Registrar of Non-Profit Organisations

Risk Management for Non-Profit Organisations

Prepared by General Registry Compliance Team
1/5/2020

CAYMAN ISLANDS
Registrar of Non-Profit Organisations

Risk Management Practices, Effective Internal Controls

1. Introduction

The public and those donating to NPOs should have confidence that money donated is used for legitimate purposes and is reaching its intended beneficiaries. Controllers are legally responsible for ensuring that the NPO's funds are properly used, adequately protected, and not misused for financial crime, terrorist or other criminal purposes. Controllers are publicly accountable, and have duties and responsibilities under the NPO Law to safeguard their NPO, its funds, property and beneficiaries. They may have employees, volunteers and agents to help, but controllers remain legally responsible. The best way that controllers can ensure a NPO's funds are not abused is by putting in place good governance and ensuring there is strong financial management, including robust internal and financial controls and risk management procedures. They should also promote the transparency and accountability of NPOs and ensure that the public can have trust and confidence in NPOs and their work.

2. Definition of Risk

Risk can be defined as the possibility that an event will occur and adversely affect the achievement or objectives of the NPO. Categories of risk include:

- **Operational Risk**: the operations of the NPO are adversely affected as a result of failure of systems, processes and management.
- **Reputational Risk:** The risk of loss in the NPO reputation due to an adverse event, leading to loss in confidence that the NPO is being run with the necessary integrity, loss of volunteers, customers and donations.
- **NPO Sector Environment Risk**: the risk of loss of confidence on the NPO sector due to a catastrophic occurrence, resulting in adverse domestic and international sanctions, loss of donations and investments.
- **Compliance risk:** the exposure to legal penalties, financial forfeiture and material loss an NPO faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices.

3. Risk management strategy

All NPOs should have a formal risk management strategy in place which will allow the management/ board of the NPO to show they are meeting their legal duty to protect the funds and property of the NPO, and applying them properly through managing risks in a realistic and reasonable way. The Registrar understands there is no one size fits all approach to risk management, especially when taken into context the nature of the NPO, its size, business model, purpose, activities and jurisdiction of operations. However the Registrar does expect that all NPOs will have some form of risk management strategy in place.

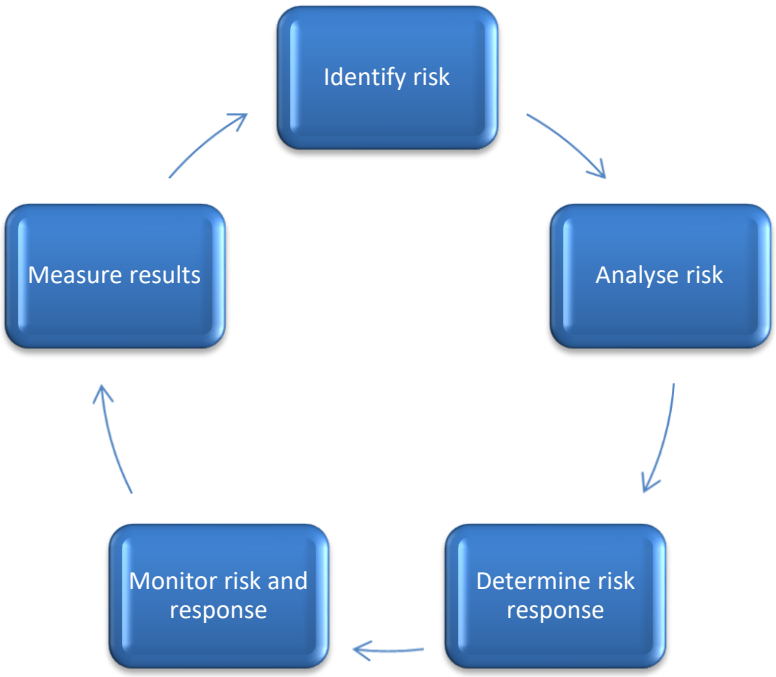
4. The risk management process

As a best practice for implementation, controllers should consider creating a formal policy which identifies the steps a NPO has taken or will take to manage risk, bearing in mind this will depend on the size and context of the NPO. This serves to demonstrate that the NPO is accountable to its stakeholders including beneficiaries, donors, funders, employees and the general public.

