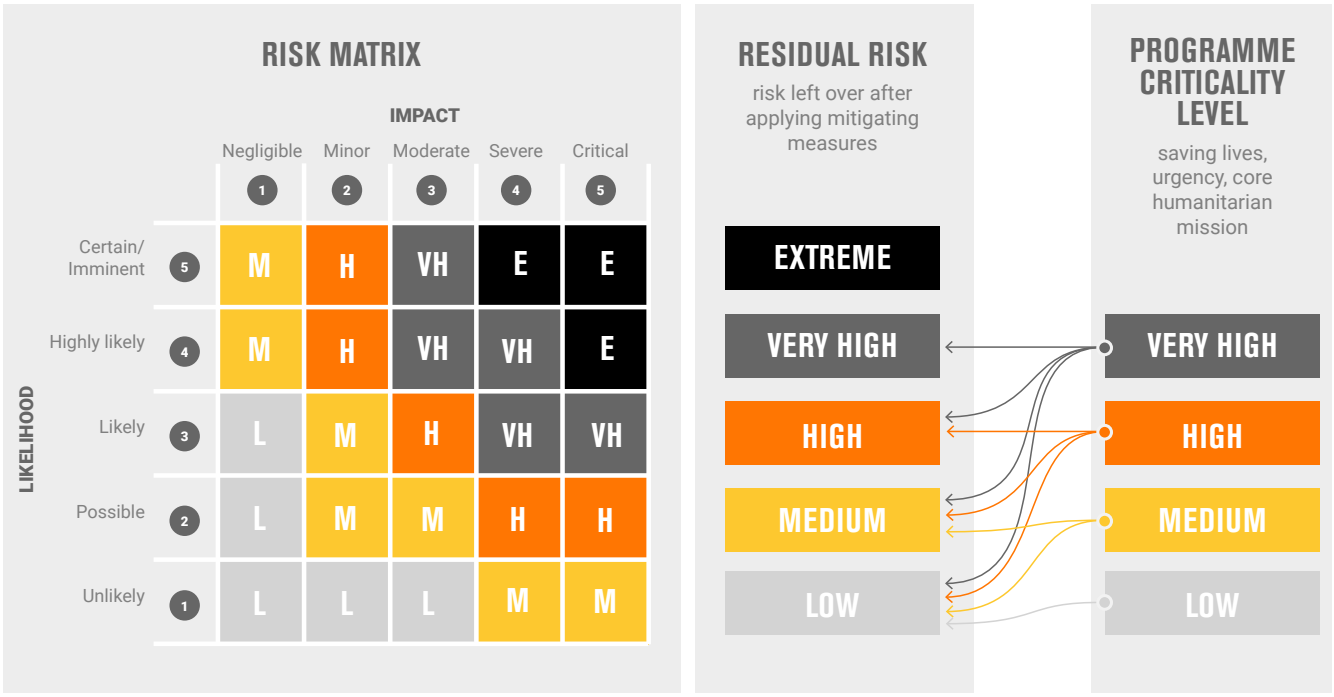
39 International Council of Voluntary Agencies, Risk and humanitarian culture: An ICVA briefing paper, https://reliefweb.int/sites/reliefweb.int/files/resources/Risk%20and%20Humanitarian%20Culture_Briefing%20Paper%202020.pdf

RISK MITIGATION AND PROGRAMME CRITICALITY

Once an organisation has identified and put risk mitigation measures into place for a particular risk–for example, counterterrorism measures–it must then assess whether there are any associated residual risks that it is unable to mitigate. After identifying these residual risks, the organisation must then assess them against its own risk appetite, or willingness to accept risk. One way to assess whether a particular risk might be outweighed by the importance of the activity involved is through a programme criticality framework.

A programme criticality framework is an approach to inform decision making around an organisation's level of acceptable risk, particularly risks that remain after an organisation has put risk mitigation measures into place. A programme criticality framework can provide a structured process to decision making that evaluates the balance of implementing an activity against the residual risks faced. A programme criticality framework should use a set of guiding principles and a systematic, structured approach to decision making to ensure that activities involving an organisation's personnel, assets, reputation, security, etc., can be balanced against various risks. Programme criticality frameworks can also help an organisation weigh residual risks against commitments to humanitarian principles, particularly those guiding who the organisation assists, and the principles of humanity and impartiality.

In the current context, many donors are pushing implementing organisations to programme in very difficult areas while also maintaining a no-risk expectation. In most of the humanitarian contexts where humanitarian organisations operate today, these two expectations are increasingly at odds and have forced practitioners to try and develop more systematic approaches to navigating these dilemmas. If an organisation has already implemented all of the risk mitigation measures it deems feasible, but it is left with residual counterterrorism risks, the next step could be for the organisation to develop a programme criticality framework



BALANCING RISK AND PROGRAMME CRITICALITY LEVEL

© NRC/Jim Huylebroek

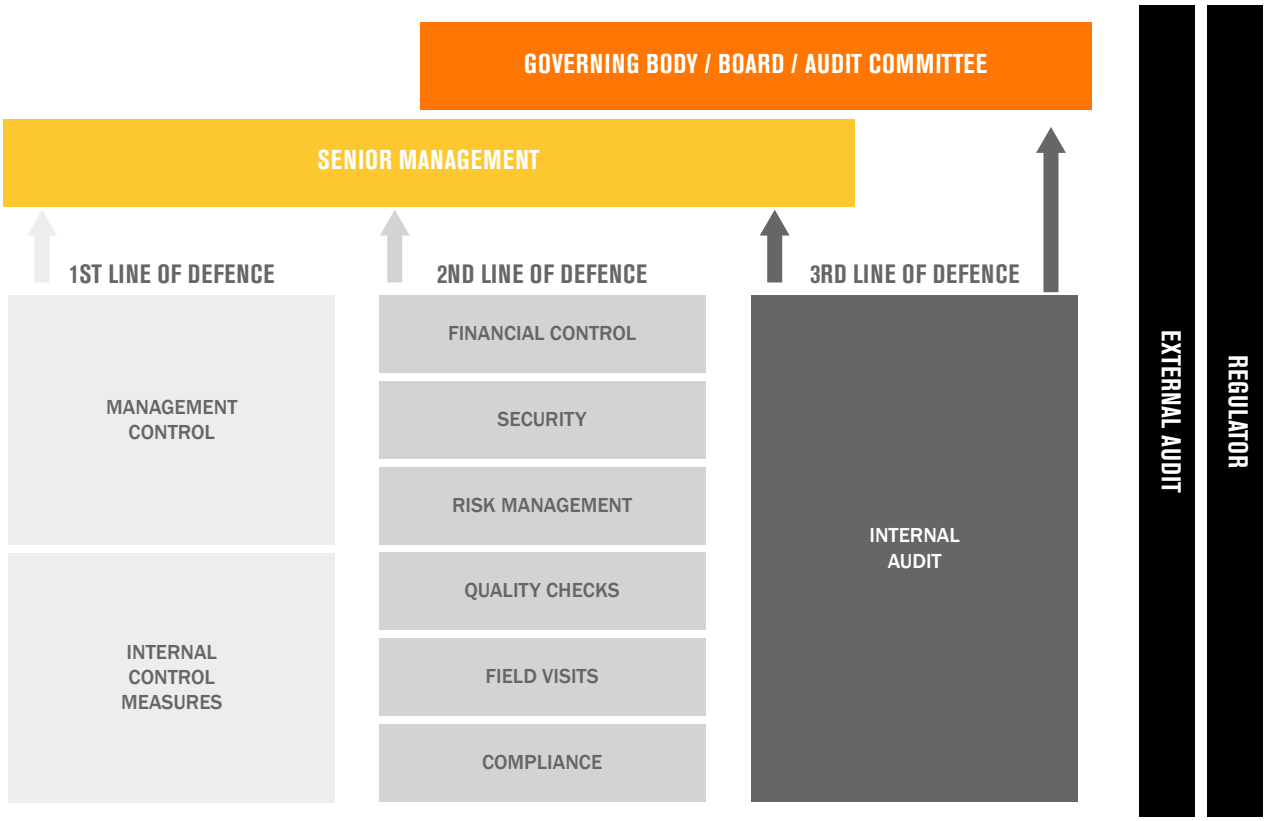
❸ Monitoring

Approaches to monitoring risk vary, but organisations tend to do so every quarter or trimester. They may also carry out ad-hoc monitoring if a specific trigger occurs. Risks related to specific programmes should be monitored throughout the programme cycle and discussed at programme review meetings.

❹ Reporting

Reporting on risk management should form part of the wider reporting processes that cover an organisation's overall direction, effectiveness, supervision and accountability.

- **Direction:** providing leadership, setting strategy and establishing clarity about what an organisation aims to achieve and how.
- **Effectiveness:** making good use of financial and other resources to achieve the desired humanitarian outcomes.
- **Supervision:** establishing and overseeing controls and risk management and monitoring performance to ensure an organisation is achieving its goals, adjusting where necessary and learning from mistakes.
- **Accountability:** reporting on what the organisation is doing and how, including reporting to donors.



THREE LINES OF DEFENCE MODEL

The "three lines of defence" model is an example of a governance model of which risk management is a key component.

Management control and internal control measures make up the first line of defence; the various risk control and oversight functions established by management make up the second; and independent assurance makes up the third. Each of the three lines of defence plays a distinct role in an organisation's wider governance framework.

An example application of this model could relate to a specific counterterrorism measure, such as the vetting of suppliers or employees, that would be implemented by staff in field offices. The process would require oversight from management as the first line of defence. As a second line of defence, compliance staff at the country or regional level would conduct spot checks and review implementation. The third line of defence is the organisation's internal audit team, which provides overall assurance to global management on the effectiveness of internal control procedures through regular audits.

SANCTIONS COMPLIANCE PROGRAMMES

The US government's Office of Foreign Assets Control (OFAC), part of the US Treasury Department, is primarily responsible for the implementation and supervision of the US government's sanctions programmes. Its Framework for OFAC Compliance Commitments strongly encourages organisations bound by sanctions regimes "to employ a risk-based approach to sanctions compliance by developing, implementing and routinely updating a sanctions compliance program (SCP)". The existence and effectiveness of such a programme is identified as a factor in any enforcement proceedings OFAC takes against organisations that may have violated sanctions and can reduce the amount of any fine imposed.[40]

OFAC states that an effective SCP should have five elements, all of which overlap considerably with the components of a risk management framework:

- **Management commitment:** Senior management should give compliance functions sufficient resources, authority and autonomy to manage sanctions risks and promote a culture of compliance in which the seriousness of sanctions breaches is recognised.
- **Risk assessment:** Organisations should conduct frequent risk assessments in relation to sanctions, particularly as part of due diligence processes related to third parties, and develop a methodology to identify, analyse and address the risks they face.
- **Internal controls:** Organisations should have clear written policies and procedures in relation to counterterrorism-related compliance, which adequately address identified risks, and which are communicated to all staff and enforced through internal and external audits.
- **Testing and auditing:** Organisations should regularly test internal control procedures to ensure they are effective and identify weaknesses or deficiencies that need to be addressed.
- **Training:** There should be a training programme for employees and other stakeholders, such as partners and suppliers.

The UK's Office of Financial Sanctions Implementation (OFSI), part of the UK government's treasury, performs a similar role. OFSI advises organisations to:

- Understand the scope and coverage of UK financial sanctions.
- Assess all aspects of proposed projects/ activities to identify whether any potential third parties are sanctioned entities.
- Tailor the organisation's compliance approach to the likelihood of dealing directly or indirectly with sanctioned entities.
- Consider other linked types of financial crime, such as terrorist financing or money laundering.
- Where risks are identified, conduct thorough checks of all points in the payment chain for project activities and of those involved in the project on the ground.

OFSI's compliance and enforcement model has four elements:

- Promote compliance by publicising financial sanctions.
- Enable compliance by providing guidance and alerts to organisations to help them fulfil compliance responsibilities effectively.
- Respond to non-compliance consistently, proportionately, transparently and effectively.
- Change organisations' behaviour through compliance and enforcement action, which will take account of measures being taken to improve future compliance.

[40] Legal Information Institute, CFR Appendix A to Part 501 - economic sanctions enforcement guidelines, https://www.law.cornell.edu/cfr/text/31/appendix-A_to_part_501

4.3 INTERNAL CONTROLS AND RISK MANAGEMENT

Internal controls are key elements of risk management frameworks. They include processes to assess, mitigate and monitor risks. Organisations can embed internal controls throughout the programme cycle and as part of its overall governance structures and reporting systems.

Internal control systems can be characterised as follows:

- **Preventive:** measures such as anti-diversion policies to ensure aid reaches its intended beneficiaries.
- **Corrective:** measures such as internal checks to establish whether counterterrorism-related risks have arisen during the programme cycle.
- **Directive:** measures such as counterterrorism policies that give staff clear guidance and establish red lines in relation to counterterrorism risks.
- **Detective:** monitoring measures such as spot checks to review whether staff have complied with counterterrorism requirements.

The following section examines various internal controls and approaches to the management of risks associated with counterterrorism measures. It includes the following components:

1. Counterterrorism policies
2. Policies for engagement with NSAG
3. Due diligence
4. Human resource policies
5. Anti-diversion policies
6. Monitoring and evaluation

Developing a counterterrorism policy

Counterterrorism policies are intended to ensure that staff comply with relevant counterterrorism measures while maintaining adherence to the humanitarian principles. They can articulate an organisation's mandate, and reiterate its commitment to the humanitarian principles, IHL and other laws and measures. They may include an overview of the measures the organisation has put in place to address concerns about the diversion of humanitarian assistance, including to DTGs. See Tool 7: Example counterterrorism policy.

