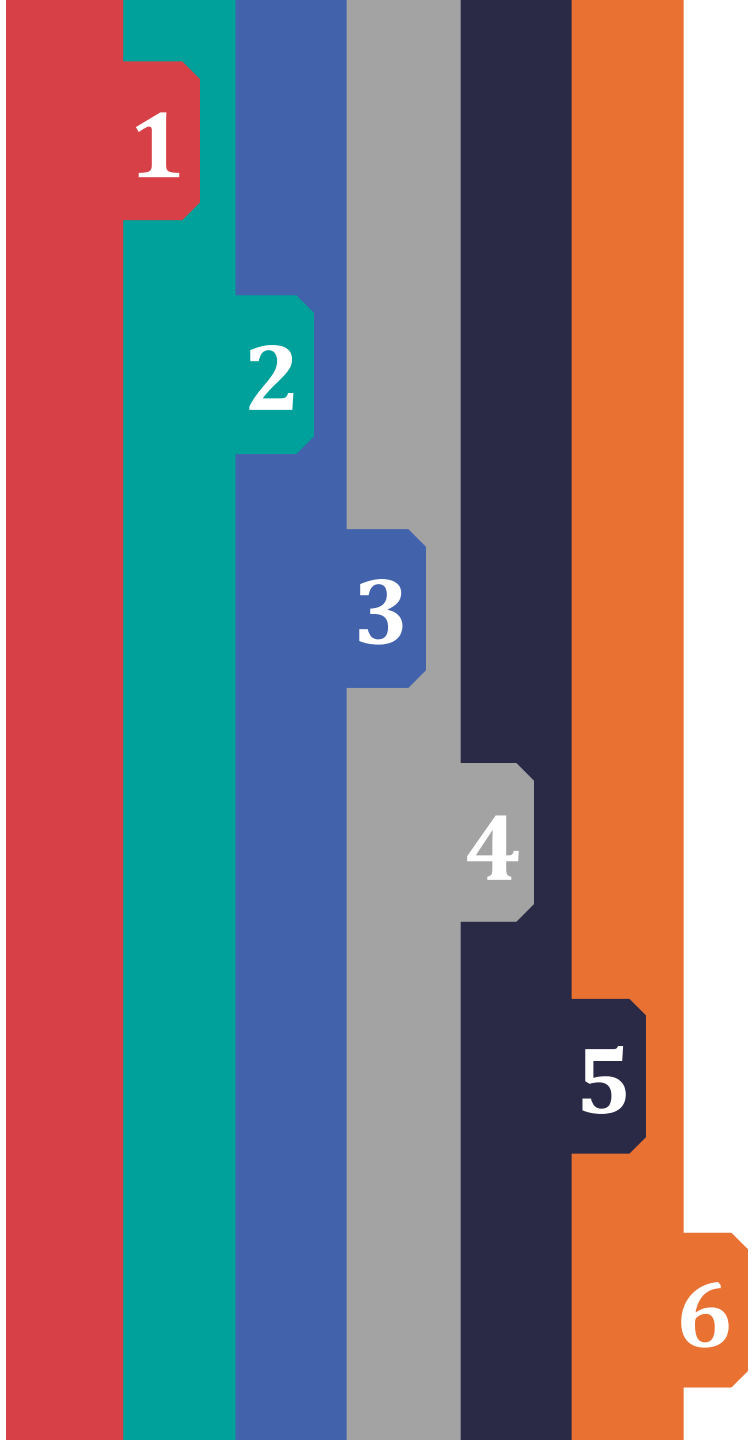
Advisory Services

Compliance & Risk | Corporate Governance
Company Secretarial | Training

Risk Assessment for Charities & Not for Profit Organisations

Guide for Trustees & Officers

March 2025



Contents

Advisory

1. How to use the risk assessment template

The managing officers/trustees of all charities and not for profit organisations (together hereon in called "**NPOs**") are required to assess and be aware of the NPOs risk exposure to financial crime and, as necessary, introduce mitigating measures to address the risk of an NPO being used for criminal purposes. Financial crime in these circumstances means money laundering, fraud, bribery and corruption.

Registered Guernsey NPOs are subject to the requirements of the Charities Law 2022. This Law requires charities to have in place adequate governance, meaning senior management are held accountable and act with integrity, to ensure public confidence in their ability to meet their intended purpose.