Risk management is a dynamic process ensuring that risks are addressed as they arise. This involves an examination of the purpose and activities of the NPO, its area or jurisdiction of operation, delivery or programs, who the NPO raise store move and use of its funds and potential threats posed to exploiting any of those phases. This process should also be cyclical (ongoing as it when an issues is identified it is addressed and where applicable reviewed again later in the year) so as to establish how previously identified risks may have changed and how the new identified risk will be mitigated. Risk management is not a one-off event and should be seen as a process that will require monitoring and assessment. It needs to be clear who has responsibility for implementation and monitoring. If a NPO has staff there should be communication with them (and, where appropriate, volunteers) at all levels to ensure that individual and group responsibilities are understood and embedded into the culture of the NPO. A successful process will usually involve ensuring that:

- ❒ new risks are properly reported and evaluated
- ❒ risk aspects of significant new projects are considered as part of project appraisals
- ❒ any significant failures of control systems are properly reported and actioned
- ❒ there is an adequate level of understanding of individual responsibilities for both implementation and monitoring of the control systems
- ❒ any further actions required are identified

- ❒ controllers consider and review the annual process
- ❒ controllers are provided with relevant and timely interim reports



The risk management cycle

The below principles are applicable to all NPOs regardless of size, nature purpose or activities. As a best practice it is recommended that NPOs formalize these processes within its respective internal framework.

- **Identify risk**: The NPO should have processes in place for identifying and reviewing the risk it faces. Risk is constant and changes from time to time, and risk reviews should be taken regularly. All NPOs raise, store, move and use cash and or resources. Implementation of a risk management framework will take into context the circumstances surrounding each phase, vulnerabilities and threats present to each phase and processes in place that addresses these vulnerabilities. Vulnerabilities or potential vulnerabilities are always present, a good risk management framework will remedy mitigate these risk. By way of example: An NPO collects funds weekly; the two persons have sole responsibility for collection, counting, entering information in the record, banking or distributing those funds and subsequently reconciling the finances. Risk exposure is unlawful taking or use of those funds, the vulnerability to each phase is that each phase can be manipulated by either person or jointly as there is no separation of

duties to include an independent third party. To mitigate this risk, have separation of duties with individuals performing different phases and each phase over looked by an independent person.)

- ❒ **Analyze risk**: This phase calls for NPOs to assess the potential seriousness of the risk. The potential loss that can result from an adverse event or development. This assessment should consider the probability or likelihood that an adverse outcome will occur as well as the potential size of the loss in the event that an adverse outcome takes place. Those NPOs that have international connections, and or remit funds off island in support of beneficiaries or humanitarian aid; or fund missionaries, must consider the potential terrorist financial risk exposure that results from these activities.
- ❒ **Determine risk response**: In this phase, management of the NPO decides how risk will be addressed. In broad terms, the NPOs risk can be dealt with by utilizing the following options:
  i) Avoid the risk: through prohibiting certain activities, stopping activities, targeting actions and exclude the identified risk, screening activities to eliminate risk and eliminating risk.
  ii) Reducing risk: through dispersal of activities, setting up controls and or reorganizing resources
  iii) Retaining or accepting the risk: through simple acceptance
  iv) Transferring the risk: through insurance, hedging, sharing the risk , outsourcing the risk or requiring indemnities
- ❒ **Monitoring Risk and Response:** Control systems should be established by the Board of the NPO to monitor risk. There should be systems for identifying situations that are getting out of control or where significant events have developed or are developing
- ❒ **Measuring Results**: The NPO should consider utilizing risk mitigative tools to assist in risk management.

5. Responsibility of Board of Directors/ Management, staff and volunteers

The responsibility for the management and control of a NPO rests with the Board of management and therefore their involvement in the risk management process is essential, particularly in setting the parameters of the processes and reviewing and considering the results. This should not be interpreted as meaning that the controllers must undertake each aspect of the process themselves. In all but the smallest NPOs, the controllers are likely to delegate elements of the risk management process to staff or professional advisers, but they do not delegate their responsibilities for it. The controllers should review and consider the key aspects of the process and results. If they do not ensure that they are properly informed of relevant risks before important operational decisions are made, it would be difficult to see how they can properly discharge their duties as NPO controllers.