Developing an NSAG engagement policy

NSAGs are present in most contemporary armed conflicts. In some contexts, NSAGs are designated as terrorist groups by the UN, the EU or by host or donor governments. Humanitarian organisations may engage with NSAGs, regardless of whether they are DTGs, for various purposes, including to negotiate access to populations in need of assistance.

To manage risks related to engagement with NSAGs who may be DTGs, some humanitarian organisations have developed policies for NSAG engagement that consider counterterrorism measures. These policies can help avoid the transfer of risk onto field-based staff by ensuring that staff have clear organisational guidance and support when engaging with these groups.

NSAG engagement polices should consider three specific kinds of counterterrorism measures: counterterrorism clauses in grant agreements, the potential criminalisation of humanitarian action, and sanctions. See Tool 8: Example NSAG engagement policy considering counterterrorism risks.

This content was developed in collaboration with Geneva Call. Geneva Call is a humanitarian organization working to improve the protection of civilians in armed conflict. Geneva Call engages NSAGs to encourage them to comply with the rules of war. More information about the organisation's work can be found here.[41]

[41] Geneva Call, Our mission, https://www.genevacall.org/

DEVELOPING A COUNTERTERRORISM POLICY	
WHO IS RESPONSIBLE FOR DEVELOPING A COUNTERTERRORISM POLICY?	
• A member of senior management should be the focal point for managing this undertaking. • Inputs from a legal adviser should be sought.	• Departments at headquarters and the field level should be tasked with providing inputs to the draft policy and reviewing it.
WHAT IS INCLUDED IN A COUNTERTERRORISM POLICY?	
• The principles and mandate to which the organisation is committed. • An overview of the laws that bind the organisation, which may include IHL, domestic laws in the countries where it is registered and operates, and sanctions. • The principles and commitments of staff members, such as ethical behaviour and anti-diversion.	• An overview of the measures the organisation has in place to provide principled humanitarian assistance, such as robust project cycle management (PCM), codes of conduct with oversight mechanisms, anti-corruption procedures, financial and procurement controls and procedures for the selection of partners and staff. • A statement of red lines that if crossed would constitute a breach of the policy.
HOW ARE COUNTERTERRORISM POLICIES DEVELOPED AND IMPLEMENTED?	
• The policy should be developed in a consultative, collaborative process to ensure it addresses the main issues that staff confront and guarantees buy in and acceptance among staff members. • A robust roll-out plan should be established, which includes awareness raising and staff training on how to adhere to the policy. • Staff should be provided with written guidance on the policy in an accompanying explanatory note that gives further detail of due diligence procedures, relevant handbooks and SOPs.	• Focal points to whom staff can turn with questions or to seek advice when dilemmas arise should be identified. • Control and oversight mechanisms, such as a reporting mechanism for violation of the policy, should be developed.
HOW OFTEN ARE COUNTERTERRORISM POLICIES REVISED?	
• Authoritative statements of principles and ethics, signed and endorsed by senior management, should generally not be revised.	• Other policy elements may need to be revised as counterterrorism measures evolve and their impact on principled humanitarian action changes.

DEVELOPING AN NSAG ENGAGEMENT POLICY THAT CONSIDERS COUNTERTERRORISM ISSUES

RATIONALE AND INTERNAL CONSIDERATIONS

- What is the purpose of the organisation's engagement with NSAGs? For example, an organisation that delivers humanitarian assistance may be concerned about indirect terrorist financing or violation of sanctions regimes, while an organisation working to promote IHL may be more concerned about the impact of material support laws on their work.
- How does the organisation safeguard the humanitarian principles in its engagement with NSAGs? How might the principles be challenged during engagement with NSAGs? For example, is there a risk to the organisation's independence through potential interference in beneficiary selection?
- What are the red lines in the engagement? Under what conditions would the organisation consider discontinuing engagement?
- What are the possible reputational risks for the organisation engaging with NSAGs? How can these risks be mitigated and managed?
- Do internal policies and procedures account for risks to staff emanating from national and international legislation? What are the potential consequences if the organisation engages with an NSAG that is designated as terrorist by the host government, on both its operations and its staff? What are the consequences if the organisation does not engage?
- Does the organisation track which staff members are negotiating with NSAGs? How does the organisation document negotiations processes? How is relevant data and information stored and protected?

COUNTERTERRORISM CLAUSES IN GRANT AGREEMENTS

- Do the organisation's grant agreements include clauses that prohibit using funds for NSAG engagement for general or specific purposes? Do relevant donors require due diligence steps during such engagement? If necessary, clarification or guidance should be sought internally. Refer to Tool 3: Reviewing counterterrorism clauses for more guidance on reviewing counterterrorism clauses in grant agreements.

SANCTIONS

- Is the NSAG designated as terrorist by the UNSC,[42] the EU[43] or by individual states, such as the US[44] or by the host government? Are high profile members or leaders of the NSAG designated under any of these regimes? It is also worth considering whether the group or its members are sanctioned by regimes that are not necessarily counterterrorism-related, as regardless of their objectives, sanctions can impact the broader legal and policy environment for a humanitarian organisation's engagement.[45]
- If the answer to either of the above questions is yes:
  - What is the scope of the sanctions and how may they impact the organisation's operations? Sanction regimes generally do not prohibit contact with DTGs, but asset freezes may require that organisations ensure that funds or dual-use goods are not made available to these groups.
  - Are there any exemptions in the sanction regime or is there a possibility to apply for a license? Exemptions normally require approval by the authority in charge of implementing the sanctions.
  - What are the consequences for violating sanctions regimes for the organisation and for staff members?
  - If staff members have questions about relevant sanctions regimes, who should they approach internally for support and guidance?

[42] United Nations, United Nations Security Council consolidated list, https://www.un.org/securitycouncil/content/un-sc-consolidated-list

[43] European Union sanctions map, https://www.sanctionsmap.eu/#/main

[44] United States Department of the Treasury, Office of Foreign Assets Control - Sanctions programs and information, https://www.treasury.gov/resource-center/sanctions/pages/default.aspx

[45] Chatham House, Recommendations for reducing tensions in the interplay between sanctions counterterrorism measures and humanitarian action, https://www.chathamhouse.org/publication/recommendations-reducing-tensions-interplay-between-sanctions-counterterrorism-measures

CRIMINALISATION OF HUMANITARIAN ACTION
• Has the organisation identified and mapped how the organisation and staff could be impacted by relevant criminal laws related to counterterrorism? Local staff members may be particularly exposed to risks related to host-country counterterrorism legislation. The following elements should be considered in such a mapping: - The national legislation of the host state, the state of registration of the organisation, the states of nationality of staff, donor states and third states with broad extraterritorial offences. - The jurisdictional links required. For example, is there a requirement for a link of nationality of staff, or of registration of the organisation? - The typical offences that could lead to the potential criminal responsibility of staff, include the following: prohibition of indirect financing of terrorism, material support laws, designated area offences that prohibit presence in areas of designated terrorist activity and the prohibition of broad forms of association with DTGs.

Due diligence

Due diligence encompasses a range of activities undertaken to ensure that humanitarian assistance reaches affected populations. When entering into an agreement or contract with another party, such as an implementing partner, due diligence includes assessing the robustness of its systems and its ability to carry out the relevant activities within the limits of an organisation's acceptable level of risk. Due diligence can involve both internal and external-facing policies and measures designed to obtain assurance of a potential partner's capacity and capability to deliver assistance and to comply with donor requirements, including those related to counterterrorism. Reviewing a potential partner's policies, systems, processes and past performance can lead to a more informed partnership that identifies, accounts for, and takes the appropriate measures to mitigate risks. Tool 9: Partnership assessment checklist could help guide an organisation's decision on whether to pursue a potential partnership.

CONDUCTING DUE DILIGENCE WITH PROSPECTIVE PARTNERS	
WHAT IS THE PURPOSE OF CONDUCTING PARTNER DUE DILIGENCE?	
• Explore opportunities for working together and identify areas for cooperation in the delivery humanitarian programs. • Ensure a possible partner organisation has effective systems and operational procedures in place. • Assess whether a potential partner poses a financial, reputational or programmatic risk to an organisation's operations and/or a protection risk for beneficiaries..	• Understand the acceptability and reputation of partner with communities and local authorities. • Confirm that the partner is not listed in any excluded party list due to linkages with criminal or political activity, terrorism or diversion of fund. • Confirm that the partner has the internal capacity to comply with all clauses influencing and included in any possible agreement, including those related to counterterrorism
WHAT AREAS COULD A PARTNER DUE DILIGENCE ASSESSMENT COVER?	
• Areas covered in a due diligence assessment will vary based on the specific situation, needs and context. Some of the domains to consider reviewing in a partnership due diligence assessment include: - Basic background and history - Mission and values - Governance - External engagement, influence, and reputation	- Organisational capacity - Operational capacity - Financial capacity - Logistical capacity
WHAT CAN AN ORGANISATION EXAMINE TO DETERMINE IF A PROSPECTIVE PARTNER'S VALUES ARE IN LINE WITH ITS OWN?	
• Human resources policies and codes of conduct. • Preventing Sexual Exploitation and Abuse (PSEA), criminal, and unethical activity policies. • Corruption and conflict of interest policies.	• Counterterrorism policies and procedures. • Stated commitments to the humanitarian principles and a do-no-harm approach.

HOW CAN AN ORGANISATION IMPLEMENT DUE DILIGENCE POLICIES AND PRACTICES?	
• Organisations can conduct due diligence assessments with the prospective partner by collecting information directly. • Organisations can collect information from other sources (e.g. other organisations that work with the prospective partner).	• Organisations can request a prospective partner complete a self-assessment; this should be used in tandem with the organisation's own due diligence assessment.

Human resources policies

Humanitarian organisations should ensure they institute human resources policies, including transparent and fair recruitment protocols, and communicate these clearly to staff. Human resources policies are a key part of organisation-wide risk management approaches and, as such, can help mitigate counterterrorism-related risks and reassure donors. Human resources policies include rules for recruiting, training, appraising, remunerating, disciplining and dismissing staff. Humanitarian organisations frequently include them in staff contracts as a legally binding set of obligations that both parties are expected to observe.

Codes of conduct are another important element of human resources policies. Codes of conduct establish standards of behaviour for an organisation and its staff. They commonly reflect a commitment to the humanitarian principles, mitigating the likelihood of compromising them.

Codes of conduct are non-binding, but they are often included in staff contracts, in which case they become a set of obligations that must be observed. Some organisations provide training and written guidance to staff on how to put their codes of conduct into practice. Codes of conduct may also include control and oversight mechanisms, such as disciplinary proceedings and whistle-blowing facilities.

REVIEWING AND DEVELOPING HUMAN RESOURCES POLICIES	
WHAT SHOULD BE CONSIDERED WHEN REVIEWING OR DEVELOPING HUMAN RESOURCES POLICIES?	
• Recruitment: Does the human resources policy and the recruitment procedures it governs ensure the most suitable and best-qualified candidates are selected, having undergone reference and employment verification and other checks? • Staff development: Does the human resources policy stipulate a plan to develop staff members' skills and improve the knowledge they require to do their job and progress in the organisation?	• Discipline: Does the policy establish clear procedures and rules for censuring staff members who violate the organisation's rules and regulations? • Appraisals: Does the policy detail how and how often such assessments take place? • Duty of care: What steps does the organisation take to ensure the health, safety and wellbeing of staff?
WHO IS RESPONSIBLE FOR HUMAN RESOURCES POLICIES?	
• Senior management, in consultation with the human resources department, is responsible for developing, reviewing and ensuring implementation of human resources policies.	• The legal department should also be consulted during their development.
WHAT SHOULD AN ORGANISATION CONSIDER WHEN IMPLEMENTING HUMAN RESOURCE POLICIES?	
• How to recruit, dismiss, remunerate, train and appraise staff. • How to develop a staff member's skills for their role.	• How to discipline staff members for violations of the organisation's policies.
HOW CAN AN ORGANISATION IMPLEMENT HUMAN RESOURCES POLICIES?	
• Human resources policies should be clearly communicated to all staff. • Relevant training should be available to staff.	• A confidential complaints or feedback mechanism should be put in place.
HOW OFTEN ARE HUMAN RESOURCES POLICIES REVISED?	
• There is no set schedule for doing so, but many organisations revise their human resources policies periodically or during a change in the organisation's circumstances.	

Anti-diversion policies

Humanitarian organisations have anti-diversion policies to mitigate the likelihood of assistance being diverted from affected populations. They may include:

- Measures to limit the likelihood of fraud and corruption.
- Procedures to regulate financial management.
- Guidance on access negotiations.
- Measures to reinforce an organisation's policies in areas such as training, information sharing, disciplinary investigations and monitoring.

REVIEWING AND DEVELOPING ANTI-DIVERSION POLICIES AND PRACTICES

WHAT SHOULD A REVIEW INCLUDE?

- There are no standardised anti-diversion policies, but they tend to address:
  - Fraud: Deception, for example by falsifying records to exaggerate the number of staff employed or beneficiaries covered by a project, to result in financial or personal gain
  - Embezzlement: The misappropriation of goods or funds for financial or personal gain
  - Corruption: Dishonest or fraudulent conduct by those in power, typically involving bribery; the aim of anti-corruption policies, including those on whistleblowers, is to ensure staff act ethically
  - Money laundering: The concealment of the origin of money obtained from criminal, terrorist or other illegal activities
  - Access: The methods by which an organisation engages with armed groups and negotiates humanitarian access

WHO IS RESPONSIBLE FOR DEVELOPING AND REVIEWING ANTI-DIVERSION POLICIES AND PRACTICES?

