ROTARIANS AGAINST MALARIA
PAPUA NEW GUINEA

Anti-Fraud Policy

Version 3.0

Feb 2025

David Guinn
Tim Freeman
Munir Ahmed
Gordon Loga
Carlos Palma

Table of Contents

Glossary

HR	**Human Resources**
IP	**Implementing Partners**
M&E	**Monitoring and Evaluation**
NGO	**Non-Governmental Organisation**
PNG	**Papua New Guinea**
PR	**Principal Recipient**
RAM	**Rotarians Against Malaria**
SR	**Sub-Recipient**

I. Introduction

This document describes the processes, procedures and team activities that are necessary to assure a robust anti-fraud policy within RAM (as the PR) and their Implementing Partners (IP). This includes the appointment of a Fraud Investigation Team to prevent, detect, respond to and deter fraud within the organisation.

Fraud and Corruption are a threat to any Organization and can potentially impede RAM's mission to effectively prevent and treat malaria across PNG. The strength of RAM is contained in its values, of which ethics and integrity are integral. Fraud can only be managed by following clear processes and policies that are in place to assure the ethical values of integrity, duty of care, accountability, dignity and respect are treated with the utmost importance. RAM recognizes that next to this, fraud and corruption (risks) needs to be properly addressed.

The purpose of this Anti-Fraud policy to combat fraud and corruption is:

- To state RAM's commitment to prevent, detect and respond to fraud and corruption
- To establish definitions of 'prohibited practices', which RAM shall apply and enforce in all RAM's activities

II. Definition of Fraud (Internal & External)

RAM considers fraud to be any act or omission that intentionally misleads, or attempts to mislead, a person to obtain a financial or other benefit or to avoid an obligation. Corrupt practices are generally understood as the offering, giving or receiving anything of value to influence improperly the actions of another person.

For the purpose of this document, Internal Fraud should be considered any purposeful action that leads to the personal gain (monetary or otherwise) of RAM employees while conducting their activities on behalf of the project, even if it does not ultimately lead to a financial or material loss to the project, though this loss is normally assumed, or the loss is diverted into another's profit.

External Fraud can be defined as the risk of unexpected financial, material or reputational loss as the result of fraudulent action of persons external to the Principal Recipient. This may therefore include fraudulent activity committed by the Implementing Partners, criminal gang networks, corrupt law enforcement, government bodies and individual members of the public. Whilst the above-mentioned consequences of fraudulent activities may be similar, external fraud is more likely to result in potential or realized reputation damage to the principal recipient, implementing partners and or the donor organizations.

Corrupt practices can be generally understood as the offering, giving or receiving anything of value to influence improperly the actions of another person. Something of value does not necessarily include pecuniary value but may include other incentives such as social favors or favors returned at later times.

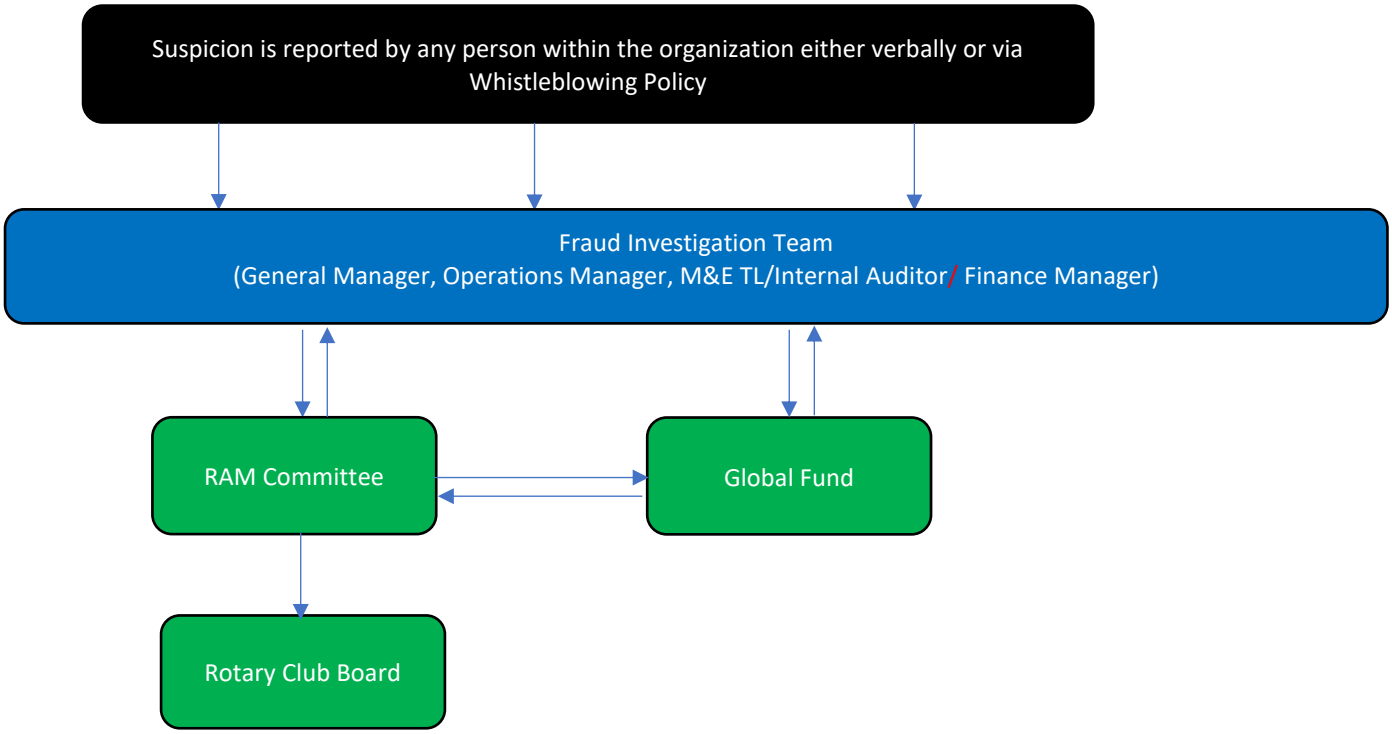
Such Internal or External fraud may include the following examples but is not restricted to the examples given:

- Awarding contracts based on personal friendships, favors or financial rewards.
- Using project funds for other purposes than specified.
- Claiming payments for activities not carried out including forgery of signatures.
- Overstating payments so receiver does not receive the full amount which is invoiced.
- Theft of funds, assets or property.
- Improper use of assets, funds or property.
- Giving any misleading information regarding project funds and project activities which may lead to loss of efficiency.
- Receiving payments more than once for the same activity carried out.
- Any purposeful action that leads to the loss of funds through either direct loss of money or actions that ultimately make the project less efficient i.e. improper use of project vehicles leading to delays in operations and consequent loss of funds.
- Undeclared Conflicts of Interest resulting in undeclared advantages. Any (potential) Conflict of Interest needs to be immediately declared to the HR department and the direct manager.
- Deliberate sabotage of company assets and business activity i.e. deliberately introducing a computer virus to the organization shared IT Network.
- Misuse of the organizations IT Network i.e. sharing of unauthorized sensitive propriety information or the distribution of inappropriate or illegal material resulting in reputational or criminal damage.
- Using the organizations IT Network for personal gain.
- Theft from other employees or Implementing Partners.
- Giving or receiving bribes or facilitation payments
- Making political donations
- Collaborating with external parties to engage in fraud

III. Zero Tolerance

RAM takes a zero-tolerance approach towards all fraudulent practices. RAM will respond firmly to such instances with appropriate and adequate measures that could include disciplinary actions, recovery of funds, termination, and referrals to civil or criminal authorities. RAM's Code of Conduct stipulates Zero Tolerance which is signed off and acknowledged by all employees when joining the organization and with every renewal of the contract on an annual basis.

IV. Governance Structure



Any person within the organisation of the PR and IP is responsible to alert the Fraud Investigation Team when he or she suspects any fraudulent activities happening, verbally, either via e-mail or via the Whistleblowing Policy (as described in VII.). The Fraud Investigation Team will first decide if adequate suspicion exists to warrant further investigation. When adequate suspicion exists, the Fraud Investigation Team will then check if the suspected fraud has indeed happened (and later via a thorough investigation, proven). If the Fraud Investigation Team suspects fraud, they will immediately inform the Chairman and the Global Fund in an official communication consisting of a formal incident report. The Chairman will inform the Rotary Club Committee. Both the Fraud Investigation Team and the Chairman will keep the Global Fund informed on the progress of the investigation.

The RAM Chairman, General Manager, Operations Manager and Finance Manager can appoint the Internal Auditor or the M&E Team to do (part of) the investigation. This will only be possible if there is no one within the M&E Team involved in the fraud case. If someone from the M&E team or RAM senior management team (General Manager, Operations Manager, and Finance Manager) is suspected in any fraud case, then a special investigation team will be formed by the RAM committee.