Controllers duties and responsibilities

NPO controllers must use their NPO's funds and assets only in furtherance of the NPO's purposes. They must avoid undertaking activities that might place the NPO's funds, assets or reputation at undue risk. They must avoid any mismanagement and or abuse of the NPO's funds.

In practice, for those situations where the risk is high, in order to meet their legal duty to protect NPO assets with the necessary care and properly to assess risk, controllers must carry out appropriate due diligence on those individuals and organisations that the NPO receives donations from, gives money to or works with closely.

In more detail

Legal requirement: controllers have ultimate responsibility for controlling and managing the affairs of a NPO. They must:

- ❒ Comply with the law (including NPO, Penal Code and Proceeds of Crime(where applicable) as an example) and act in the best interests of the NPO
- ❒ Comply with the legal principles of duty of care and duty of prudence and maintain control of charitable funds
- ❒ Ensure that the NPO's funds are used properly, lawfully and in furtherance of the NPO's purposes

A Controller's duty of care requires that they exercise reasonable care and skill in carrying out their responsibilities to ensure this is the case.

Controllers must avoid undertaking activities that might place the NPO's funds, assets or reputation at undue risk. This duty applies in a number of ways. NPOs can take risks. However, as a minimum, controllers must consider, identify and manage the risks and their impact on the NPO and its property.

Controllers' duties and responsibilities for monitoring the end use of funds

NPO controllers must use their NPO's funds and assets only in furtherance of the NPO's purposes. They must ensure that funds are properly protected so that, for example, they are not used for illegal or improper purposes, including for terrorist and other criminal purposes.

In practice, a significant aspect of a controller's legal duty to protect NPO assets with the necessary care means ensuring that where a NPO gives money to partners or beneficiaries, or uses partner and delivery agents, or where it funds other projects, NPO controllers must properly and appropriately monitor the

use of the NPO's funds, checking both that funds reach their destination and that they are used for the purposes intended.

Monitoring end use of funds

In order to comply with their duty of prudence, controllers must use NPO funds only in furtherance of the NPO's purposes, as set out in its objects. They must also ensure that the NPO's funds are spent for the purpose for which they were raised. Controllers' duty of care requires that they exercise reasonable care and skill in the circumstances in carrying out their responsibilities to ensure that this is the case.

Unlawful use of charitable funds

The use of NPO money or property for unlawful purposes cannot in any circumstances be regarded as a proper use, and is in breach of NPO law and potentially against the Penal Code. It is not acceptable for a NPO to carry out activities that are unlawful either in the Cayman Islands or in an overseas country in which it operates. Controllers might not be able to protect their NPO entirely from criminal abuse, but they have a legal duty of care to the NPO and must therefore take reasonable steps to protect it as best they can. This duty of care applies to the protection of all of the NPO's property, including funds, property and reputation.

What an individual NPO and its controllers must or should do in their NPO and what is a reasonable and proportionate approach to adopt when taking action to comply with those legal duties will depend on a range of factors.

It will, for example, depend on:

- ❒ Different aspects of a NPO's work and the risks which arise
- ❒ How much money is involved
- ❒ Whether partners and funds are overseas and what local problems there are - for example in areas of conflict

All NPOs must have, as a minimum:

- ❒ Some form of appropriate internal and financial controls in place to ensure that all their funds are fully accounted for and are spent in a manner that is consistent with the purpose of the NPO – what those controls and measures are and what is appropriate will depend on the risks and the NPO.
- ❒ Proper and adequate financial records for both the receipt and use of all funds together with audit trails of decisions made – records of both domestic and international transactions must be sufficiently detailed to verify that funds have been spent properly as intended and in a manner

consistent with the purpose and objectives of the organisation. This information is also crucial in assisting the NPO in assessing any potential risk of terrorist financing.

