Protecting Your Association
From
Terrorist Financing and Money-Laundering Risks

November 1, 2025

Background

Most incorporated associations (and other nonprofits) in Papua New Guinea do vital work that support families and our communities. These associations are often funded through donations. Whether your association works to provide education, healthcare, other social services, your organisation depends on public trust and the belief that every kina goes to good causes.

Unfortunately, a small number of bad actors sometimes try to use charities and associations to hide the source of illegal funds or to move money for criminal purposes, including the funding of violent extremism. There are no reported cases of PNG charities financing terrorism, but similar incidents have occurred elsewhere in the region. Staying alert helps protect your organisation and the wider sector.

This short guide will first explain how bad actors can misuse associations funds or operations for money laundering or even terrorist financing. The guide then offers straightforward, practical steps you can take—like checking who your donors are and keeping clear records—to keep your organisation safe and trustworthy.

1. How Incorporated Associations can be misused

Incorporated associations (and even unincorporated non-profit organisations) can be misused in multiple ways that can compromise funds and damage reputation. Most of these risks are linked to larger associations that have significant cash flows, but even smaller associations will benefit from being aware of these risks. They include:

- Donated funds can be routed through fake contractors, shell companies, inflated salaries for non-existent staff, or spent on fictional campaigns.
- Legitimate programmes can be used to move cash, goods, or even people under cover of normal charitable operations.

- Complex chains of donations, cross-border transfers, or using virtual assets can hide the origins of the true donors (a concern with large donations).
- The appointment of volunteers or even committee members who have links to groups engaged in political violence or holding extremist views can help an association undertake these risky actions.

2. Warning signs in your day-to-day operations

This is a short list of "red flags" that should cause concern:

- A new or repeat donor who makes large gifts but insists on anonymity or refuses reasonable identity checks.
- Large or frequent donations that do not match the donor's known profile or capacity.
- Donations or other payments being routed through multiple intermediaries or foreign accounts without clear explanation for these unusual pathways.
- Sudden changes in project scope, beneficiaries or spending patterns without clear documentation.
- Requests to award contracts to unfamiliar vendors or to pay large sums to overseas third parties.
- Volunteers or staff who avoid oversight, request unusual financial arrangements, or appear to act on behalf of unknown third parties.

3. Measures to Guard Against Risks

Adopting a risk-based framework helps prevent abuse while preserving operational integrity:

- Verify identity and, where reasonable, the source of funds for single donations or grouped donations above an agreed threshold. [Example threshold: K20,000 for a single donation or K30,000 of aggregate donations in a year. You can adjust the threshold to what is appropriate for your organisation.] If the donor is a corporate entity, then checking the corporate register of its home jurisdiction is a first step in this process.
- Keep an audit trail of donor names and contact details, reasons for donations, receipts, invoices and records of how funds were spent. Keep records for a minimum of 7 years.
- Segregate financial roles inside your association. Make sure no one person can both create, approve and record the same payment. Also, split responsibilities so that more than one person checks and signs off on large transactions. Separating financial roles creates checks and balances, which makes schemes like money laundering or inflated purchase orders harder to execute and easier to detect.
- Conduct periodic assessments of all programs to identify any gaps what was promised and what was delivered. If a program's outputs or costs diverge from plans, investigate and document the reasons.

- Strengthen internal governance with clear conflict-of-interest policies, transparent decision-making, and independent audits.
- Open a dedicated account for your association and do not co-mingle funds from other sources in that account. Use a licenced financial institution for your (banks and most credit unions) for your association's accounts.
- Train staff and volunteers to recognise red flags and to follow reporting and escalation steps inside the organisation.

4. What to do if you suspect misuse

- Do not confront suspected donors or staff directly in ways that could alert wrongdoers.
- Preserve records and any relevant emails, contracts or bank statements.
- Escalate the matter to your board or compliance committee. You may need to seek legal or regulatory advice
- Where required by law or internal policy, file a suspicious matter report with FASU or notify your bank and the IPA as appropriate.

5. Next steps

You should review your current policies against the risks and protection measures outlined above. You may need to do things like:

A. Review your donor intake procedures and set practical thresholds for identity and source-of-funds checks.

B. Put in place basic segregation of duties for financial transactions.

C. Schedule staff and volunteer training sessions on red flags, record keeping and any new policy changes taken as a result of this guide.

D. For larger associations, consider establishing a small compliance or oversight committee to oversee new policies and any reported red flags.