V. Fraud Risk Management Framework (Preventive)

A robust Risk Management framework is an essential element in meeting corporate responsibilities of transparency and accountability. Developing such a framework includes but is not limited to the following:

1. Identifying areas of high risk – this is the first step in dealing with the problem and is required prior to any further analysis and assessment can be taken. It is important to understand that risk identification is not limited to financial risk e.g. while a physical attack against an employee in the field to steal project funds resulting in death can result in a high financial loss, further reputational damage to the entire project could potentially shut it down.
2. Assess the Risks – Once an organization has identified its own risk areas, a fraud risk assessment covering all relevant areas of operation can provide the platform for a framework and strategy for a sustainable, long-term monitoring and review process.
3. Involve all Staff – Ensure all staff have the potential to identify possible fraud risk as also trained during the Moral Compass Training described in chapter VIII.
4. Continuously assess the risks of fraud within the organization – The Chairman, General Manager, Operations Manager and Finance Manager will continuously identify and improve the areas of high risk.
5. Common Risk Areas – Areas of fraud risk vary from industry to industry and from organization to organization. However, six areas of risk apply to most organizations:
   i) Purchasing, payroll and HR
   ii) Sales and fixed assets
   iii) Cash and Cheques
   iv) Physical Security
   v) Piracy, intellectual property, and confidential information
   vi) Intellectual technology/information system

RAM will ensure procedural manuals are developed for each of the above six areas. RAM has already developed HR, Fixed Asset and Procurement manuals, remaining manuals will be developed over time.

VI. General Fraud Policy Statement and Compliance

Both PR and IPs are to be committed in conducting the work with the utmost integrity and transparency. To maintain these standards and to fulfill the legal and ethical responsibility as "stewards" of our donors' and investors' funds, the PR and IPs need to be relentless in the efforts to combat fraud.

Every person from the PR and IP is accountable for the prevention, detection, and reporting of fraud, theft, forgery, misappropriation, bribery, corruption, or other suspicious or unethical activity within the person's area of responsibility.
RAM Management will be responsible for implementing the proper response to reports of fraud or other suspicious activity, including working closely with the RAM M&E department to conduct investigations, and timely reporting to the Global Fund in accordance with applicable legal and contractual requirements.

This policy applies to any incident or suspicion of fraud, theft, forgery, misappropriation, bribery, corruption, other irregular activity, involving employees as well as consultants, vendors, contractors, grantees, sub-contractors and sub-recipients, program partners, and other organizations engaged in business or programs with RAM.

VII. Whistle-blowing Policy

The Whistle-blowing Policy is there to give any person within the organization the ability to send a (fraud) alert via a third party. By blowing the whistle on misconduct in an organization or with a specific third party/contractor, one alerts the organization to the fact that its stakeholders are being wrongfully put at risk or have been, or are being, harmed.

The PR's duty is to manage the funds responsibly, including proactively protecting those funds from abuse or misdirection so that they can reach their intended destinations for their intended purposes. Intentional mismanagement or misappropriation of funds is a serious breach of trust for two obvious reasons:

- The intended beneficiaries – namely, those affected by malaria – would be harmed as funds earmarked for their benefit are diverted and not used for their benefit
- Donors cannot be expected to continue donating funds that are managed irresponsibly or wasted

The PR and IPs are committed to safeguard whistle-blowers and provide the opportunity to treat all whistle-blowing reports as either confidential or anonymous. The choice between confidential or anonymous whistleblowing is that of the whistle-blower alone. With anonymous whistleblowing it is essential that all details (and supporting documentation) are shared during the first contact as it won't be possible to come back to this person and ask questions. When the whistle blower decides to do this anonymously, he or she will need to use a third-party phone or block the number.

The whistle-blower is always protected even if the disclosed information turns out to be misguided or false. In the case of internal whistle-blowers, where it is considered necessary, the PR may recommend the temporary reassignment of a person who has allegedly been the subject of retaliation or other measures appropriate to protect against further acts of retaliation. Any such recommendation will only be submitted with the approval of the staff member involved and appropriate measures will be taken to fully safeguard employee confidentiality possible.

Given the propensity of violent retaliation (pay back) within PNG society physical protection may be required for the whistle-blower and their family members should it be judged necessary.

Reporting under this policy in no way protects a whistle-blower from sanctions arising from their own wrongdoing. On other words, blowing the whistle is no "escape hatch" for complicity in misconduct.