- ❒ Given careful consideration to what due diligence, monitoring and verification of use of funds they need to carry out to meet their legal duties.

Take reasonable and appropriate steps to know who their beneficiaries are, at least in broad terms, carried out appropriate checks where the risks are high and have clear beneficiary selection criteria which are consistently applied. As regards to monitoring, in most cases, some form of monitoring is likely to be required.

In all these cases, the more complex or significant the activity or project for the NPO, the more money or the higher the number of transactions involved, the more steps that are likely to be required as reasonable to ensure a controller complies with these duties, even when balancing this with the volume and cost of administration this may involve. What is appropriate and proportionate therefore depends on the nature of the risk, its potential impact and likelihood of occurring. What is important is for controllers to be able to show that the action they have taken is reasonable in light of those risks and actions.

The existing requirements for independent examination and audit in larger NPOs may assist controllers, but they should not be relied on as the only way or fail safe way of ensuring no abuse takes place.

Responsibility outside of the controller board

Others may also have a role in supporting controllers in carrying out these responsibilities, such as Senior Officers, staff they employ to carry out a monitoring role or internal and external auditors or independent examiners. However, controllers need to remember that they remain responsible and accountable for ensuring proper monitoring takes place and their legal duties are met.

6. Responsibility of the NPO

Under the NPO Law the Registrar of NPOs has responsibility to ensure that NPOs have the requisite internal controls in place to mitigate the terrorist financing risk. Controllers and senior officers must therefore be aware that NPOs have systems and controls in place to ensure proper and legitimate use of funds in furtherance of their NPO's purposes.

Controllers must therefore act prudently in the receipt and expenditure of charitable funds. They must ensure where applicable (for example, large cash donations) that the funds received by the NPO are legitimate. When using funds to support charitable activity, controllers must ensure they take

reasonable steps, taking account of the particular circumstances, to protect the funds from being abused, including for criminal and terrorist purposes.

This means that the controllers must exercise sufficient control over their NPO's financial affairs and act prudently in choosing their partners. As an absolute minimum, they must keep proper and adequate financial records for both the receipt and use of funds and audit trails of decisions. Records of both domestic and international transactions must be sufficiently detailed to show that funds have been spent properly as intended and in a manner consistent with the purpose and objectives of the organisation. Grants made to other organisations must be disclosed in accounts. It is understood that in many NPOs, duties related to the operational management of the NPO funds may be delegated to a treasurer or in some large NPOs to a Finance Committee. Controllers however remain accountable for these funds and should at all times ensure that the requisite internal controls are implemented to assist them in being informed.

These responsibilities underpin and operate alongside good internal governance, transparent accountability and strong financial management. Ensuring proper internal and financial controls and risk management procedures are in place and implemented is vital.

7. Compliance in practice

In order to demonstrate that they have complied with this duty, controllers may need to implement realistic and reasonable risk management strategies to identify and mitigate significant risks to the NPO's funds and assets. If these are used *they should be relevant and proportionate given the NPO's activities and nature of its operations*. Risks may take a number of forms, including operational, financial, reputational and external, as well as compliance with the law and regulations. Controllers' duty of care requires that they exercise reasonable care and skill in the circumstances, in carrying out their responsibilities to ensure this is the case.

As well as protecting the NPO from internal abuse, it is also the responsibility of NPO controllers to exercise reasonable care over the selection, use and monitoring of a NPO's partners, donors and beneficiaries. When choosing partners to work with, controllers should assess the need to conduct due diligence, and where applicable conduct the relevant due diligence checks to ensure that they are appropriate partners / beneficiaries for them to work with. They must also take reasonable steps to ensure the NPO's funds will be properly used.

8. Controls

The Board of Director/ Management must ensure that sound systems of internal controls are in place to safeguard the NPOs assets. This includes annual reviewing the NPOs internal policies related to controls, to ensure there are still addressing the identified risk.