Advisory Services have designed a template risk assessment to guide NPOs in reviewing the risks to which their business is subject. Whilst this document focuses mainly on financial crime, governance and operational risks, the template can be utilised to cover any type of risk should that be considered necessary.

The Board, governing body or managing officials (hereon in collectively called "**the Board**") of the organisation should consider the risks to which their particular NPO is subject, using the Guidance and complete the document. The document should also record the controls that have been put in place to manage, reduce or remove those risks.

Completion of this exercise should give the Board or other governing body comfort that any areas in which the NPO is exposed to risk have been adequately considered and controlled.

Once complete the assessment should be tabled at a Board meeting, discussed and any outcomes clearly documented. The assessment should then be reviewed by the Board on an annual basis or whenever there are material changes to the business of the organisation.

2. Why is a risk assessment required?

Guernsey's National Risk Assessment ("NRA") published in December 2023, provides an overview of Guernsey as a jurisdiction and an analysis of the risks facing Guernsey regarding money laundering and terrorist financing. The NRA recognises the unique risk profile of NPO's and the potential for abuse in this sector. NPOs play a valuable role in society, channelling funds to philanthropic causes. However, the lack of regulatory oversight, the type of financial transactions involved, and the nature of some governing bodies can make them more vulnerable to abuse for illicit purposes.

This document sets out a simple structure that will allow senior officials of the organisation to:

- Identify the main risks that are faced by the charity;
- Identify new or emerging risks that are faced by the charity;
- Identify and put in place mitigants and controls for those risks; and
- Report on and monitor the risks.

3. Overview of the organisation

At the start of the risk assessment, you should include a detailed overview of the organisation. This may include:

- Date of inception and country of incorporation;
- Purpose – i.e. what the charity does;
- Governance structure – i.e. the Board and any Committees or advisory groups;
- Size of the charity including assets;
- Jurisdictional reach – include fund raising, activities and relevant connections such as staff and governing body;
- Staff and volunteers;
- Premises;
- Methods of fund raising; and
- Whether or not the charity is registered with the Guernsey Registry.

There is no one size fits all for this and the summary should reflect the nature scale and complexity of the organisation. The reader should have a good understanding of what the charity does, how big it is, the impact it has and where the money flows from and to from the summary description.

This section should also include an overall summary of the Board's assessment of risk. By way of example, a relatively small Guernsey based charity that only receives and uses funds in Guernsey may surmise that it has a lower risk profile within the NPO population. Charities that have a more international focus, particularly those that donate money to higher risk countries or areas that are vulnerable to corruption (for example, war relief charities) may surmise that their risk profile is higher than the general NPO population.

4. Acknowledgement of responsibility

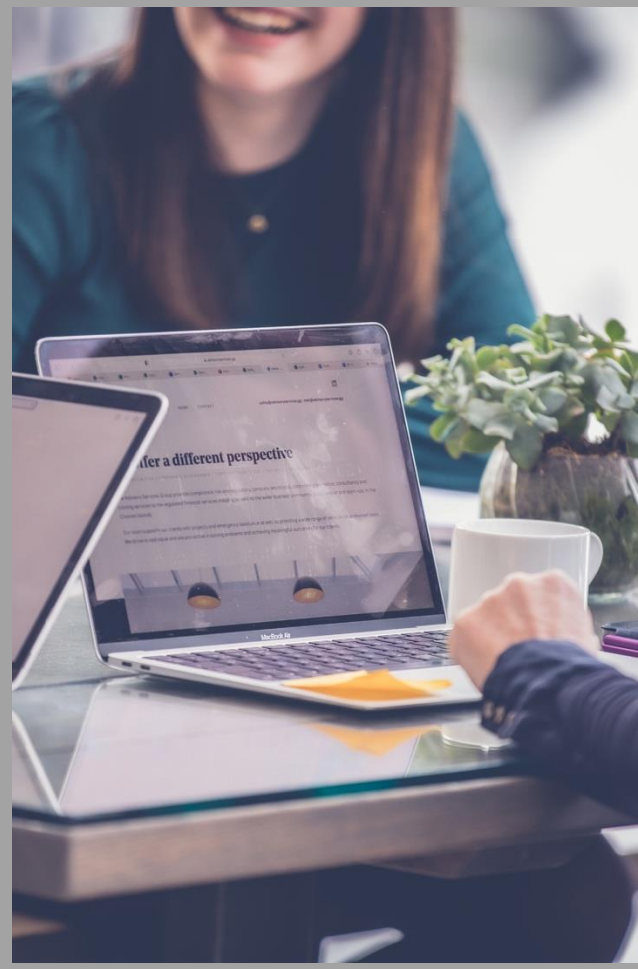
In this section of the risk assessment, the governing body and any senior management should acknowledge their responsibilities under any relevant legislation or regulatory requirements as well as formalising and documenting any delegation of roles.

