Anti-terrorism and anti-money laundering policy

Document manager: Corporate Controller
Document name: Anti-terrorism and anti-money laundering policy
Approved by Board of Directors date: 28 November 2024
Version 2.1 27 November 2024

Contents

1. Objective.

Cordaid is firmly committed to preventing any use of its funds—directly or indirectly—for terrorist activities. The organization also ensures that its resources are not used to launder the proceeds of crime. Cordaid understands that when funds are diverted to terrorist groups or used for criminal acts, it undermines the intended projects and harms the most vulnerable individuals and communities.

Additionally, Cordaid is dedicated to preventing terrorists from exploiting its organization, staff, or infrastructure for their activities.

Furthermore, any suggestion that an NGO is connected to terrorism or money laundering can severely damage its reputation and erode the trust and support of beneficiaries, partners, the public, and donors.

This policy's goal is to safeguard Cordaid from funding terrorism, violating sanctions, or becoming a conduit for money laundering and terrorist activities.

2. Scope

This policy applies to all staff members and consultants at Cordaid's Global and Country Offices. Additionally, all implementing partners, donors, and suppliers are required to adhere to the measures aimed at preventing the misuse of the organization and its assets, including any activities related to terrorism, the financing of terrorism, or money laundering.

Although we operate in high-risk areas for terrorism, Cordaid collaborates closely with local partner organizations, most of whom we have known for a long time. We believe that this approach significantly reduces the risk of our funds unintentionally reaching those who would misuse them for unlawful purposes. Nevertheless, we recognize the serious implications of any proven or alleged terrorist funding and the potential abuse of our organization by terrorists. Therefore, we are committed to addressing these risks effectively. Cordaid has introduced measures in its selection process for staff, consultants, volunteers, partner organisations, suppliers, and donors to further minimize associated risks.

The legal framework in the Netherlands for preventing the funding of terrorism and money laundering is primarily governed by the "Wet ter voorkoming van witwassen en financieren van terrorisme" (Wwft), which translates to the "Law on the Prevention of Money Laundering and Financing of Terrorism." Although the Wwft may not directly apply to Cordaid, the organisation must comply with its regulations indirectly through financial transactions with banks and interactions with chartered accountants. Additionally, the "Sanctions Act 1977" outlines the requirements for compliance with international sanctions and imposes obligations on organisations to prevent activities that could violate these sanctions.

On the EU level, INGOs operating in EU countries are also subject to the EU Anti-Money Laundering Directives (AMLDs)[1] , establishing common rules and standards for preventing money laundering and terrorist financing across member states.

[1] EU Anti-Money Laundering and Countering Financing of Terrorism Legislation, available at: https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en#legislation

Internationally, UN Security Council resolutions impose sanctions on individuals, groups, or entities involved in terrorist activities or financing, and INGOs must comply with these sanctions and avoid any involvement with sanctioned entities.[2]

3. Dissemination

The Anti-Terrorism and Anti-Money Laundering Policy is publicly accessible on both Cordaid's external website and its internal intranet. All updates will be shared with Cordaid staff, partners, donors, and consultants through the Cordaid Intranet or the International Website. Key components of the policy are included in the primary process descriptions that form part of the onboarding program for all new staff members.

Additionally, the Anti-Terrorism and Anti-Money Laundering Policy is referenced in all legal agreements with partner organizations, donors, consultants, and suppliers, along with a link to the entire document.