- Overall responsibility lies with senior management, which should assign responsibility to the relevant departments for implementing practices related to staff training, producing written guidance and carrying out control mechanisms such as audits.
- Field staff have a key role to play in the development of anti-diversion policies and practices, and should be consulted to ensure they are relevant and realistic.
- The legal department should also be consulted.

WHAT CONTENT SHOULD AN ANTI-DIVERSION POLICY INCLUDE?

- A statement of principles and definition of terms.
- Procedures for preventing diversion: standardising and maintaining bank records; standardising accounting practices, such as account codes and donor codes; classifying costs, for example as direct or indirect; ensuring internal controls, including the segregation of duties between staff responsible for procurement, finance, disbursing cash, payroll and liquidations; and financial reporting requirements.

HOW ARE ANTI-DIVERSION POLICIES AND PRACTICES IMPLEMENTED?

- All staff should receive training on the organisation's anti-diversion policies.
- All staff should receive written guidance on implementation.
- Control and oversight mechanisms, such as audits, spot checks and regular reports, should be put into place.

HOW OFTEN ARE ANTI-DIVERSION POLICIES AND PRACTICES REVISED?

- There is no set schedule for doing so, but many organisations revise their anti-diversion policies every few years or if they are found to no longer be fit for purpose.

Monitoring and evaluation (M&E) frameworks

Counterterrorism and M&E

M&E serves two purposes for humanitarian organisations. It provides the basis for learning and programme improvement, and it establishes evidence to meet internal and donor-related documentation and reporting requirements.

Humanitarian organisations should pursue three M&E strategies to mitigate counterterrorism-related risks:

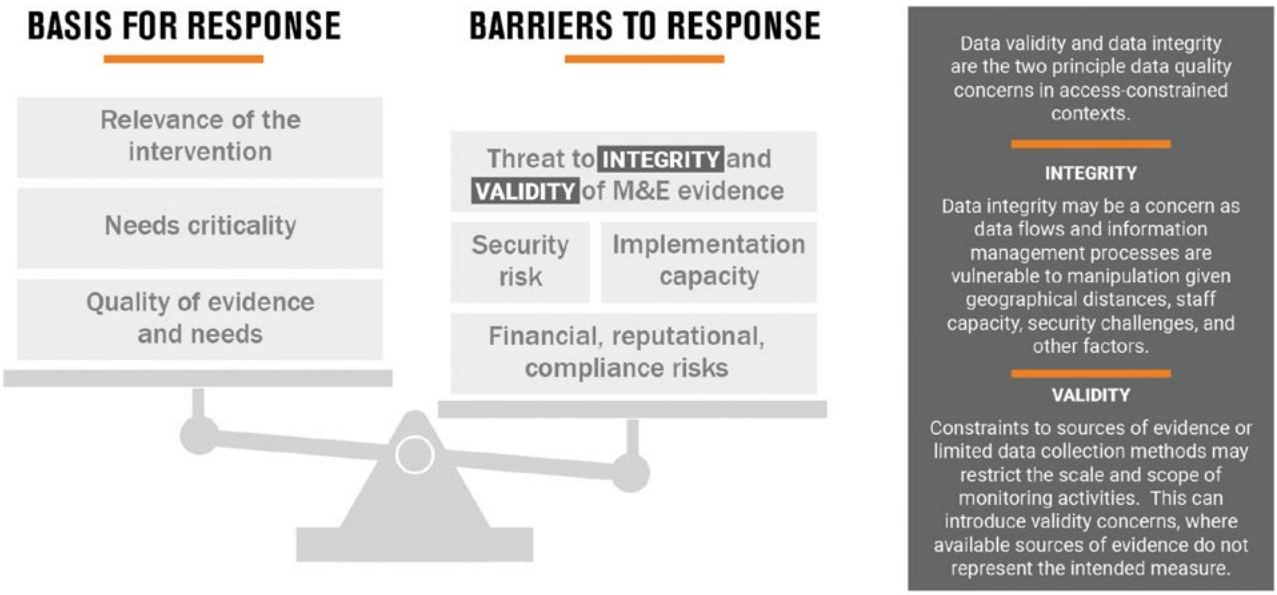
- Implement the best M&E system possible in the given context.
- Ensure transparency regarding the quality of M&E feasible.
- Take considered programme criticality decisions where M&E evidence is absent or weak.

Counterterrorism risks often arise in situations where humanitarian access is already constrained because of the presence of NSAGs who are DTGs.

In situations of constrained access M&E processes may be imperfect and there is a risk that some data may not accurate. An accurate assessment of the quality of M&E processes helps to determine how successful an organisation has been in using them to mitigate the risk that resources are diverted to DTGs.

A tool such as Tool 10: M&E minimum standards can help measure the quality of M&E processes objectively. The minimum standards also provide a concrete way of communicating M&E risks to donors to ensure that all parties are aware of them before a project is implemented.

M&E quality is an important consideration during programme criticality decision making. If the M&E minimum standards in Tool 10 indicate that M&E processes will be weak, management should take a programme criticality decision to weigh the potential humanitarian results of the intervention against the associated obstacles and risks, in this case to decide whether it is worth implementing the project if little or no data on its outcomes will be available.



Developing and implementing M&E systems

DO ALL PROJECTS HAVE THE FOLLOWING ELEMENTS OF AN M&E SYSTEM?

- **Results framework:** This is a cause-and-effect explanation of a project that predicts how activities and inputs will contribute to the objectives of the intervention. It should include indicators the project will measure to test key assumptions.
- **Indicator matrix and monitoring tools:** The former defines each indicator and stipulates how and when it will be measured. The latter are the questionnaires or other tools used to collect monitoring data.
- **Monitoring:** The use of the tools and methods described in the indicator matrix to collect and analyse data and determine performance.
- **M&E information management:** A system to ensure M&E data is maintained and accessible. Such a system may include a results database where indicator performance is tracked; a filing system for reports, distribution lists, photographs and other documents; and a case management database to track beneficiary engagement. An information management system can support an organisation's assertion that it knows who received assistance.
- **Evaluation plan:** Evaluations look at a programme's longer-term outcomes and impact. All programmes should have an evaluation plan, including a timeframe for evaluations, and their scope, purpose and funding sources.
- **Staff:** M&E requires enumerators to conduct interviews and collect data among the targeted communities; analysts to convert the raw monitoring data into indicator results and set them in a meaningful context; and management to be accountable for reporting requirements and use of the indicator results to improve programme design. Enumerators and analysts may be dedicated M&E staff or drawn from programme teams.

WHAT STRATEGIES EXIST TO MITIGATE CONCERNS ABOUT M&E QUALITY IN AREAS WHERE COUNTERTERRORISM RISKS ARE A CONCERN?

- **Contribution analysis:** If it is not possible to measure certain high-level indicators directly, a set of testable logical statements could be developed that demonstrate the programme's contribution to them. If, for example, an organisation purchases tents and distributes them to people who do not have shelter, and those people use the tents, it can reasonably conclude that the tents have made a positive contribution to protecting the recipients from the elements. Contribution analysis requires a carefully thought-out results framework. Read more about contribution analysis here.[46]
- **Triangulation:** Using various sources of data about the same indicator reduces the risk of poor quality and potentially misleading data. Photographs of aid distributions help to triangulate beneficiary lists, for example, and focus groups can be used to triangulate outcome indicator surveys.
- **Sample size and randomisation:** The careful selection of respondents can produce data and analysis that can be extrapolated to apply to all beneficiaries. Samples need to be sufficiently large, and all beneficiaries must have an equal chance of being included in them. Investing in rigorous and robust sampling methods will greatly increase the quality of M&E data. Read more about sampling here.[47]
- **Mobile data capture:** If enumerators capture data on a mobile device rather than on paper, records can be time, date and location stamped. This information allows supervisors to confirm that sampling methods were properly implemented and identify other data quality issues. There is also less risk of transcription errors or manipulation because the data-entry step from paper to digital is eliminated. KoBoToolbox[48] is a mobile data capture platform in use among some humanitarian organisations and offers many data capture tutorials.
- **Supervision:** Remotely managed programmes require more supervision, particularly to ensure M&E quality. Supervisors are needed to oversee data collection, clean data and ensure reporting and results make sense. This means investing in more staff hours and more dedicated staff to review reports and data from the field.
- **Feedback mechanism:** This provides a way for beneficiaries to submit independent comments on programme performance. Feedback mechanisms are difficult to put in place in areas where access is constrained, but when they can be implemented, they are a powerful way of learning about programme quality and triangulating M&E results. Read more about this in this paper from ALNAP.[49]
- **"Independent" monitoring:** Bias is always a concern, and a genuinely objective assessment of project performance can be useful. True independence, however, can be difficult to achieve, particularly in areas where access is constrained. Focusing on independence or engaging independent monitors may simply exchange one set of biases that are easier to anticipate for another that is harder to quantify.

---

46 BetterEvaluation, Contribution analysis, https://www.betterevaluation.org/en/plan/approach/contribution_analysis

47 Better Evaluation, Sampling, https://www.betterevaluation.org/en/rainbow_framework/describe/sample

48 KoBoToolbox, Powerful tools for data collection, https://www.kobotoolbox.org/

49 ALNAP, What makes feedback mechanisms work? https://bit.ly/306Ij8M

PCM and counterterrorism risks

PCM guidelines can form one component of a risk management framework for addressing counterterrorism issues, helping organisations to identify, evaluate and mitigate potential risks effectively throughout the different PCM phases.

This practical guide to PCM and counterterrorism risks[50] draws on content from this toolkit. It outlines the origin and impact of counterterrorism measures and proposes actions for humanitarian organisations to consider throughout the programme cycle to help identify, manage, and mitigate counterterrorism-related risks.

[50] Norwegian Refugee Council, Practical guide: Project cycle management and counterterrorism risks, https://www.nrc.no/resources/reports/practical-guide-project-cycle-management-and-counterterrorism-risks/

5 RESOURCES

Tool 1: Risk categories and operational impacts

Tool 2: Examples of counterterrorism clauses

Tool 3: Reviewing counterterrorism clauses

Tool 4: Go/No-Go checklist in relation to counterterrorism measures

Tool 5: Criteria for calculating risk impact and likelihood

Tool 6: Example risk matrix

Tool 7: Example counterterrorism policy

Tool 8: Example NSAG engagement policy considering counterterrorism risks

Tool 9: Partnership assessment checklist

Tool 10: M&E minimum standards

Project Cycle Management and counterterrorism risks

RISK CATEGORIES AND OPERATIONAL IMPACTS

TOOL 1

Risk category	Operational impact
CRIMINAL	**Prosecution over the provision of support to designated terrorist groups (DTGs):** The broad definition of support for terrorism that some states have adopted makes this a risk for humanitarian organisations and their staff if they are deemed to have provided support for DTGs by carrying out certain activities. For example, the US Supreme Court ruled in 2010 that training DTG members in international humanitarian law (IHL) was classed as material support and so prohibited. **Criminalisation of staff:** Criminal laws designed to counter terrorism have the potential to criminalise humanitarian workers. Local staff members may be particularly exposed to risks under the host country's counterterrorism legislation. Potential offences that could involve criminal responsibility include presence in an area of designated terrorist activity, the indirect financing of terrorism and broad forms of association with proscribed groups.
SECURITY	**Insecurity:** Engaging with non-state armed groups (NSAGs), regardless of whether they are DTGs, is a key element of gaining and maintaining secure access to people in need. Engagement also helps to establish consent and acceptance for humanitarian organisations' activities, which is vital to ensure staff safety. Counterterrorism measures can create uncertainty for organisations about whether contact with NSAGs that are also DTGs is permissible. Some organisations refrain from engaging with these groups as a result. Organisations that fail to engage with NSAGs because of counterterrorism concerns risk negative perceptions of partiality and non-neutrality, which in turn puts staff at risk. Other organisations do engage with these groups, but do not provide staff with support and guidance about how to do this. This can create a "don't ask, don't tell" approach whereby field-based staff engage without the knowledge of senior management, and feel unable to openly discuss dilemmas and risks.

CONTRACTUAL	**Delay:** The inclusion of counterterrorism clauses in grant agreements can delay the implementation of humanitarian initiatives while organisations work with donors to try to negotiate changes or seek clarity about vague wording. The fact that donors do not always inform organisations when they introduce a new counterterrorism clause or change the wording of existing clauses only increases the likelihood of delays. Some requirements, including screening and/or vetting procedures, may also delay the provision of assistance. Delays can also occur as a result of bank de-risking, which happens when banks refuse, or take longer than expected to provide transfers to locations perceived as high risk in order to minimise their own exposure to accusations of facilitating terrorist financing. **Lower quality of response:** Compliance with donor counterterrorism requirements may reduce the quality of an organisation's response by causing it to choose modalities perceived as lower risk even if they are less appropriate and effective for a particular context. **Risk transfer to staff:** Counterterrorism-related wording in grant agreements can be vague and difficult to interpret. It is not uncommon for humanitarian organisations to accept these clauses without fully understanding the requirements involved. Staff tasked with implementing a project under a grant agreement may not have been involved in negotiating it, but they shoulder the burden of complying with the requirements, and organisations often do not provide the necessary guidance or support on how to do so. **Risk transfer to local partners:** International NGOs often pass on donor counterterrorism requirements to local partners in the form of "flow-down clauses" without ensuring they understand what signing the clause entails, or that they have the resources and capacity to comply. Local partners may accept requirements that are impossible for them to adhere to or that endanger their staff as a result. **Establishing a precedent:** This can occur when one organisation accepts a counterterrorism clause that others deem unacceptable. Some organisations may choose to negotiate more favourable terms, but their leverage and ability to do so is weakened if others have already accepted the requirements. **Loss of funding:** Some organisations have refused donor funding as a result of uncertainty about, or unwillingness to accept the terms of counterterrorism clause required of them. Expenditure may also be disallowed under a contract if an organisation does not comply with all donor regulations.
HUMANITARIAN PRINCIPLES	**Compromised impartiality:** In order to minimise exposure to counterterrorism risks, organisations may choose not to provide assistance in areas controlled by NSAGs that are also DTGs, regardless of the humanitarian needs there. This compromises the impartiality of their response and leaves affected populations without the assistance they need simply because of their location. If an organisation is not perceived as impartial, it can also put staff safety at risk.