[1]Internal controls are defined as a system of governance through which policies, processes, tasks, behaviors and other aspect of the NPO that, taken together, helps the NPO to:

- Operate effectively and efficiently; these operations should allow the NPO to respond in an appropriate way to significant risk to achieving the NPOs objectives
- Help to ensure that there is a high quality of external and internal financial reporting
- Helps to ensure that compliance with the NPO Law and other applicable laws and regulations; and also with internal policies for the conduct of business of the NPO is taking place.

There are three main types of controls:

- ❒ Preventative – controls that prevent vulnerability from being exploited. E.g. the NPO having a system in place to ensure that prior to sending funds off island it has conducted some due diligence on the beneficiary to mitigate the risk of terrorist financing.
- ❒ Detective – controls that allows management of the NPO to identify a system failure and mitigate potential significant loss. E.g. an audit/ reconciliation of the monthly finances to ensure that the balance on the bank statement is justified through legitimate expenses and corresponding financial records
- ❒ Corrective- controls that are implemented post discovery of an exploited vulnerability. E.g. separation of duties within the funding cycle. Separations between the people, who collect, reconcile and deposit the cash.

[1] Turnbull Report

9. Risk based approach

As a guiding principle, the greater the risks, the more NPO controllers and senior officers have to do to ensure that there is an understanding of the related risk, implement the relevant controls needed to address the risk and conduct where applicable frequent reviews to demonstrate that the risk management process is being monitored.

Bearing in mind that majority of NPOs operate on a voluntary basis and there is limited resources available, an effective way of addressing this issue is by implementing and executing a risk base approach to managing the NPOs risk. Simply put, a risk base approach is directing attention where it is most needed to address the more critical risk with the limited resources.

An effective risk base approach program requires the NPO to understand where its major risk is located, the controls needed to mitigate that risk, whose is responsible for ensuring that the controls are executed and an ongoing monitoring to ensure that the program is working.

In this context means the actions controllers take should:

- ❒ Stop abuse of the NPO, its funds and property taking place.
- ❒ Use greater effort and stronger measures for higher risks, meaning for some risks, controllers must take certain action but for other risks, there is greater discretion and flexibility about what to do
- ❒ Take account of the amount of money at risk as a significant factor, although this will not and cannot be the only factor - in some cases, where there are very high risks a number of important steps are still required to safeguard what might be a relatively small amount of money from the NPO's perspective
- ❒ Be flexible enough to adapt to and complement the NPO and its work
- ❒ Avoid negative impact on people donating to or benefiting legitimately from the work of the NPO
- ❒ Not duplicate the work or responsibilities of others
- ❒ Not where possible be unduly costly or administratively burdensome for the NPO, although a short term or one off cost needs to be assessed against the long term benefits, assurances

required and donor and public expectations; but controllers should do what is necessary at their discretion even if there are associated costs.

Risk based approach in practice

Controller's responsibilities apply to controllers of all NPOs, whatever its size and or activities. What this means in practice however depends on the circumstances. The extent, form and detail of the project and partner monitoring checks and due diligence that is required, and how this should extend to donors and beneficiaries, will depend on the nature of the risks in the particular circumstances. The level of checks and procedures required will be dependent on the nature of the activities the NPO carries out, and how and where they are undertaken. Where the risks are high - such as in areas where it is well known or likely that proscribed and other terrorist organisations are known to operate - controllers must ensure those steps are sufficiently robust.

The starting point is: the greater the risks, the more NPO controllers need to do to mitigate them.

Due Diligence to a Risk Base Approach

In the context of controllers due diligence and monitoring responsibilities, the risks are affected by a number of factors. This center on what activities the NPO undertakes, where, how and by whom. In the context of due diligence and monitoring responsibilities, the risks are affected by a number of factors. For example:

- ❒ What activities are being carried out?
- ❒ How are activities going to be delivered and the timescales involved?

Who' will carry them out? Will it be staff controlled and supervised by the NPO? If a NPO is using other organisations as partners or agents, this may or may not increase the risks. By using third parties, controllers may manage the risks to their staff and to the NPO, but only as long as the controllers put in place good monitoring and reporting arrangements and formalize the relationship to protect the NPO. If proper safeguards are not put in place this may increase the risks to the NPO.

- ❒ Where' will the project be based?