4. Related policies, process descriptions, procedures and tools

This policy should be read in connection with the following Cordaid policies, process descriptions, procedures and tools:

Policies:

- Integrity Policy (part of the Integrity Framework)
- Fraud Policy
- Cordaid Code of Conduct
- Procurement policy (part of Procurement manual)
- Partner Alliance policy
- Risk Management policy
- Data Protection Policy

Process descriptions:

- Integrity Framework
- Project Based Working: Identification, Inception, Implementation and Completion process
- Procurement manual
- Safe recruitment guideline

Tools:

- Partner capacity and risk assessment (PCRA)
- Third Party Check (currently World Check One)

[2] UN Security Council Resolution 2462 (2019), available at: https://documents.un.org/doc/undoc/gen/n19/090/16/pdf/n1909016.pdf?token=p06G5C5SwBuxEgV1Ce&fe=true

5. Definitions

A terrorist is defined as an individual or group that uses **violence, intimidation, or threats** to create fear, often with the intent to achieve a political, ideological, or religious objective. Terrorism typically involves **deliberate acts** intended to cause harm or disrupt society, targeting civilians or non-combatants to influence a government, organisation, or population.

A terrorist organisation is a group or collective entity that systematically engages in **terrorism**. These organisations operate through planned, coordinated acts of violence to instil fear, coerce governments, or influence a population or specific groups to achieve their desired goals.

A **terrorist act** is any intentional act of violence, intimidation, or threat designed to cause fear, harm, or disruption, typically to achieve a political, ideological, or religious objective. These acts are deliberately carried out to target non-combatants or civilians and are intended to influence governments, organizations, or populations by creating a sense of fear or insecurity.

Key characteristics of a terrorist act include:

1. **Use of violence or threat:** This can involve physical attacks (e.g., bombings, shootings, or kidnappings) or threats to cause harm to individuals, groups, or property.
2. **Deliberate targeting of civilians or non-combatants:** The primary goal is to instill fear or disrupt the normal functioning of society, rather than combat between armed forces.
3. **Political, ideological, or religious motivation (in Combination with Violence)**: Such acts are driven by specific objectives, including political change, ideological promotion, or religious agendas, but must involve the use or threat of violence to qualify as terrorism. Non-violent advocacy or action does not fall under this category.
4. **Instilling fear and coercing change:** The intent is to create widespread panic and force governments, organizations, or individuals to comply with demands or to change their policies.

Examples of terrorist acts include suicide bombings, mass shootings, hijackings, attacks on infrastructure, and cyberterrorism. These acts often have a far-reaching impact, both in terms of human casualties and in terms of economic, social, and political consequences.

Money laundering is the process by which the proceeds of crime are channelled through financial systems to disguise their illegal origin.

6. Prevention

Cordaid has the following measures in place to reduce the risk of accidentally and deliberately funding terrorism or being used for terrorist activities and /or money laundering:

Pre-employment screening (PES). Following current HR screening regulations and procedures, Cordaid checks the names of all individuals with whom it intends to enter into an employment contract or any other form of cooperation against national and international sanctions and terrorist lists beforehand.

Due Diligence on partners, suppliers and donors: Cordaid has established a partner alliance policy and procurement policy that outlines the limitations on the types of organisations with which we collaborate. For new partner organisations, a partner capacity and risk assessment (PCRA) is performed, indicating the different risks of working together with this partner (unless the Decision Tree in the PCRA grants an exemption based on the existence of another form of partner assessment that delivers similar due diligence). Before entering into any business cooperation, contract, or other relationship with a partner, supplier, or donor, Cordaid requires a thorough check for their presence on national and international sanctions and terrorist lists, as well as any criminal records. This verification is conducted using World Check One (WCO). If the WCO check indicates potential risks related to terrorism or money laundering, further investigation will be carried out. Cooperation with the organization will only be considered if this additional research provides sufficient guarantees.

Code of Conduct Cordaid has a Code of Conduct that applies to both its staff and contract partners. All staff members and contract partners are required to sign the Code of Conduct when they join the organization or enter into a contract with Cordaid. This Code explicitly emphasizes the obligation of staff and contract partners to help prevent unethical and criminal activities.

Audit Committee: Cordaid's Audit Committee, a part of the Supervisory Board, supports the Supervisory Board in meeting its responsibilities by independently reviewing financial statements and assessing the effectiveness of our internal controls. This committee also monitors the performance of both external and internal audit functions. Additionally, it assists the Supervisory Board in determining the nature and extent of the risks it is willing to accept in order to achieve its strategic objectives.