EXAMPLES OF COUNTERTERRORISM CLAUSES

TOOL 2

These clauses are provided as examples of the wording that has appeared in grant agreements. They should not be interpreted as best practice, nor as necessarily being compatible with principled humanitarian action.

EXAMPLES OF CLAUSES FROM HUMANITARIAN DONORS

Example A

Consistent with local and international legislation and applicable United Nations Security Council resolutions, the Participants are firmly committed to the international fight against terrorism. It is XXX's policy to seek to ensure that none of its resources are used, directly or indirectly, to provide support to individuals or entities associated with terrorism and that XXX staff and its programmes activity are compliant with counter terrorist financing legislation. In accordance with this policy, XXX expects the Partner and all Downstream Partners to make themselves aware of and comply with obligations under the relevant counter terrorist financing legislation.

The Partner will seek to ensure that none of the funds or assets provided under this Arrangement are made available or used to provide support to individuals, groups or entities associated with terrorism to aid, or otherwise support, terrorists or terrorist organisations. The Cooperation Partner agrees that it shall use all reasonable efforts to ensure that funds received under this Agreement are not used to engage in, support or promote violence, terrorist activity or related training of any kind and will take all appropriate precautions and institute all procedures necessary to prevent any portion of the funds from being so used. The Cooperation Partner shall screen its Implementing Partners to ensure that no such funds, other financial assets and economic resources will be made available, directly or indirectly, to, or for the benefit of, a natural or legal person, group or entity associated with terrorism consistent with European Union's Consolidated list of persons, groups and entities subject to EU financial sanctions including those named on the following lists as updated from time to time …

Example B

By signing and submitting this application, the prospective recipient provides the certification set out below:

The Recipient, to the best of its current knowledge, did not provide, within the previous ten years, and will take all reasonable steps to ensure that it does not and will not knowingly provide, material support or resources to any individual or entity that commits, attempts to commit, advocates, facilitates, or participates in terrorist acts, or has committed, attempted to commit, facilitated, or participated in terrorist acts...

Example C

The recipient must obtain the prior written approval of XXX before providing any assistance made available under this Award to individuals whom the Recipient knows to have been formerly affiliated with Boko Haram or the Islamic State of Iraq and Syria (ISIS)-West Africa, as follows: fighters, non-fighting members, individuals who may have been kidnapped by Boko Haram or ISIS-West Africa but held for periods greater than six months, and those under the control or acting on behalf of the same. Former affiliates do not include civilian populations who only resided in areas that were, at some point in time, controlled by the groups. The decision of XXX shall be provided promptly to the Recipient. Under no circumstances will the Recipient be obliged in this context to share any individual/personalised beneficiary data with XXX.

DEVELOPMENT DONOR CLAUSES

Example D

The Recipient undertakes:

Ⓐ to fully comply with anti-money laundering and terrorism financing standards in accordance with the FATF Recommendations, and implement, maintain and, if necessary, improve its internal standards and guidelines (including without limitation in relation to customer due diligence) appropriate to avoid any Sanctionable Practice, act of money laundering or financing of terrorism;

Ⓑ as soon as the Recipient or XXX becomes aware of or suspects any Sanctionable Practice, act of money laundering or financing of terrorism, to fully cooperate with XXX and its agents, in determining whether such compliance incident has occurred. In particular, the Recipient shall respond promptly and in reasonable detail to any notice from XXX and shall furnish documentary support for such response upon XXX's request.

Example E

ARTICLE 1. The Partner and XXX are committed to taking appropriate steps to ensure that funds provided under this Agreement are not used to aid, or otherwise support, terrorists or terrorist organisations.

ARTICLE 2. The Partner agrees that it shall use all reasonable efforts to ensure that funds received under this Agreement are not used to engage in, support or promote violence, terrorist activity or related training of any kind and will take all appropriate precautions and institute all procedures necessary to prevent any portion of the funds from being so used.

ARTICLE 3. The Partner shall screen its Implementing Partners to ensure that no such funds, other financial assets and economic resources will be made available, directly or indirectly, to, or for the benefit of, a natural or legal person, group or entity associated with terrorism consistent with European Union's Consolidated list of persons, groups and ties subject to EU financial sanctions.

ARTICLE 4. The Partner shall include in its agreements with its Implementing Partners, contractors and subcontractors a clause requiring that the recipient of Grant funds screens its potential subsequent Implementing Partners, contractors and subcontractors as per Article 3 above and uses all reasonable means to ensure that none of the funds provided under those agreements are used to benefit individuals or entities associated with terrorism.

ARTICLE 5. If, during the course of this Agreement, the Partner discovers any link whatsoever with any organisation or individual associated with terrorism, it must inform XXX immediately. The Cooperation Partner shall provide XXX with an account of all the known facts and shall continuously thereafter consult with XXX on the further handling of the matter.

REVIEWING COUNTERTERRORISM CLAUSES

TOOL 3

INTRODUCTION

Each grant agreement should be reviewed thoroughly before signing, regardless of whether your organisation has signed agreements with that donor in the past. Donors might not inform partners when they introduce new counterterrorism clauses or change the wording of existing clauses. Additionally, counterterrorism clauses are not always found in the sections of grant agreements where you might expect them. A complete review, including staff from across the organisation such as partnership advisers, legal advisers and programme managers helps ensure that any problematic language is identified in time to seek clarity from the donor or to try and renegotiate the wording. It should be noted that not all donor-imposed counterterrorism requirements appear in grant agreements. Other documents and information required by the donor, including as part of proposal submission, should also be considered.

Questions to consider

The following checklist is not exhaustive, but highlights some of the questions you can consider when reviewing an agreement:

- ✔ Does the agreement refer to international conventions or treaties, UNSC resolutions, donor policies, domestic or international laws or donor state regulations?
- ✔ Does the counterterrorism clause include the terms “intent”, “knowledge”, “knowingly” or “reasonableness”?
- ✔ Does the clause include language that is vague or unclear, such as “associated with” or “directly or indirectly”?
- ✔ Would you be required to vet or screen staff, partners or beneficiaries against lists of designated terrorist groups?
- ✔ Does the agreement include specific requirements or language on the recruitment of staff?
- ✔ Does the counterterrorism clause oblige you to incorporate the same clause in any sub-agreements?
- ✔ Would complying with the agreement impede your ability to adhere to the humanitarian principles?
- ✔ Would complying with the counterterrorism clause affect your acceptance among affected populations and parties to the conflict?

- ✔ What would the impact on beneficiaries be if your organization does not accept the agreement, or if it does accept and agrees to comply with the clause?
- ✔ Would you be unable to give staff and partner organisations clear instructions about how to comply with the obligations?

If the answer to any of the questions above is "yes"

❶Clarify the obligations and terms of the partnership agreement

- ✔ Consult internally with your senior management, policy advisers, legal personnel and others.
- ✔ Consult an external legal adviser for an interpretation of the clause.
- ✔ Based on this information, consider developing a note to file outlining an internal interpretation of the clause.
- ✔ Consult other organisations that receive funds from the same donor or partner.
- ✔ Ask the donor or partner for its own interpretation of the clause, the degree of liability inferred and the obligations to ensure compliance, bearing in mind that this interpretation may be as strict as possible.

❷Negotiate the terms of the agreement

As a result of the above consultations, you may choose to negotiate terms of the partnership agreement. This decision should be agreed by your senior management, policy advisers, legal personnel and other relevant departments.

- ✔ Identify areas of potential conflict between the terms of the agreement and your organisation's policies, operational capacity and humanitarian principles.
- ✔ Establish a position on which terms of the agreement are acceptable or unacceptable.
- ✔ Clarify the above position with the donor or partner.
- ✔ Share existing or planned risk management policies and practices.

If the answer to any of the initial questions is still "yes"

If the answer to any of the initial questions is still "yes" after negotiation, the organisation's management will have to assess the risks and liability involved for the organisation and its staff, its potential partners and sub-contractors and other humanitarian organisations. These risks should be weighed against potential risks to the organisation's humanitarian objectives before a decision is taken regarding whether to sign.
The go/no-go checklist could help to guide any such decision.

GO/NO-GO CHECKLIST IN RELATION TO COUNTERTERRORISM MEASURES

TOOL 4

INTRODUCTION

For any decision on funding opportunities, you should consult reference documents, such as a donor's official guidelines to ensure they do not contradict your organisation's internal policies or compromise a principled approach.

Specific conditions related to counterterrorism are not always known when responding to a call for proposals from new donors or previously untapped funding mechanisms, but it is important to consider them as early as possible, and certainly before entering into any legal agreement or contract. This will ensure compatibility with internal policies and standards and identify any red lines that might be crossed.

Location:		**Donor:**	
Funding Mechanism:		Checklist completed by (name, title):	
Signature:		Date:	

RESET

If the answer is "no" to any of the questions below

If the answer is "no" to any of the questions below, you should undertake additional analysis and approval should be sought from your organisation's senior management before a decision is made.

Approved donors:

❶ **Is the donor on a list of pre-approved partners and/or have you worked as a partner with this donor before?**

☐ YES ☐ NO

If no, seek additional information about the donor to ensure the partnership would not compromise independence or neutrality.

❷ **Has your organisation already worked with this donor on this particular funding mechanism?**

☐ YES ☐ NO

If no, seek additional information about the funding mechanism to ensure the partnership would not compromise independence or neutrality.

❸ **Does the funding opportunity require a national government or a specific government entity to be involved in implementation or oversight of your organisation?**

☐ YES ☐ NO

If yes, consider the authority in question carefully when you answer question 8.

Nature of opportunity:

❹ **Have you reviewed the funding opportunity document and confirmed a strategic and programmatic fit between your organisation's objectives and priorities and the donor's?**

☐ YES ☐ NO

If no, consider whether the opportunity should be pursued.

❺ **Is the objective of the funding opportunity humanitarian and not political?**

☐ YES ☐ NO

If no, seek additional information.

❻ **Do you know whether the donor has any counterterrorism-related requirements?**

☐ YES ☐ NO

If yes, ensure these requirements are reviewed by a legal adviser.

If no, seek additional information.

❼ **If you answered "yes" to the previous question, are you confident that accepting funds from the donor will not have any negative effects on your organisation's respect, real or perceived, for the humanitarian principles?**

☐ YES ☐ NO

If no, the opportunity must be dropped.

RESET

❽ **Are you confident that accepting the donor's funding and counterterrorism-related requirements will not have any negative effects on your organisation's reputation and acceptance among beneficiaries, host communities and others, or increase protection risks for the civilian population?**

☐ YES ☐ NO

If no, the opportunity must be dropped.

❾ **Does this funding opportunity …**

Allow your organisation to provide impartial assistance based on needs alone?

☐ YES ☐ NO

Allow your organisation to operate independently and without the imposition of a political agenda, including in the selection of target locations and beneficiaries?

☐ YES ☐ NO

Require your organisation to share data or information which goes beyond standard beneficiary intention surveys, and which could be used for security or military purposes?

☐ YES ☐ NO

If no to any of the above, the opportunity must be dropped.

Humanitarian access and security:

❿ **Have you conducted a context analysis, including a mapping of stakeholders, and a security risk assessment for the project location?**

☐ YES ☐ NO

If no, you should undertake a field visit to identify the main health, safety and security risks, and inform the go/no-go decision. You should record the main risks and mitigation measures in the project document.

⓫ **Are you confident there are no groups present in the target area that the donor designates as terrorist?**

☐ YES ☐ NO

If no, how will compliance with the donor's requirements be ensured while maintaining a principled approach?

Organisational capacity:

⓬ **Does your organisation have the financial management, grant management and project management capacity to implement the project?**

☐ YES ☐ NO

If no, ensure the resources required, including human resources, are included in the budget and covered by the donor.