Relevant legislation or regulatory requirements may include:

- Companies Law
- Charity Law
- Any governing body for the particular NPO type – e.g. national or international sports bodies
- Anti-money laundering & countering the financing of terrorism requirements

This statement should also include how the risks will be monitored. This will depend largely on the size and frequency of transactions within the NPO but monitoring activities may include:

- Compliance checks on controls – e.g. monthly reconciliation of payment approvals
- Bank reconciliations
- Audited financials or independent bookkeeping oversight
- Data gathering and reporting of MI to the Board



5. Documenting the risks (1/2)

The Board should consider any relevant risks to the NPO within the following categories. Some example risks have been given for illustration purposes. There is no one size fits all and every NPO will be subject to different risks. Once a risk is identified the Board should consider what the impact would be if that risk materialised, and what mitigation and controls are in place. As a result of this consideration an overall residual risk can be assessed and documented. If the overall residual risk is high or outside of the Board's overall appetite, then the Board may wish to consider documenting what action they will take to rectify.

The risk areas have been separated out into different key areas such as money laundering risk, governance risk etc. It should be noted that not all of these topics may be applicable to your particular NPO, and some could be combined for ease of administration.

The columns should be completed as follows:

Risk Description: Include an overall description of the issue that the charity may face that poses a key risk to its ability to fulfil its purpose.

Impact: Consider how that risk could manifest itself in a negative way for the NPO. For example, loss of funding, reputational damage, legal action etc

Likelihood of occurrence: This should be an honest assessment of the likelihood that this issue may arise generally within your sector. This assessment is not an exact science. It may help to consider each risk in the context of all the risks you identify and rank them low, medium or high.

In certain situations, it may be acceptable to have high risks and certain types of NPOs may have all risks categorised as highly likely to occur. The key is that the NPO also has in place strict management and controls to manage these higher levels of risk.

5. Documenting the risks (2/2)

Mitigation and controls: These are all the procedures and controls the NPO has in place to try to stop the risk from manifesting. Certain risks may be wholly outside of the control of the charity, for example, government policy, and this should be clearly stated.

Guernsey's Financial Intelligence Unit has published the following list of example controls an NPO might employ:

- Segregation of duties where possible;
- Regular bank reconciliation checks and multiple signatories for all bank account activity;
- Restricting full access to areas of accounting systems;
- Regular review of and spot checks on payroll records to ensure consistency with staff movements;
- Reconciliation of supplier statements, invoices and creditor balances;
- Documented authority thresholds for the approval of and payments to suppliers;
- Having professionally audited accounts;
- Random checks to ensure expenditure below key thresholds is legitimate; and
- Procedures to address any employee/trustee connections with suppliers.

Overall Residual Risk: This is the Board's assessment of the likelihood of risk once the controls are factored in. This will depend on the Board's view of the efficacy of the controls. For example, if a control is two A Signatories must approve payments but in practice the Board knows these controls are often not adhered to then they should consider the risks to be unmitigated until those controls are managed properly.

Board Action: This column details what oversight the board should have on the controls. This could be delegated to another governing body or to staff. This stands as a good checklist for the Board to use at each meeting to ensure it is continuing to meet all its obligations and not exposing the charity to unnecessary risk.