Policies and procedures: Cordaid has implemented an Integrated Management System for risk management, quality management, and internal control, based in part on the COSO Integrated Framework for Internal Control and the Three Lines of Defense principle. This system outlines Cordaid's key processes along with the necessary policies and procedures, including finance, procurement, administration, and asset management guidelines. These procedures apply across the entire organization and must be followed by all staff in Cordaid's country offices and the Global Office.

Third-party check: The Quality Management department uses World Check One (WCO) to carry out the necessary checks on the presence of persons on sanctions and terrorist lists.

Segregation of duties: Key financial process responsibilities are divided among several employees instead of being assigned to one individual. Multiple signatures and/or system workflow approvals are required at different stages of any financial transaction process to prevent unauthorized transactions.

"Three lines of defense"-internal control system: Cordaid has implemented an internal control system based on the "three lines of defense" principle. A key aspect of this model is the first line of defense, which consists of processes and procedures—including management controls—in our primary operations. The second line of defense offers support and advice to line management staff and the Board. Finally, the third line of defense provides independent assurance.

Budget management: Budget versus actual expenditure reports are prepared and reviewed with senior management monthly for each project and organizational unit. Every three months, a comprehensive consolidated report is shared with the Supervisory Board. Budgets are maintained in the accounting system.

Proper books and records : Cordaid utilizes a multi-currency accounting system that effectively tracks income and expenditures, specifically linked to projects, funding sources, and external third parties. Each income and expenditure entry is associated with donor or source codes, ensuring that all program

expenditures are connected to specific projects and partner codes. Additionally, Cordaid retains all supporting documentation, including receipts, invoices, and other relevant documents, in compliance with legislative requirements**.**

Cash and Bank management: Controls include regular cash counts and monthly bank reconciliations, authorisation levels for financial operations, segregation of duties, and required signatures or system approvals. Additionally, cheques must be signed by two individuals, and all bank transfers require dual signatures.

7. Detection

Annual external audit and external project audits: Cordaid conducts an annual external audit of its financial statements, and around 60% of all projects undergo external audits. The external auditors pay special attention to any transactions that raise suspicions of funding terrorism or money laundering. In accordance with the Wwft regulations, these transactions must be reported to the authorities and further investigated by the auditors.

Banking system: Cordaid transfers 95% of its funds through Dutch and international banks, which are subject to the Wwft (Dutch) as well as the sanction regulations of the UN and the European Union. As a result, all of Cordaid's transfers undergo screening, and any transfers to high-risk countries require explicit verification, including detailed information about the purpose and destination of the transfer. If the documentation is insufficient, banks will not approve the transfers. Additionally, Dutch banks are obligated to notify tax authorities about any suspicious transactions that may be related to money laundering.

8. Monitoring & reporting

Any incidents of potential criminal activity identified within Cordaid, whether detected proactively or retroactively, will be reported to the appropriate officer based on the nature of the issue. This may include the Anti-Corruption and Anti-Fraud Officer (ACAFO), the Integrity and Safeguarding Officer (ISO), or the Global Security Advisor (GSA).

Suspicion of terrorism financing and/or money laundering will be addressed by the ACAFO, following the same procedures as suspected fraud. This includes the application of any relevant sanctions. Please refer to paragraph 7 of Cordaid’s Anti-Fraud Policy for further details.

9. Responsibilities & Non-Compliance

The Board of Directors owns and approves this Anti-terrorism and Anti-money Laundering Policy. The Corporate Controller is responsible for keeping the procedure up to date and must review the policy at least once a year. The departments of Quality Management & Compliance, Institutional Fundraising &

Donor Relations, Corporate Finance, and Internal Audit will be consulted when updating the policy. All staff members will be informed of any updates to the policy through Cordaid's Intranet.

Non-compliance with this policy may result in disciplinary measures, including but not limited to termination of collaboration or employment contracts, and may also lead to criminal liability under the applicable laws.