RESET

CRITERIA FOR CALCULATING RISK IMPACT AND LIKELIHOOD VALUES

TOOL 5

RISK IMPACT

Descriptor	Score	Impact operations and staff or beneficiaries
INSIGNIFICANT	**1**	• No impact on operations • No impact on staff or beneficiaries • Complaint unlikely • Contractual or criminal risk remote • Remote risk to adherence to humanitarian principles
MINOR	**2**	• Slight impact on operations • Slight impact on staff or beneficiaries • Complaint possible • Contractual or criminal risk possible • Possible risk to adherence to humanitarian principles
MODERATE	**3**	• Some operational disruption • Potential for adverse reputational risk, avoidable with careful handling • Complaint probable • Contractual or criminal risk probable • Probable risk to adherence to humanitarian principles
MAJOR	**4**	• Operations disrupted • Adverse reputational risk unavoidable (local media) • Complaint probable • Contractual or criminal risk probable • Major risk to adherence to humanitarian principles
EXTREME/ CATASTROPHIC	**5**	• Operations interrupted for significant period of time • Major adverse reputational risk unavoidable (national media) • Major contractual or criminal risk expected • Loss of beneficiary confidence • Extensive risk to adherence to humanitarian principles

RISK LIKELIHOOD

Descriptor	Score	Impact on operations and staff or beneficiaries
REMOTE	**1**	May only occur in exceptional circumstances
UNLIKELY	**2**	Expected to occur in a few circumstances
POSSIBLE	**3**	Expected to occur in some circumstances
PROBABLE	**4**	Expected to occur in many circumstances
HIGHLY PROBABLE	**5**	Expected to occur frequently and in most circumstances

EXAMPLE RISK MATRIX

TOOL 6

RISK MATRIX

LIKELIHOOD	IMPACT: Negligible (1)	Minor (2)	Moderate (3)	Severe (4)	Critical (5)
Certain/ Imminent (5)	M	H	VH	E	E
Highly likely (4)	M	H	VH	VH	E
Likely (3)	L	M	H	VH	VH
Possible (2)	L	M	M	H	H
Unlikely (1)	L	L	L	M	M

EXAMPLE COUNTERTERRORISM POLICY

TOOL 7

1. PURPOSE AND BACKGROUND

As a non-profit non-governmental humanitarian organisation, World Response is committed to acting in a manner consistent with international humanitarian law and to undertaking its activities in accordance with the principles of impartiality, neutrality and independence. World Response is committed to ensuring that assistance and protection reach those most in need, and to preventing and mitigating the risk of aid diversion.

World Response's mandate means that the organisation sometimes operates in the same area as individuals and entities that states or intergovernmental organisations have designated as terrorist. Counterterrorism legislation in World Response's registration, operation and donor countries impose responsibilities and obligations on it and its staff. Non-compliance with these requirements may lead to disallowed costs, termination of grant agreements, legal action, fines, criminal charges and determinations of ineligibility for grants.

This policy sets out the main principles that will allow World Response to deliver assistance and protection to those most in need in accordance with humanitarian principles, while complying with relevant counterterrorism legislation and obligations.

2. MAIN PRINCIPLES

Humanitarian principles

World Response remains committed to accountability and transparency and adheres to the principles of humanitarianism and 'do no harm' set out in:

- ✔ The Code of Conduct of the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief
- ✔ The 2010 Humanitarian Accountability Partnership Standard in Accountability and Quality Management
- ✔ The SPHERE Humanitarian Charter and Minimum Standards in Humanitarian Response

General principles

World Response is required by domestic law to ensure that none of its funds or other assets are made available to people or groups listed under UN Security Council resolution 1267. Some of World Response's donor states have also established their own counterterrorism requirements. World Response may have contractual obligations to these donors to comply with their national counterterrorism frameworks. In addition, World Response must follow local laws in the countries in which it operates, including those related to counterterrorism.

World Response has put in place appropriate controls to prevent or mitigate the risk of intentional and/or reckless diversion of aid to non-state armed groups (NSAGs) in order to ensure that assistance and protection reach the intended beneficiaries.

These controls include:

- ✔ An ethical code of conduct, enforced by clear disciplinary procedures, which is binding on all World Response staff and consultants, and includes obligations to safeguard World Response assets and to act strictly in accordance with humanitarian principles of neutrality and impartiality.
- ✔ Programme cycle management systems that require systematic needs assessments and robust post-distribution monitoring.
- ✔ Anti-corruption procedures that focus on preventing fraud, theft and waste, including the diversion of aid and funds.
- ✔ Internal vetting of staff, contractors and implementing partner organisations with World Response contracts of more than $X against applicable terrorism lists.
- ✔ Mandatory internal requirements to report suspicious transactions involving criminal groups, which would include individuals and groups engaged in acts of terrorism.

Duty of care

World Response is committed to providing clear, relevant guidance and support to staff and partners at all levels on how to best manage and implement programmes and operations in relation to counterterrorism measures.

Vetting

World Response will vet potential partners, contractors, and vendors above a certain threshold, and candidates for employment and employed staff above a specific grade.

In accordance with the humanitarian principles of impartiality and independence, World Response will not vet beneficiaries, nor will it require partners to do so.

Allegations of misconduct

World Response staff who become aware of information suggests that World Response assets might have been used to promote or facilitate terrorism must immediately report such information to XXX in accordance with the relevant policy.

3. IMPLEMENTATION AND COMPLIANCE

World Response's director and board have overall responsibility for ensuring the organisation manages risk appropriately and activities are undertaken in accordance with World Response's policies and procedures.

4. RELATED DOCUMENTS

- ✔ Standard operating procedure: vetting
- ✔ Data protection policy
- ✔ Logistics handbook
- ✔ Financial handbook
- ✔ Policy on engagement with NSAGs

EXAMPLE NSAG ENGAGEMENT POLICY CONSIDERING COUNTERTERRORISM RISKS

TOOL 8

1. PURPOSE AND BACKGROUND

World Response may engage with non-state armed groups (NSAGs) in the course of its operations in order to provide protection and assistance to those in need, regardless of where they are located. This may involve engaging with groups or individuals that have been designated as terrorist by states or international organisations, such as the UN Security Council and the EU. Any engagement with NSAGs should be in accordance with international humanitarian law (IHL) and consistent with the humanitarian principles of humanity, impartiality, neutrality and independence. In its engagement with NSAGs, World Response must comply with relevant counterterrorism measures. This engagement policy is complemented by World Response's counterterrorism policy.

This policy is intended to set out the main principles that enable World Response to engage NSAGs in accordance with its mandate, while complying with relevant legal frameworks. It is also intended to provide guidance to staff who carry out this engagement.

2. MAIN PRINCIPLES

Purpose of engagement

The purpose of engagement with NSAGs in general is to allow World Response to carry out its mandate, which may require the organisation to engage with any party to an armed conflict. In each context, World Response will identify and clarify the specific goal and scope of engaging NSAGs in that context and will develop a tailored and context-specific engagement strategy to provide guidance to staff.

Context-specific engagement guidance and counterterrorism measures

World Response will provide staff with guidance on NSAG engagement tailored to the objectives of its operations in each relevant context. The guidance will identify counterterrorism measures relevant to the specific context, including sanctions, criminal law measures and donor requirements. XXX will be responsible for developing the guidance. The guidance should be approved by XXX.

Engagement strategies will include:

- ✔ Identification of who approves the engagement and whether there are any red lines, including identification of the circumstances under which the engagement would be terminated.
- ✔ Identification of suitable entry points for engagement.
- ✔ Identification of points of leverage for engagement and incentives for compliance.
- ✔ Identification of who undertakes the engagement, including whether such engagement should be carried out by local intermediaries, e.g. local community leaders.
- ✔ Guidance on prioritisation of resources in the context of engagement, including in terms of the level of engagement and how such engagement will be sustained.
- ✔ Guidance on the level of confidentiality of the engagement process and balancing such confidentiality with transparency about the engagement process and its objectives.
- ✔ Identification of the risks of this engagement for staff and for the organisation, including due to the possible reaction of the host state, and identification of risk-mitigation measures.

Sanctions

Identify whether any of the individuals or groups to be engaged under a national or international sanctions regime.

- ✔ If no, is there a likelihood or risk that a group may become listed or start to cooperate with a listed group?
- ✔ If yes, identify whether the sanction regimes in place prohibit the engagement or the purpose of the engagement, e.g. the delivery of humanitarian assistance.
- ✔ If yes, identify if there are any exemptions or licenses that could be used. If so, identify if this would lead to delays.

Donor regulations

- ✔ Identify if donor agreements for this context prohibit engagement with NSAGs for the purpose of the delivery of humanitarian assistance to areas controlled by NSAGs or if they require particular due diligence steps.
- ✔ If such assistance is prohibited, identify whether it is possible to negotiate with the donor.

Criminal law measures

- ✔ Identify whether staff are at risk of criminal liability under the law of the host state, the states of nationality of the staff, or a third state. Appropriate legal advice should be sought for this step.
- ✔ Identify risk-mitigation measures.

Legitimacy

As an impartial humanitarian organisation, World Response is aware that engaging with NSAGs may be perceived as providing legitimacy to NSAGs. World Response reaffirms that engagement with NSAGs for humanitarian purposes does not affect the legal status of NSAGs in accordance with IHL, in particular Common Article 3 to the Geneva Conventions. In addition, such engagement does not constitute an unlawful interference into the internal affairs of a state. World Response has the following policies to mitigate the risk of providing legitimacy to NSAGs through its engagements with them:

- ✔ Code of conduct for staff
- ✔ Counterterrorism policy

PARTNERSHIP ASSESSMENT CHECKLIST

TOOL 9

INTRODUCTION

This partnership assessment checklist can be used at the country level when considering potential new partnerships, particularly partnerships with an organisation that you have never previously worked with. By encouraging the rating of various elements under each area, and the formalised documentation of each element, the checklist provides a starting point for an organisational assessment and due diligence. The relevance of each element included in the checklist will vary according to your specific situation, needs and the context. It is recommended to use this checklist as a template, adapting it as necessary to ensure adequate focus on the most important aspects related to your specific proposed partnership.

Ⓐ BASIC DATA

Full name of the organisation and abbreviation:	
Assessment carried out by:	
Address and e-mail of contact person:	
Date of assessment:	
Sources of verification: (meeting, document review, other)	
Existing partnership with this organisation?	
If yes, when did cooperation with this organisation start?	

RESET

B SUGGESTED PREREQUISITES WHEN SELECTING NEW PARTNER ORGANISATIONS

Prerequisites	Yes	Comments
The organisation is legally registered in the country	☐	
The organisation has a Management Board	☐	
The organisation produces an annual audited financial statement	☐	
The organisation and its senior management have been screened against counterterrorism lists and you confirm there is no match	☐	

C BACKGROUND AND GOVERNANCE

Type of organisation (NGO, government, research institution, other)	
Year it was founded	
Date of last assessment (for existing partner organisations)	
Date of last external evaluation carried out on this organisation and by whom (for potential new partner organisations)	

Organisational Structure	
Are there organisational by-laws?	☐ YES ☐ NO
Is there a stated mission and vision?	☐ YES ☐ NO
Does the organisation have a constituency/membership base?	☐ YES ☐ NO
Is there an organisational structure/chart?	☐ YES ☐ NO
Board functions	
Are regular board meetings held?	☐ YES ☐ NO
Is documentation from meetings/minutes available?	☐ YES ☐ NO
Are the agenda items relevant to the work of the board?	☐ YES ☐ NO

Your assessment	☐ Weak ☐ Fair ☐ Strong
Comments	

RESET

Ⓓ EXTERNAL ENGAGEMENT AND INFLUENCE

Networks and coordination	
Is the organisation involved in networking with other NGOs, humanitarian organisations or networks?	☐ YES ☐ NO
Does the organisation coordinate its work with other NGOs (local, national, international)?	☐ YES ☐ NO
Is there visible community participation, and does the organisation directly interact with beneficiaries?	☐ YES ☐ NO
Government interaction	
Does the organisation coordinate with the government/authorities?	☐ YES ☐ NO
Does the organisation engage in public processes?	☐ YES ☐ NO
Information and advocacy	
Does the organisation produce information materials regularly?	☐ YES ☐ NO
Does the organisation hold public events for fundraising or other purposes?	☐ YES ☐ NO
Does the organisation work through the media?	☐ YES ☐ NO
Does the organisation use advocacy as a foundation of its work?	☐ YES ☐ NO
Does the organisation perform any lobbying activities?	☐ YES ☐ NO
Counterterrorism policies and procedures	
Does the organisation have and follow counterterrorism policies and procedures that enable it to comply with donor requirements, such as systematic vetting of its implementing partners and suppliers against recognised lists of terrorists?	☐ YES ☐ NO

What influence does the organisation have?	
Who has influence over the organisation?	
Can the potential partner negatively affect your organisation's credibility and legitimacy? What and how significant are the risk factors? How important could the partnership be for your organisation? If criticism has been raised, how has the organisation addressed this?	

Your assessment	☐ Weak ☐ Fair ☐ Strong
Comments	

RESET

E PROGRAMMATIC CAPACITY

What is the mission statement of the organisation?	
What are the target group(s)/ beneficiaries of the organisation?	
What is the geographical focus of the organisation?	
What is the programmatic focus of the organisation?	

Does the organisation:		
Uphold and abide by the humanitarian principles?	☐ YES	☐ NO
Support the provision of impartial assistance solely based on needs?	☐ YES	☐ NO
Operate independently without the imposition of a political agenda?	☐ YES	☐ NO
Uphold a do-no-harm approach?	☐ YES	☐ NO
Have a long-term plan/strategy in place?	☐ YES	☐ NO
Have a framework for Accountability to Affected Populations?	☐ YES	☐ NO
Have a Code of Conduct?	☐ YES	☐ NO
Have policies and procedures to prevent sexual exploitation and abuse?	☐ YES	☐ NO

Your assessment	☐ Weak	☐ Fair	☐ Strong
Comments			

RESET

F OPERATIONAL CAPACITY

Where does the organisation work in the country and what is its in-country structure and field presence?	
How many staff members work in the country office/programme?	
Are the main operational functions adequately staffed and resourced (finance, logistics, M&E)?	
What is the organisation's in-country management structure?	

