Prescribed Non-Profit Organisation (NPO) Programme Risk Assessment (PRA) Checklist

The activity/project

- Is the activity clearly within the NPO's objectives?
- How much experience does the NPO have in undertaking the activity?
- Are proper policies and procedures in place to prevent or mitigate terrorist financing from occurring directly or indirectly? Do the procedures include preparing a risk appetite statement, risk register, carrying out sanctions screening, training staff, carrying out on-going monitoring and other relevant controls?
- Are volunteers, employees and controllers sufficiently trained in relation to diversion and terrorist financing risks to be able to effectively carry out their work? Have they been vetted (e.g. screened against relevant sanctions lists and proscribed terrorist lists)?
- What lessons has the NPO learnt from its own previous experience, or that of other organisations working in the same area and/or carrying out the same type of activity, which may assist it in avoiding or mitigating terrorist financing risks?

Legal

- Are there any specific laws and requirements to be aware of in carrying out the activity?
- Are there any Jersey, UK and/or local sanctions in force?
    - Do licences need to be obtained from sanctions authorities?
- Are volunteers, employees and controllers required to sign a confirmation that they have read and understood their obligations, including to seek to avoid diversion from occurring?

Finance

- What is the NPO's financial position and is there enough money available to support the proposed activity?
- How will the funds get to the project?
    - Will it be transferred via the formal banking system direct to the recipient?
    - Will Money Service Businesses or other methods falling outside the formal banking system be used?
    - Will cash or other money remittance methods outside of a Jersey bank account be used?
    - Does the method used to get funds to the project represent a change of approach that needs to be notified to the JFSC?

Cyber

- Are the NPO's staff familiar with 'red flags' which might indicate an attempted cyber-attack e.g. a suspicious e-mail might suggest an attempted phishing attack?
- Does the NPO have a backup of any information critical to its operations?
- Is the NPO able to protect the computer and email accounts that it uses by employing strong passwords and multi-factor authentication?
- Have other NPOs undertaking similar activities been the target of cyber-attacks?

Associate NPOs (also known as Partners)

- Are Associate NPOs being used?
- What risks does the use of Associate NPOs pose?
    - Have these Associate NPOs been used before?
    - How have they been identified and what systems and controls do they have in place to prevent or mitigate terrorist financing from occurring?
    - Who are their owners and controllers?
    - What are the risks of the Associate NPO not delivering?
- What controls are in place with the Associate NPOs to mitigate risks?
    - Has a written agreement been put in place with the Associate NPO?
        - Does it include a clear statement that neither party will tolerate diversion, or parties who will facilitate diversion?
        - Does it stipulate what the funds may be used for, under what circumstances, and which beneficiaries the donations may benefit?
        - Does it require the contracting parties to report suspicious transactions and suspected sanctions breaches to the relevant authorities?
        - Does it allow for the contracting parties to end the contractual agreement if diversion occurs?
        - Has a clause been included to accommodate random spot checks?
    - Can funds be recovered if necessary?
    - What other problems might there be?

Significant Donors

- Are donations amounting to £10,000 or above received over a 12-month period, either as a single payment or cumulatively, from the same Donor?
- Are donations amounting to over 50% of total donations received by the prescribed NPO over a 12-month period, either as a single payment or cumulatively, from the same Donor?
- Is the NPO particularly reliant on a particular Donor, to the extent that it would be unable to function if the Donor withdrew their support?
- Is there a suggestion that the NPO is being used as a conduit for funds to a third party that would not align with its objects and may amount to diversion?

Beneficiaries

- 'What' activities are being carried out?
- ‘Why’ is the activity being carried out (the rationale)?
- 'How' are activities going to be delivered and the timescales involved?
- 'Who' will carry them out?
    - Will there be local staff controlled and supervised by the NPO?
- 'Where' will the project be based?
- ‘When’ will the project take place (date of commencement, duration)
- What 'methods' are used to safeguard NPO funds?
- What is the 'public profile' of the proposed work?
- Is the proposed work likely to draw media attention and/or local or public interest?
- Where 'third parties' may be involved, and not just delivery partners, what degree of influence or control does the NPO exert?
- Is the NPO able to carry out adequate monitoring?

General Third Party Risk Considerations

- What due diligence activities should be put in place before commencing the business relationship or carrying out the one-off transaction?
- What is the rationale for the business relationship or one-off transaction, with reference to the overall purpose, activity and capability of the NPO?
- What kind of on-going monitoring of the relationships should be carried out?
    - Is this only appropriate for significant relationships?
- If a third party is charging a fee for their services, is it proportionate to what is being provided?

External Factors

- What factors are outside the NPO's direct control?
- What knowledge does the NPO have about the country or region they are planning to operate in? Is that knowledge sufficient?
- Has the NPO taken into account and documented any relevant circumstances arising in the particular country or region of operation?
- Specific risks could arise from working in an area (or in a jurisdiction bordering an area) where there may be:
    - Internal conflict or other violent or military action
    - Known terrorist or criminal activity
    - Poor infrastructure in remote or sparsely populated areas
    - Instability or frequent changes in the government/political environment
    - Lack of banking facilities
    - High levels of bribery and corruption.