6. Appendix: Worked examples of risks (1/4)

Money Laundering

Risk Description	Impact	Likelihood of occurring	Mitigation & Controls	Overall Residual Risk	Board Action
A donor submits money that originates from the proceeds of crime	The reputational impact of being seen to utilise illicit funds could irreparably harm the NPO and its ability to raise future funds.	Low	To a certain extent this risk may be outside of the control of the charity if donation details are public. Where donation details are on request the NPO may have vetting procedures for all donations from outside the Bailiwick and amounts above £X	Low	Monitor vetting process annually.
A volunteer fraudulently uses the NPOs money to facilitate crime.	The NPO could be subject to legal proceedings and would suffer significant reputational damage.	Low	All volunteers are vetted and monitored. Dual signatures are required on all payments over £500.	Low	Monitor volunteer vetting processes annually.
A payment is made to a sanctioned individual	The NPO could be subject to legal proceedings and would suffer significant reputational damage.	Low	All beneficiaries of payments are subject to screening against sanction lists.	Low	Board monitor screening process.

6. Appendix: Worked examples of risks (2/4)

Terrorist Financing (N.B. only required if the NPO has non-Guernsey connections)

Risk Description	Impact	Likelihood of occurring	Mitigation & Controls	Overall Residual Risk	Board Action
The charity makes a donation in good faith but that money is then syphoned off and/or utilised by a terrorist organisation	Legal and regulatory action may be taken against the charity and its staff if found to have financed terrorism. The reputation of the charity may suffer irreparable damage.	Medium	Full due diligence will be undertaken on all recipients of donations. Due diligence will be carried out on a risk based process depending on the country or territory. All payments are subject to dual sign off at Board level.	Low	Review due diligence standards and payment sign off controls on a 6 monthly basis.
The charity provides equipment to a region in good faith but that equipment is used to facilitate terrorist activity	Legal and regulatory action may be taken against the charity and its staff if found to have financed or facilitated terrorism. The reputation of the charity may suffer irreparable damage.	Medium	The charity procedures include descriptions of all dual use goods. Any good rated at a medium to high risk will be subject to extensive due diligence	Low	Board will ensure procedures, including diligence on recipients of donations are reviewed at least annually.
Donations are rerouted by State Sponsors	Monies would be used for unintended purposes and may lead to reputational damage as well as the charity not being able to meet its purpose.	Low	This risk is mainly outside of the control of the charity however, payments to regions considered at higher risk of being rerouted by State Sponsors must be signed off by two Board members and subject to a fully documented risk assessment.	Low	Board will ensure procedures, including jurisdictional assessments are reviewed at least annually.

6. Appendix: Worked examples of risks (3/4)

Governance Risk

Risk Description	Impact	Likelihood of occurring	Mitigation & Controls	Overall Residual Risk	Board Action
The Board fails to adequately oversee the operations of the charity which result in a failing in one of the risk areas identified within this BRA.	At the most serious level directors may be prohibited from serving as directors/trustees. The charity would suffer reputational damage and would be unlikely to meet its main purpose.	Medium	Board members are given regular governance training on their ongoing obligations and at all times monitor their ability to meet their commitments to the charity as they fall due.	Medium	The Board will ensure it meets all training requirements.

Financial Risk

Risk Description	Impact	Likelihood of occurring	Mitigation & Controls	Overall Residual Risk	Board Action
A volunteer steals donated money before it can be paid to the charity.	The charity will lose out on funding and may suffer reputational damage.	Low	All volunteers are vetted prior to being given exposure to cash collection. Where collection is likely to be more than £200 two volunteers will be required.	Low	Review volunteer vetting process on an annual basis.

6. Appendix: Worked examples of risks (4/4)

Legal Compliance Risk

Risk Description	Impact	Likelihood of occurring	Mitigation & Controls	Overall Residual Risk	Board Action
The Board fail to meet their Company and Charity obligations with the Guernsey Registry	The charity may be subject to a discretionary penalty. For serious failings the organisation may be subject to adverse media.	Medium	The charity has in place adequate policies, procedures and controls to ensure all Company and Charity Law obligations are met in a timely fashion. Staff are given annual training on obligations and procedures.	Low	The Board review the policies, procedures and controls of the charity on an annual basis.

IT / Cyber Risk

Risk Description	Impact	Likelihood of occurring	Mitigation & Controls	Overall Residual Risk	Board Action
Emails are sent to the charities supporters from fake accounts purporting to be from the charity to elicit funds.	Funds may be lost to fraudsters. Reputational damage may mean future donors are less willing to donate funds.	Medium	The charity implements industry standard cyber security measures on websites and emails.	Low	Assess cyber security measures