Does the organisation have:	
An adequate filing system?	☐ YES ☐ NO
Personnel guidelines?	☐ YES ☐ NO
Administrative guidelines?	☐ YES ☐ NO
Security procedures?	☐ YES ☐ NO
A documented risk register and a risk management process?	☐ YES ☐ NO

Your assessment	☐ Weak ☐ Fair ☐ Strong

Comments

RESET

FINANCIAL CAPACITY

What donors are currently supporting the organisation's programmatic activities?	
What is the current overall budget for the organisation's activities?	

Accounting system	
Is there a detailed accounting manual?	☐ YES ☐ NO
Does the organisation have the necessary software for accounting?	☐ YES ☐ NO
Are the financial documents properly maintained?	☐ YES ☐ NO
Are costs booked in the accounts in a timely manner?	☐ YES ☐ NO
Can the organisation provide periodic financial reports at the project level?	☐ YES ☐ NO
Financial control	
Does the organisation have its own bank account registered in its own name?	☐ YES ☐ NO
Is the external audit carried out in a timely manner?	☐ YES ☐ NO
Does the organisation comply with audit requirements?	☐ YES ☐ NO
Are the financial records accurate?	☐ YES ☐ NO
Cost effectiveness	
Is the organisation cost conscious/are alternatives considered to minimise costs?	☐ YES ☐ NO
Are quotations or invoices collected before purchases are made?	☐ YES ☐ NO

Your assessment	☐ Weak ☐ Fair ☐ Strong
Comments	

RESET

H LOGISTICAL CAPACITY

What are the organisation's logistics procedures, and which written logistics regulations exist?	
Describe the logistical setup of the organisation.	

Procurement	
Does the organisation have clear procurement regulations?	☐ YES ☐ NO
Does the organisation have a clear policy for segregation of duties and delegation of authority in the procurement process?	☐ YES ☐ NO
Does the organisation have a procurement plan?	☐ YES ☐ NO
Does the organisation have a procurement tracking and reporting system?	☐ YES ☐ NO
Does the organisation maintain a supplier database?	☐ YES ☐ NO
Asset and warehouse management	
Does the organisation have an asset database?	☐ YES ☐ NO
Does the organisation have routines for handing over, write-off, sales and disposals of assets?	☐ YES ☐ NO
Does the organisation have procedures for managing stocks and warehouses?	☐ YES ☐ NO
Drivers and vehicles	
Does the organisation have a maintenance program for its vehicles?	☐ YES ☐ NO
Does the organisation have a driving security and safety policy?	☐ YES ☐ NO
Does the organisation have a driver training program?	☐ YES ☐ NO

Your assessment	☐ Weak ☐ Fair ☐ Strong
Comments	

RESET

OVERALL RATING /SUMMARY	WEAK	FAIR	STRONG
Background and governance	☐	☐	☐
External engagement and influence	☐	☐	☐
Programmatic capacity	☐	☐	☐
Operational capacity	☐	☐	☐
Financial capacity	☐	☐	☐
Logistical capacity	☐	☐	☐

RECOMMENDATIONS BASED ON THE ASSESSMENT	
PLACE/DATE/SIGNATURE OF PERSON WHO CARRIED OUT THE ASSESSMENT:	

RESET

M&E MINIMUM STANDARDS

TOOL 10

INTRODUCTION

Programme teams in access-constrained contexts will often struggle with data quality when measuring results. Two principle data quality concerns in these contexts include data validity and data integrity. Your measurements may be invalid (i.e. available sources of evidence do not represent what you are intending to measure) due to constraints to sources of evidence or your data collection methods. You may also have data integrity concerns as data flows and information management processes are vulnerable to manipulation given the distances involved, staff capacity, security challenges, and other factors. These data quality concerns limit your organisation's ability to confirm deliverables, improve programmes and measure the change your organisation may have contributed to.

They also exacerbate three risks for your organisation:

1. **Reputational/operational:** your organisation's reputation, and its ability to raise funds, negotiate access and advocate, will be undermined if programmes are not delivering value to beneficiaries;

2. **Financial:** your organisation may not have the documentation necessary to meet donor requirements, which could lead to disallowed costs;

3. **Do no harm:** programmes could put beneficiaries or staff at risk, increase tensions in communities or do harm in other ways.

Your organisation's staff responsible for programming in access-constrained contexts can use creative methods and sources of evidence to mitigate threats to data quality. The M&E minimum standards is a tool to measure if these efforts are likely to be successful when applied to output indicators. The results allow your organisation to measure confidence in the monitoring data, particularly in areas where direct access is often impossible.

M&E MINIMUM STANDARDS – DOMAINS

The M&E minimum standards divides remote monitoring activities and methods into six domains. The domains complement and compensate for each other. If activities in one domain are impossible, more effort in another may compensate. The six domains are:

❶ **Triangulation:** Multiple sources of evidence on the same indicator can be used together to give more confidence to any findings. This may include process data such as waybills, goods-received notes or workflow documentation. In many instances, it includes mixing research methods to pose the same question to different people and groups in different ways. For example, your survey about latrine use may be triangulated with a focus group discussion and photos of the latrines. Triangulation mitigates both integrity and validity threats.

❷ **Data chain of custody:** How your teams in the field capture and transmit data to project management staff can reduce or increase data-quality vulnerabilities. Mobile data capture can ensure that data is digitally captured, with time, date and location stamped, and tagged with the identity of the person collecting and transmitted it directly and immediately to a secure server. This reduces the opportunity for mistakes or manipulation when data is entered, aggregated, and reported and provides an opportunity for you to conduct data audits and spot-checks. This data can include surveys, distribution documentation, photos, attendance reports and other monitoring processes. Efforts in this domain mitigate data integrity threats.

❸ **Population-based surveys and sampling methodologies:** Outcome monitoring processes return to the recipients of assistance to learn how they made use of your organisation's support. Using commonly accepted statistical methods to establish robust sample sizes and methods for including individuals in the sample will ensure that these processes reflect objective reality rather than the opinion of key individuals. The correct use of these methods mitigates data validity and integrity threats.

❹ **Beneficiary initiated feedback:** Where feedback handling mechanisms exist and function, they provide a robust accountability control for your organisation's programmes. These channels may include email, SMS, WhatsApp, phone calls, and/or complaint boxes. An important element of a feedback system is ensuring that beneficiaries understand their entitlement. Feedback systems that exist on paper, but have not resulted in registered feedback, do not offer your programme teams the same confidence. A functioning feedback handling mechanism mitigates validity and integrity threats by serving as an alternative source of evidence and a deterrent to manipulation.

❺ **Independence:** Having an independent look at implementation is highly desirable, but very challenging in a remote-management context. In many contexts, your organisation's senior staff and your donors can provide an independent verification of results with ad hoc visits and spot-checks. However, in areas that are difficult to access, this can be quite challenging or even impossible. You could consider contracting local third-party monitoring firms or other 'independent' monitors; however, these monitors must negotiate their access through the same constraints as your organisation and often rely on the same pool of last-mile staff, and the independence of these external monitors cannot be assumed. Independent data collection mitigates data integrity threats.

❻ **Documented direct contact with beneficiaries:** Direct contact with beneficiaries may be documented at the moment of handover or service deliver and again during an outcome monitoring process. In some challenging contexts, your distributions may occur quickly and without documentation; or your local partners may engage with beneficiaries but provide only summary reports to your organisation. Your organisation's ability to review the primary data documenting beneficiary engagement mitigates data integrity threats.

SCORING THE M&E MINIMUM STANDARDS

The questions in the table below evaluate an activity against the six domains of the M&E minimum standards and provides a score. The score gives your management a measure of the confidence they can have in the reported output results.

Instructions:

Facilitation by your organisation's M&E staff or another group external to the implementation team, if possible, can promote a more reflective and independent assessment. Fill the tool at the activity level. Consider related output and outcome indicators together as one monitoring process. Fill the tool for each different implementation modality. For example, if a food distribution is conducted house-to-house in one location and at a centralised distribution point in another location, fill the tool for each modality. Give each question a 'yes' or 'no'. A 'yes' is awarded only when the method is available or implemented three-quarters of the time or more. Partial points are not possible.

In some cases, the six domains look at different aspects of the same monitoring activity. For example, outcome monitoring may contribute to triangulation, direct contact with beneficiaries and population-based surveys. However, in some contexts an outcome monitoring process may only achieve points in one or two of these domains. For example, if your outcome monitoring relies on direct observation, there may not be points for population-based surveys or documented direct contact with beneficiaries.

When you calculate the score before implementation, you should consider concrete plans and commitments to move forward. The results can inform a programme criticality decision, where your management decides if a programme can move forward or not. The results will also become part of the programme documentation to share with donors, internal management and others.

When the score is calculated after implementation, your team should review the primary data supporting each domain. The score is the measure of confidence your organisation can have that the programme existed. This is an important metric for future audits. Comparing the before and after scores will improve how your teams use the tool in the future.

Minimum Score:

A suggested minimum score is 57 for life-saving programming and 84 for other types of programming. Your teams should go beyond the minimum whenever the context allows.

M&E MINIMUM STANDARDS

META data	
Date the tool was completed	
Country	
Sector and activity	
Location	
Completed before or after implementation?	

RESET

Remote monitoring approach domain	Value	Explanation	Response (Yes)
Documented direct contact with beneficiaries	**20**		
Is evidence of outputs documented at the point of delivery or handover to the beneficiary?	13	This is the primary source of verification for the relevant output indicator profile. The objective here is to capture the transaction of providing the good or service. For distributions, this is signed beneficiary lists. For services delivered to groups, it could be signed attendance lists or photos showing all attendees receiving the service.	☐
Is there documented direct contact with beneficiaries providing evidence of outcomes?	7	This is the primary source of verification for the relevant outcome indicator profile. Most often it will be a population-based outcome survey. However, it may also be key-informant interviews with only a few beneficiaries.	☐
Documented direct contact with beneficiaries:		**Section score:**	
Triangulation	**20**		
Are two independent sources of evidence of the activity available?	12	Registration documentation, distribution photos, post-distribution monitoring (PDM) data, etc. For sources of evidence to be independent of each other, they must have very distinct methods (e.g. photos and registration) or be separated in time (e.g. PDM and registration). A registration and exit interviews conducted at the time of distribution would not be independent. Sources of evidence must demonstrate the scale and the nature of the assistance. For a distribution of 1,000 food baskets, photos would need to show 1,000 people receiving the basket and some images of the basket contents, a registration document would need 1,000 names and the content of the basket, etc.	☐
Are three independent sources of evidence available?	8		☐
Triangulation:		**Section score:**	

RESET

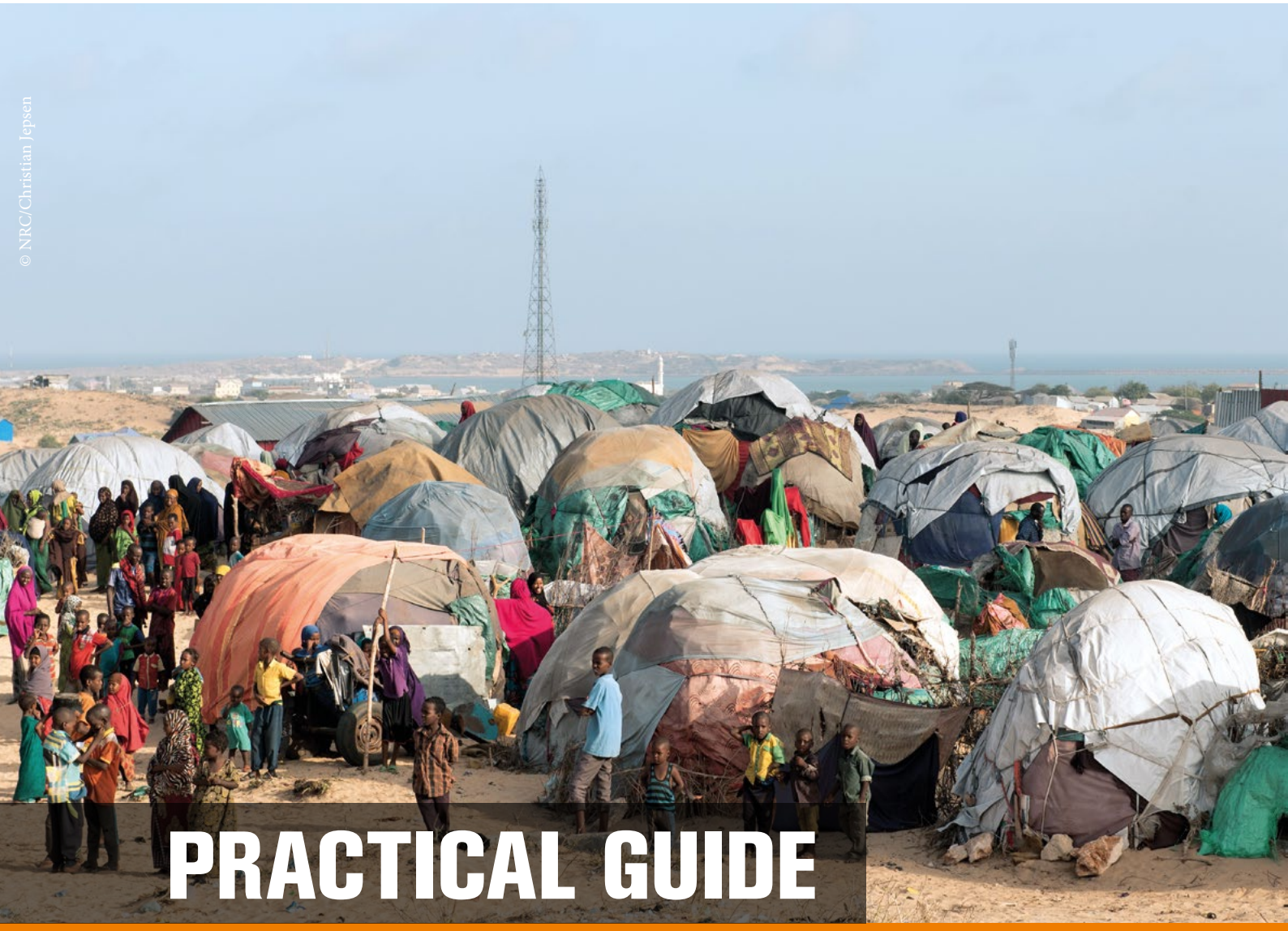
Remote monitoring approach domain	Value	Explanation	Response (Yes)
Data chain of custody	20		
Is the data transmitted from the field to the project management team via a mobile data capture platform or deposited directly into a file sharing application controlled by your organisation?	2	The objective is for the data to be transmitted from your field team to the project management team via a secure method as early in the data processing flow as possible.	☐
Is the data entered into a mobile data capture platform at the point of capture?	14	The point of capture is the interview, the observation, when the photo is taken, etc.	☐
Data chain of custody:		**Section score:**	
Population-based surveys and sampling	**20**		
Is the confidence interval 5 or less and the confidence level 95% or greater?	6		☐
Is the confidence interval 5 or less and the confidence level 90% or greater?	6		☐
Are those in the sample randomly selected with an approved randomisation method?	8	Consult internal sampling guidance or external resources and tools.	☐
Population-based surveys and sampling:		**Section score:**	
Beneficiary initiated feedback	**20**		
Are all beneficiaries informed of their entitlement from this specific activity?	7	This may be with posters, radio announcements, or other communication.	☐
Is there one independent feedback channel?	2	This may be WhatsApp, SMS, calling, complaint boxes, etc. Beneficiaries reaching out to the implementation team with feedback does not count as a channel for this exercise.	☐