Fraud or abuse can be reported to the Chairman, Project Manager and Finance Manager:

- Chairman: +675 76861013 (Rio Fiocco)
- General Manager: +675 71612093 (Munir Ahmed)
- Operations Manager: +675 79965704 (Lindsay Nisan
- Finance Manager: +675 79965703 (Mamta Aswal)

Details needed for the report:

- Type of alleged wrongdoing
- Where and when did these events occur
- Who are the people involved and who has knowledge about the matters reported?
- How the individual, organization or company committed the alleged wrongdoing
- Why the conduct should be investigated and why the matter is being reported
- All documents and references to other sources that support the complaint

What happens after the report is made:

- Initial screening resulting in a determination of the most appropriate action
- If decided to pursue, an investigation is started and/or in the event of a breach of national criminal laws, the national authorities for prosecution will be involved. If the matter is criminal in nature staff will be hesitant to act if Police are involved as the Police will demand to know where the allegation originated from. This needs to be managed carefully as information provided to the Police can sometimes be easily tracked back to the source who may be trying to act anonymously for fear of "pay back".

VIII. Fraud Awareness & Prevention Training (Moral Compass etc)

Fraud Awareness and Prevention Training is an integral step in combatting fraud within Rotary Against Malaria and it's Implementing Partner's. This training is mandatory for all RAM staff, where it is deemed to be appropriate dependent on the staff members' role. Training occurs as part of the induction process and on a regular basis (at least once a year) as a review process. Training also requires ongoing communication updates to all staff when new risks are identified, or a particular fraudulent offence has become prevalent within the organization.

To assure all people working for the PR and IP know and understand exactly what "Fraud" is, there are "Moral Compass trainings" in which the following information is shared and tested:

- What is right and what is wrong: (including below)
    - How to properly manage project fund money and understand where the money is coming from
    - How to properly pay the volunteers
    - How to properly manage the acquittals
    - How to properly arrange taking time off
    - How to not get trapped (bribery) as nothing is for free
- Who/what is affecting us in doing the right thing: (including below)
    - Elders and family
    - Culture and belief
    - Religion
    - Law of the land and Human Rights as defined by the United Nations
    - The employer
- How to assure everyone is doing the right thing and keep their job:
    - Guided by the law of the land and the employer
- Why having a moral compass is important?
    - Many people do not think before they act (as they act subconsciously)

- Don’t assume that things are right because everyone else does it
- Think before you act and think about the consequences of the actions before they happen
- Lessons learned: Test if people really understand what Fraud is

Every member of staff is responsible for:

- Acting with propriety in the use of Company resources and the handling and use of Company funds whether they are involved with cash or payments systems, receipts or dealing with suppliers or customers.

- Being conscious to the possibility that unusual events or transactions could be indicators of fraud

- Reporting details immediately through the appropriate channel, if they suspect that a fraud has been committed or see any suspicious acts or events

- Co-operating fully with whoever is conducting internal checks, reviews, or fraud investigations

IX. Reporting

A person within the PR or IP who becomes aware of, or suspects, that any fraud or other financial misconduct has taken place, regardless of the context and amount involved, must immediately report the information to the RAM Chairman and/or the RAM General Manager or Operations Manager or Finance Manager, unless the whistle-blowing process is being followed. They will then notify the RAM Senior Management Team (SMT). The Fraud Investigation Team will then investigate the potential fraud case and report to both the RAM Chairman and General Manager.

The Chairman and/or RAM General Manager will timely disclose any (suspected) fraud to the Global Fund as required by law or agreement violations involving fraud, theft, forgery, misappropriation, bribery, corruption, or similar activities potentially affecting the funder’s award. Disclosure will be made to the Global Fund regardless of whether they were billed for the losses. These disclosures will be made in accordance with relevant regulations and contractual requirements. RAM may also report cases of fraud to law enforcement authorities, as appropriate.

X. Investigation

Each incident of suspicious activities or suspected fraud will be subject to rigorous, independent review by staff not organizationally associated with the section where the suspected fraud has occurred. Information developed during the review and any resulting reports may be shared among RAM Management and appropriate members of Senior Management overseeing or involved in the activities.

It's imperative to follow set a process when investigating an allegation of fraud. This ensures fairness for the alleged perpetrator and assists in any prosecution that may result. The role of the investigator is to act as an impartial party whose job is to collect facts and report those facts as backed up by the evidence presented. The investigator should not formally present an opinion if it is not supported by the evidence presented.

XI. Confidentiality and Protection Against Retaliation

In order to comply with obligations from PR/IP to the Global Fund and maintain the integrity and fairness of the investigative process, employees should refrain from conducting any investigative activity on their own, such as contacting parties, requesting information from any source, or disclosing allegations to anyone within or outside the PR/IP, other than those identified in this policy. Efforts will be made to treat information received as confidential to the maximum extent possible consistent with the PR/IP's obligations to report and cooperate with donor or government auditors and investigators. The alleged perpetrator is entitled to a fair investigation and should be presumed innocent until proved otherwise. Confidentiality is imperative in this process as it also acts to protect the organisation against possible law suits should the alleged perpetrator be cleared of any wrongdoing.