RESET

Remote monitoring approach domain	Value	Explanation	Response (Yes)
Are there two independent feedback channels?	3	This may be WhatsApp, SMS, calling, complaint boxes, etc. Beneficiaries reaching out to the implementation team with feedback does not count as a channel for this exercise.	☐
Does your organisation have a history of receiving feedback from beneficiaries of that partner/team in that location?	8	Has one actionable piece of feedback been formally submitted to your organisation relating to work done by your team in this location?	☐
Beneficiary initiated feedback:		**Section score:**	
Independence	**70**		
Do certain senior managers visit the project location unannounced and at will?	25	'At will' means that access does not require special permissions or approval and that physical access is not overly onerous (e.g. driving less than four hours from a major airport). Senior staff should be those based outside the implementation area.	☐
Do any senior managers visit the project location unannounced and at will?	25	Are visas or access permission only available for certain individuals? If so, then this is a no.	☐
Do junior or locally based staff visit the project location unannounced and at will?	3		☐
Is the data collected by staff who are not on the implementation team? This may be another team, another partner or a contracted monitoring party.	3	Was there a segregation of duties for the M&E data collection so that one team did the implementation and another team collected the data?	☐
Is the data collected without the involvement of local authorities or the implementation team in the field?	14	Remote management often means that last-mile enumerators must negotiate access through the same gatekeepers as the implementation team or have the implementation team introduce them to beneficiaries. This is a 'yes' only if the data collection is truly independent of local authorities and implementers.	☐
Independence:		**Section score:**	
Total score:			

RESET

NRC NORWEGIAN REFUGEE COUNCIL



PRACTICAL GUIDE

PROJECT CYCLE MANAGEMENT AND COUNTERTERRORISM RISKS

This practical guide draws on content from NRC's 'Toolkit for principled humanitarian action: managing counterterrorism risks'. It outlines the origin and impact of counterterrorism measures and proposes actions for humanitarian organisations to consider throughout the programme cycle to help manage and mitigate counterterrorism-related risks.


© NRC/Emad Badwan, 2014.

WHERE DO COUNTERTERRORISM MEASURES COME FROM?

Counterterrorism measures are introduced through:

❶ UNSC resolutions and other international instruments

❷ Regulations introduced by regional bodies such as the European Union (EU)

❸ States' domestic laws

Once introduced, these measures are often reflected in donor grant agreements. These measures include a variety of approaches, including designating groups or individuals as terrorist, and criminalising the provision of financial and other types of support to those designated as terrorist, or those 'associated with terrorism'.

WHY ARE THESE MEASURES RELEVANT FOR HUMANITARIAN ORGANISATIONS?

Humanitarian organisations often operate in conflict-affected environments in which counterterrorism measures may apply; for example, where one or more parties to a conflict is a designated terrorist group (DTG). In accordance with international humanitarian law and the humanitarian principles, organisations should make decisions regarding where to operate based on assessments of needs. Engaging with DTGs may be necessary to secure access to people in need of assistance. Counterterrorism measures may impede organisations' ability to engage with these groups, and may result in penalties being imposed on organisations that do.

WHAT ARE THE RISKS FOR HUMANITARIAN ORGANISATIONS?

Risk Category	Operational Impact
Criminal	**Prosecution over the provision of support to DTGs:** The broad definition of support for terrorism that some states have adopted makes this a risk for humanitarian organisations and staff who carry out certain activities. **Criminalisation of staff:** Criminal laws designed to counter terrorism have the potential to criminalise humanitarian workers. Local staff members may be particularly exposed to risks under the host country's counterterrorism legislation.
Security	**Insecurity:** Engaging with non-state armed groups (NSAGs), regardless of whether or not they are DTGs, is a key element of gaining and maintaining secure access to people in need. Engagement also helps to establish consent and acceptance for humanitarian organisations' activities, which is vital to ensure staff safety. Counterterrorism measures can create uncertainty for organisations about whether contact with NSAGs that are also DTGs is permissible.
Contractual	**Delay:** The inclusion of counterterrorism clauses in grant agreements can delay the implementation of humanitarian initiatives while organisations work with donors to try to negotiate changes or seek clarity about vague wording. Some requirements, including screening and/or vetting procedures, may also delay the provision of assistance. Delays can also occur as a result of bank derisking, which happens when banks refuse, or take longer than expected to provide transfers to locations perceived as high risk, in order to minimise their own exposure to accusations of facilitating terrorist financing. **Lower quality of response:** Compliance with donor counterterrorism requirements may reduce the quality of an organisation's response by causing it to choose modalities perceived as lower risk even if they are less appropriate and effective for a particular context. **Risk transfer to staff:** Counterterrorism-related wording in grant agreements can be vague and difficult to interpret. It is not uncommon for humanitarian organisations to accept these clauses without fully understanding the requirements involved. Staff tasked with implementing a project under a grant agreement may have had no involvement in negotiating it, but they shoulder the burden of complying with the requirements. **Risk transfer to local partners:** International NGOs (INGOs) often pass on donor counterterrorism requirements to local partners in the form of "flow-down clauses" without ensuring they understand what signing the clause entails, or that they have the resources and capacity to comply. Local partners may accept requirements that are impossible for them to adhere to or that endanger their staff as a result. **Establishing a precedent:** This can occur when one organisation accepts a counterterrorism clause that others deem unacceptable. Some organisations may choose to negotiate more favourable terms, but their leverage and ability to do so is weakened if others have already accepted the requirements. **Loss of funding:** Some organisations have refused donor funding as a result of uncertainty about, or unwillingness to accept the terms of counterterrorism measures required of them. Expenditure may also be disallowed under a contract if an organisation does not comply with all donor regulations.
Humanitarian principles	**Compromised principles:** In order to minimise exposure to counterterrorism risks, organisations may choose not to provide assistance in areas controlled by NSAGs that are also DTGs, regardless of the humanitarian needs there. This compromises the impartiality and needs-based nature of their response and leaves affected populations without the assistance they need simply because of their location. If an organisation is not perceived as impartial, its acceptance by NSAGs and local communities may be impacted. This can limit access and put staff safety at risk.


© NRC/Tuva Raanes Bogsnes

HOW CAN HUMANITARIAN ORGANISATIONS MITIGATE THESE RISKS?

Humanitarian organisations can mitigate these risks by ensuring they have the following in place:

- A risk management framework
- An established process for reviewing counterterrorism clauses in grant agreements and clear red lines outlining the language and conditions that are not acceptable
- Internal policies providing staff with guidance on counterterrorism measures and on engagement with NSAGs that may be DTGs, including red lines to ensure adherence to the humanitarian principles
- Project cycle management (PCM) guidelines that consider counterterrorism risks

PCM guidelines that consider counterterrorism risks can help ensure that organisations identify, evaluate and mitigate these risks effectively during the program cycle. The PCM guidelines below are designed to help humanitarian organisations approach project design and implementation in a principled way in contexts where counterterrorism measures may pose challenges to principled humanitarian action.

Note that risk management cannot eliminate counterterrorism risks; it can only reduce the likelihood of occurrence and mitigate against potential impacts. Organisations should identify and take reasonable actions to manage risks, and after having done so, decide if the remaining 'residual' risks are acceptable or not. This decision should be based on a program criticality assessment, which weighs the residual risks against the severity of needs and the expected humanitarian results.

PROJECT CYCLE MANAGEMENT FOR COUNTERTERRORISM RISKS

PHASE ONE: PROGRAMMING

Main programme activities at this point might include:

- Determination of overall programme strategy
- Development of context analysis
- Development of risk analysis

Phase one checklist

Context analysis and stakeholder mapping:

- Does your organisation have a risk management framework in place? Are staff aware of the components relevant to their roles, such as policies related to counterterrorism measures and engagement with NSAGs, sanctions, counterterrorism legal frameworks your organisation may be required to comply with, and donor conditions related to counterterrorism that it may have already committed to?
- Have you carried out a context analysis for your country of operation, including an updated stakeholder mapping?
- Have you filled in a context-specific risk register to identify and evaluate operational risks related to counterterrorism, including risks to your organisation's ability to adhere to the humanitarian principles and the principle of "do no harm"? Have you identified options for mitigating these risks? A risk register template can be found here

PHASE TWO: IDENTIFICATION

Main programme activities at this point might include:

- Identification and verification of needs, target areas and beneficiary groups
- Identification of funding opportunities
- Development of project log frame
- Decision on whether to proceed with development of proposal

Phase two checklist

Targeting:

- Refer back to the context analysis and risk register from phase one and update according to the proposed programme and target area.
- Identification of current risks: Is your choice of modality or target area, or your beneficiary targeting influenced by counterterrorism measures? If yes, revisit your decisions to ensure they are in line with a principled approach and adhere to your organisation's red lines.
- Does your stakeholder mapping reveal the presence of groups in the target area who are designated as terrorist or sanctioned by your potential donor(s) and/or the host state? If so, how will you ensure you are able to engage with them in a principled way?
- Identification of mitigation measures: Define different options available.

Funding:

- Donor conditions related to counterterrorism are not always known in advance of responding to a call for proposals, but it is important to consider them as early as possible.
  - If you are considering a funding opportunity from a new donor, have you reviewed the standard grant agreement carefully for counterterrorism requirements?
  - Existing donors can change counterterrorism requirements without notifying partners. Have you reviewed the specific grant agreement before signing

RISKS RELATED TO DONOR COUNTERTERRORISM CONDITIONS:

Donors have different approaches to counterterrorism clauses in grant agreements – some do not include specific language on counterterrorism, but will include language addressing the need to prevent diversion, fraud and corruption. Others include strict requirements specifically related to counterterrorism. An example is USAID's Anti-Terrorist Certification (ATC), which must be signed by grantees and states to certify that, 'The Recipient, to the best of its current knowledge, did not provide, within the previous ten years, and will take all reasonable steps to ensure that it does not and will not knowingly provide, material support or resources to any individual or entity that commits, attempts to commit, advocates, facilitates, or participates in terrorist acts, or has committed, attempted to commit, facilitated, or participated in terrorist acts'.

The risks associated with signing this certification became clear in 2018, when USAID claimed that because the INGO Norwegian People's Aid (NPA) provided 'training and expert advice or assistance' to DTGs in the course of programmes in Iran and Gaza, its certification to USAID that it did not knowingly provide material support or resources to any prohibited parties was false.

NPA contested these claims, stating that it had not provided support to 'terrorism', and that it did not receive USAID funding in Gaza or Iran. NPA had signed an ATC to accept USAID funding in South Sudan. USAID argued that, once signed, the ATC applied globally to any projects that USAID grantees implemented, anywhere in the world, irrespective of the donor. This interpretation indicated that USAID had significant influence over projects funded by other donors. Although NPA disagreed on the fairness of USAID's claims, due to the estimated costs, resources and time necessary to take this case to trial, NPA concluded that the most reasonable option was to agree on a settlement. NPA agreed to pay US$2.025 million to the U.S. Government.

PHASE THREE: FORMULATION

Main programme activities at this point might include:

- Development of project proposal and budget
- Development of an M&E matrix and assessment of M&E quality
- Decision on whether to proceed, taking donor conditions and programme criticality into account

Phase three checklist

Proposal planning and development:

- Does your proposal take the previously identified risks related to counterterrorism into account?
- Have you included all potential counterterrorism-related risks and mitigation measures in your risk register and risk matrix?
- Do you intend to work with local partners? If yes:
  - Have you talked to your potential partner about counterterrorism-related risks?
  - Have you considered the possibility that you may transfer risks to the local partner, and how you can share them rather than passing them on?
  - Have you assessed the local partner's capacity to manage risks and comply with contractual requirements related to counterterrorism?

Review of donor contract:

- Have you identified a counterterrorism clause in your donor contract? If so, does it prevent or impede a principled humanitarian approach? Has a legal adviser reviewed the clause? See Annex 1: "Reviewing counterterrorism clauses" for more guidance.
- Decide whether to proceed with the funding opportunity.

M&E assessment:

- Taking the risks identified in your register into account, assess whether you will be able to achieve minimum M&E standards.
- Assess the quality of your M&E processes to establish how successful they are likely to be in mitigating the risk of diversion and, in the case of it occurring, identifying where.
- Share the results of your assessment with your potential donor if necessary, to ensure they are aware of the M&E quality expected.

Program criticality decision making:

- Depending on the counterterrorism risks and mitigation measures identified in your risk register and the quality of your M&E processes, you may need to take a decision based on programme criticality.
  - Have you weighed the severity of needs and the expected humanitarian results of the project against the risks associated with achieving that objective? This type of assessment can be done using a tool such as the UN's programme criticality assessment. The resulting decision should be documented and followed through careful monitoring of project implementation and changes in the operating environment.

PHASE FOUR: IMPLEMENTATION

Main programme activities at this point might include:

- Development of work plan
- Grant opening meeting
- Monitoring
- Progress review

Phase four checklist

Grant opening meeting:

- Have you confirmed that the project team is aware of counterterrorism-related risks and mitigation measures identified in the risk register and matrix?
- Have you confirmed that staff are aware of any counterterrorism-related compliance requirements imposed by the donor?
- Have you confirmed that the project team understands your organisation's red lines in terms of the humanitarian principles?

Periodic project review:

- Have you evaluated the current situation against the risks previously identified? Have any of the risks materialised and if so, what have their impacts on the project been?
- Do you need to revise or update the risk register to reflect unforeseen challenges related to counterterrorism or changes in the operating environment?
- Do any changes in the operating environment related to counterterrorism require you to inform or consult internal and external stakeholders, including donors?
- Have you crossed any of your organisation's red lines in relation to counterterrorism and principled humanitarian action? If so, document how these decisions were made and monitor and record their impact on your project, and any wider impacts in terms of reputation and staff security.
- If your donor has imposed counterterrorism-related compliance requirements, have these impeded project implementation, including adherence to the humanitarian principles?

© NRC/ Enayatullah Azad

PHASE FIVE: EVALUATION AND AUDIT

Main programme activities at this point might include:

- Grant closure meeting
- Internal reporting
- Reporting to donors

Phase five checklist

Grant closure meeting:

- Have you systematically reviewed challenges related to counterterrorism, including those related to access and adherence to the humanitarian principles, and the decisions made to deal with these challenges?
- Have you documented the impact counterterrorism measures may have had on project implementation, and any wider impacts in terms of your organisation's reputation and staff security?
- Have you documented and reported challenges and decisions to internal stakeholders?
- Have you ensured these are filed together with all other documentation related to the project for audit purposes?
- Have you identified lessons learned to inform the development and implementation of future projects?

RISKS RELATED TO INDIRECT SUPPORT TO A DTG:

Humanitarian organisation Global Solidarity works in Area X, which is controlled by local authorities who have strong links with a group designated as terrorist by the UNSC. Owing to security considerations, operations in Area X are managed remotely. Global Solidarity undertook a tendering process for the provision of water trucking for Area X. After the bid process, which the remote management team administered, one of the bidders alleged that contractors had to pay 3 per cent of the contract value to the local authorities in order to obtain approval to operate in Area X. Global Solidarity's staff in Area X confirmed that this was accurate. None of the detailed bids for any of Global Solidarity's previous projects had included any mention of this fee. These fees crossed Global Solidarity's red line in relation to facilitation payments, and potentially posed a counterterrorism risk, owing to the relationship between the local authorities and the DTG. The remote management team immediately suspended new contract signings until the matter could be fully investigated. A report was handed over to Global Solidarity's regional anti-corruption adviser, who launched an internal investigation. Associated donors were informed and external legal advice was sought.

Global Solidarity engaged with the United Nations Office for the Coordination of Humanitarian Affairs (OCHA), requesting that they intercede to obtain a waiver from local authorities exempting all humanitarian organisations from these fees to ensure programs could continue. The waiver was successfully obtained.

Global Solidarity engaged the donor that funded the water trucking project in discussions on risk sharing. The donor agreed that there was no fault on Global Solidarity's side and commended the organisation for its transparency on the issue. However, the donor still chose to classify the costs as non-reimbursable and therefore subject to repayment.

This incident reflects the obstacles faced in providing aid in environments where local authorities and DTGs may be linked, and the additional challenges related to managing operations remotely. Coordination and collaboration can bring about solutions when these issues arise, but ultimately the burden of risk is borne entirely by humanitarian organisations, reflecting the importance of anticipating and planning for these kinds of challenges before they arise.

Note: This case study describes actual events but has been anonymised.

PCM guidelines like those above form one component of a risk management framework that can help an organisation to identify, evaluate and mitigate potential counterterrorism-related risks effectively throughout the different PCM phases. By mainstreaming consideration of these risks, organisations can ensure they are better prepared to deal with them when they arise. Consult NRC's 'Toolkit for principled humanitarian action: managing counterterrorism risks' for more information.

ANNEX 1: REVIEWING COUNTERTERRORISM CLAUSES

It is vital organisations review each grant agreement thoroughly before signing to ensure they are aware of what they are agreeing to, regardless of whether they have signed previous agreements with the same donor or not. Donors are not obliged to inform partners when they change the wording of counterterrorism clauses or introduce new clauses. These clauses are not always found in the sections of grant agreements where they might be expected. A compl ete review, which might include searching the agreement for relevant terms, helps to ensure that any problematic language is identified in time to seek clarity from the donor or try to renegotiate wording.

Questions to consider

The following checklist is not exhaustive:

- Does the agreement refer to international conventions or treaties, UNSC resolutions, donor policies, domestic or international laws or donor state regulations?
- Does the counterterrorism clause include the terms “intent”, “knowledge”, “knowingly” or “reasonableness”?
- Does the clause include language that is vague or unclear, such as “associated with” or “directly or indirectly”?
- Would the recipient be required to vet or screen staff, partners or beneficiaries against lists of DTGs?
- Does the agreement include specific requirements or language on the recruitment of staff?
- Does the counterterrorism clause oblige the recipient to incorporate the same clause in sub-agreements?
- Would complying with the agreement impede the recipient’s ability to adhere to the humanitarian principles?
- Would complying with the counterterrorism clause affect the recipient’s acceptance among affected populations and parties to the conflict?
- Would the recipient be unable to give staff and partner organisations clear instructions about how to comply with the obligations?

If any answer to the questions above is "yes"

❶ Clarify the obligations and terms of the partnership agreement

- Consult internally with senior management, policy advisers, legal personnel and others.
- Consult an external legal adviser for an interpretation of the clause.
- Based on this information, consider developing a note to file outlining an internal interpretation of the clause.
- Consult other organisations that receive funds from the same donor or partner.
- Ask the donor or partner for their own interpretation of the clause, the degree of liability inferred and the obligations to ensure compliance.

❷ Negotiate the terms of the agreement

As a result of the above consultations, the organisation may choose to negotiate terms of the partnership agreement. This decision should be agreed by senior management, policy advisers, legal personnel and other relevant departments.

- Identify areas of potential conflict between the terms of the agreement and the organisation's policies, operational capacity and humanitarian principles.
- Establish a position on which terms of the agreement are acceptable or unacceptable.
- Clarify the above position with the donor or partner.
- Share existing or planned risk management policies and practices.

If the answer to any of the initial questions is still "yes" after negotiation, the organisation's management will have to assess the risks and liability involved for the organisation itself, its potential partners and sub-contractors and other humanitarian organisations before deciding whether or not to sign the agreement.

6 RISK LIBRARY

International Council of Voluntary Agencies (ICVA), *Risk and Humanitarian Culture: An ICVA Briefing Paper*, 2020, https://bit.ly/3cuvCH9

Christian Aid, *The Grand Bargain and the issue of Risk Management*, 2019, https://bit.ly/2MuQioa

Human Security Collective, *Derisking and Civil Society: Drivers, Impact and Solutions*, 2019, https://bit.ly/2AAVRyv

International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts – Recommitting to Protection in Armed Conflict*, 2019, https://bit.ly/2Mvguip

InterAction, and Humanitarian Outcomes, *NGOs & Risk: Managing Uncertainty in Local-International Partnerships*, 2019, https://bit.ly/3eLgWoP

InterAction, *Resources on NGO Risk Management*, 2019, https://bit.ly/3cwlq0U

The Cash Learning Partnership (CaLP), *Cash and Voucher Assistance and Risk in Financial Management and Compliance Briefing Note*, 2019, https://bit.ly/2yZm0Xg

The New Humanitarian, *The creeping criminalisation of humanitarian aid*, 2019, https://bit.ly/2U3DJUX

U4 Anti-Corruption, and Transparency International, *Managing corruption challenges in humanitarian settings*, 2019, https://bit.ly/3gYS1Ab

Humanitarian Policy Group (HPG) and Overseas Development Institute (ODI), *Counter-terrorism, bank de-risking and humanitarian response: a path forward*, 2018, https://bit.ly/2Mtap62

HPG, and ODI, *The impact of bank de-risking on the humanitarian response to the Syrian crisis*, 2018, https://bit.ly/2U6Ei00

Norwegian Refugee Council (NRC), *Principles under Pressure: the impact of counterterrorism measures and preventing/countering violent extremism on principled humanitarian action*, 2018, https://bit.ly/3cwWc2r

Médecins Sans Frontières (MSF), *Bridging the Emergency Gap*, 2018, https://bit.ly/2U6ErR6

NRC and United Nations Office for Coordination of Humanitarian Affairs (OCHA), *Presence and Proximity - To Stay and Deliver, Five Years On*, 2017, https://bit.ly/2XWZuHe

Charity and Security Network, *Financial Access for US Non-Profits*. 2017, https://bit.ly/30e0aue

Chatham House, *Recommendations for Reducing Tensions in the Interplay Between Sanctions, Counterterrorism Measures and Humanitarian Action*, 2017, https://bit.ly/3f0JBGH

Harvard Law School Program on International law and Armed Conflict (HLS PILAC), *Pilot empirical survey study on the impact of counterterrorism measures on humanitarian action*, 2017, https://bit.ly/2U7dop5

MSF, *Perilous terrain. Humanitarian action at risk in Mali*, 2017, https://bit.ly/2MvihUF

Geneva Call, 2016 *In their words: Perceptions of armed non-state actors on humanitarian action*, 2016, https://bit.ly/3cqADkc

Global Public Policy Institute (GPPi), and Humanitarian Outcomes, *The effects of insecurity on humanitarian coverage*, 2016, https://bit.ly/2Y2ITSj

HLS PILAC, *Understanding humanitarian exemptions: U.N Security Council Sanctions and Principled Humanitarian Action*, 2016, https://bit.ly/305sFu7

Humanitarian Outcomes, and InterAction, *NGOs and Risk: How international humanitarian actors manage uncertainty*, 2016, https://bit.ly/2U3Gndl

Humanitarian Outcomes, and InterAction, *Residual Risk Acceptance: An advocacy guidance note*, 2016, https://bit.ly/3cyseLE

Humanitarian Outcomes, *What It Takes: Principled pragmatism to enable access and quality humanitarian aid in insecure environment*, 2016, https://bit.ly/2Ubh4pA

Humanitarian Outcomes, ODI and Humanitarian Practice Network (HPN), *Tug of War: Ethical decision-making to enable humanitarian access in high-risk environments*, 2016, https://bit.ly/2Ay1ttn

Humanitarian Outcomes, and InterAction, *NGO Risk Management: Principles and Promising Practice*, 2016, https://bit.ly/2MshYtB

HLS PILAC, *Suppressing Foreign terrorist fighters and supporting principled humanitarian action*, 2015, https://bit.ly/2Azritc

NRC, *Risk Management Toolkit: In relation to counterterrorism measures*, 2015, https://bit.ly/2XX26F2

Humanitarian Outcomes, *Secure Access in Volatile Environments*, 2014-2016, https://bit.ly/2yZq1uO

Harvard Law School, *An Analysis of Contemporary Counterterrorism-related Clauses in Humanitarian Grant and Partnership Agreement Contracts*, 2014, https://bit.ly/3eLlj3d

MSF, *Where is everyone? Responding to emergencies in the most difficult places*, 2014, https://bit.ly/2z2h6ZL

HPG, and ODI, *Paradoxes of presence: Risk management and aid culture in challenging environments*, 2013, https://bit.ly/3gOgZlH

NRC, and OCHA, *Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action*, 2013, https://bit.ly/2XYo7Dp

Humanitarian Policy and Conflict Research (HPCR), *Humanitarian Action under Scrutiny: Criminalizing Humanitarian Engagement*, 2011, https://bit.ly/2AC7u8w

OCHA, *To Stay and Deliver*, 2011, https://bit.ly/2zZYSIL

Global NPO Coalition on Financial Action Task Force (FATF), *Report Collection*, http://fatfplatform.org/reports-3/

NRC NORWEGIAN REFUGEE COUNCIL

TOOLKIT
FOR PRINCIPLED HUMANITARIAN ACTION

MANAGING COUNTERTERRORISM RISKS