RAM implements and maintains processes to prevent, detect and respond to any retaliation happening against any people who report a suspicion or have knowledge of Prohibited Practices.

XII. Fraud Response (Plan)

The Fraud Investigation Team is responsible for the investigation, reporting and managing a (potential) fraud case from beginning to end. A Fraud Response Plan is necessary to assure the Anti-Fraud is effective in their investigation and timely action is taken in the event of a fraud. Also, to help minimize losses and increase the chances of a successful investigation. The Plan defines authority levels, responsibilities for action, and reporting lines in the event of a suspected fraud or irregularity. It acts as a checklist of actions and a guide to follow in the event of fraud being suspected. The plan is designed to enable the PR to:

- Prevent further loss
- Establish and secure evidence necessary for criminal, civil and/or disciplinary action
- Determine when to contact the police and establish lines of communication
- Assign responsibility for investigating the incident
- Minimize and recover losses
- Review the reasons for the incident, the measures taken to prevent a recurrence, and determine any action needed to strengthen future responses to fraud

i. Actions following detection

When any member of staff within RAM or any of the IPs suspects that a fraud has occurred, he/she should immediately notify the RAM Chairman or the General Manager. Speed is of the essence and the initial report can be verbal and must be followed up within 24 hours by a written report addressed to the RAM Chairman and the General Manager:

- The amount/value, if established.
- The position regarding recovery.
- The period over which the irregularity occurred, if known.
- The date of discovery and how the suspected fraud was discovered.
- Whether the person responsible has been identified.
- Whether any collusion with others is suspected.
- Details of any actions taken to date.
- Any other information or comments which might be useful.

Before completing the report above, it may be necessary for the General Manager to undertake an initial enquiry to ascertain the facts. This enquiry should be carried out as speedily as possible after suspicion has been aroused: prompt action is essential. The purpose of the initial enquiry is to confirm or negate, as far as possible, the suspicions that have arisen so that, if necessary, disciplinary action including further and more detailed investigation may be initiated.

ii. Investigation / Further Actions

When fraud is suspected, an investigation by the Fraud Investigation Team will take place to:

- Determine the facts
- Consider what, if any, action should be taken against those involved
- Consider what may be done to recover any loss incurred
- Identify any system weakness and look at how internal controls could be improved to prevent a recurrence.

After proper investigation, RAM will take legal and/or disciplinary action in all cases where it is considered appropriate. There will be consistent handling of cases without regard to position or length of service of the perpetrator.

Where an investigation involves a member of staff and it is determined that no criminal act has taken place, the Fraud Investigation Team will liaise with HR and the appropriate line manager to determine which of the following as occurred and therefore whether, under the circumstances, disciplinary action is appropriate:

- Gross misconduct (i.e. acting dishonestly but without criminal intent)
- Negligence or error of judgment was seen to be exercised
- Nothing untoward occurred and therefore there is no case to answer

Where the Fraud Investigation Team judges it cost effective to do so, RAM will normally pursue civil action in order to recover any losses.

Where initial investigations point to the likelihood of a criminal act having taken place, the Fraud Investigation Team will refer the matter to the Royal Papua New Guinea Constabulary. Caution is

necessary when involving the RPNGC and should be done after a carefully considered plan ensuring the safety of all involved is taken into account.

iii. Recovery of Losses

The recovery of losses should be a major objective of any fraud investigation. To this end, the quantification of losses is important. Repayment of losses should be sought in all cases. Where necessary, external advisors can be involved, or legal advice should be sought on the most effective actions to secure recovery of losses.

iv. Protection of Evidence

If the initial examination confirms the suspicion that a fraud has been perpetrated, then to prevent the loss of evidence which may subsequently prove essential for disciplinary action or prosecution, the head of investigation (within the Fraud Investigation Team) should:

- Take steps to ensure that all original evidence is secured as soon as possible
- Be able to account for the security evidence at all times after it has been secured, including keeping a record of its movement and signatures of all persons to whom the evidence has been transferred
- Not alter or amend the evidence in any way
- Keep a note when investigators came into possession of the evidence

v. Learning from Experience

Following completion of the case, the Fraud Investigation Team prepare a summary report on the outcome and lessons learned and circulate it to the Global Fund. The Chairman and General Manager will take the appropriate action to improve controls to mitigate the recurrence of the fraud. Where a fraud has occurred, management will review the system and enhance internal control.