The risks may increase where it is in a conflict zone or within a local community under the influence of individuals linked to terrorism, or where criminals are known to operate. The risk will vary if it is in a region or country which is currently unstable or where the infrastructure is poor.

There may be additional factors to consider in respect of risks because of local issues. Are there local disputes which will affect delivery of the project? For example, will the local dispute mean certain people may be excluded from participating in the charitable activity or that certain people will be given preference or only allowed to participate, whether or not they have charitable needs? Or, for example, do the partners or beneficiaries who may operate in a different regulatory system understand what they need to do for the NPO?

- ❒ What 'methods' are used to safeguard NPO funds?

In order to operate effectively and transparently when delivering aid or undertaking other charitable work, every NPO should have access to formal banking facilities. It is a decision for the NPO as to which bank there chose to hold their account. However, the Registrar would have serious concerns if NPOs were not able to operate because of a lack of banking services. If financial services are declined or withdrawn from a NPO, harm could result to its work, its ability to operate transparently and ensure it can safeguard its funds. If the NPO or a local partner has to use cash, or alternative money systems and payment mechanisms, such as Money Service Businesses (MSBs), then they will need to take extra precautions and do more to protect the funds and ensure close monitoring of their use.

- ❒ The 'public profile' of the proposed work and the likely media and/or local or public interest in it
- ❒ Where 'third parties' may be involved, and not just delivery partners, what degree of influence or control does the NPO exert, for example, is the NPO able to carry out adequate monitoring?

Controllers also need to bear in mind that some risks may only become evident once a relationship with a donor, beneficiary or partner or the work has begun. As these materialize, the risks are likely to need to be reassessed.

10. <u>The 'know your' principles Why is due diligence important?</u>

As previously indicated; these measures are not applicable to every NPO neither to every transaction of receipt of donation. It is important that NPOs consider those high risk situations,(for example receiving large cash donations or donating funds to high risk jurisdictions) and apply these recommended measures.

In high risk scenarios, in order to ensure that they are fulfilling their duty to manage their NPO's funds properly, controllers need to know where the funds come from, how they are to be applied in accordance with the NPO's objects and who will be involved in delivering the charitable services.

The voluntary nature of NPOs and their areas of work can make them vulnerable to people who want to misuse NPOs for their own gain. NPOs are highly valued in society and the very nature of NPOs can make

them attractive targets for criminal abuse such as fraud, theft and money laundering. People also abuse NPO for private advantage, for example by ensuring a NPO uses a particular organisation or individual to provide services which are not necessarily charged on the best terms available. Financial abuse and crime can result not only in a significant loss of charitable funds but also in damage to public trust and confidence in NPOs more generally.

Examples

A NPO might engage a person or organisation to provide charitable services on its behalf to beneficiaries. Without proper due diligence the NPO might be persuaded to drop standards and use a provider who in reality they know little about or whose services are below par and not value for money. This can create opportunities for others to abuse the NPO and allow some of the NPO's funds to be diverted for criminal and or terrorist purposes.

Incidents of abuse of NPOs are small in number compared to the size of the sector. However, it does happen, and when it does the impact on the NPO and its work can be great. It also affects public trust and confidence in NPOs. NPOs by their very nature, services offered and the fact that most of the operations involved high levels of trust, expose NPOs to vulnerabilities of internal abuse; the Registrar is aware of these risk as such it is important that NPOs and controllers take this risk seriously.

Some NPOs may be at greater risk because of the activities they undertake or their structure, for example, numerous fundraising activities delegated to multiple persons and spread over different areas, where controls are hard to implement. However, no NPO is immune so all NPO controllers must ensure that they are aware of and assess the risks and take proper steps to manage them. Simple risk mitigative method would be set documentation related to all monies raised and reconciliation where these activities involve for example raffle tickets or other paper generated activities.

Criminals may exploit NPOs by misappropriating the NPO's funds through fraud, theft, money laundering or diverting charitable funds from legitimate charitable work. Examples of the types of fraud and financial crime that NPOs may be susceptible to include:

1) **Donations**: using a NPO to launder proceeds of crime, or to make a credit card donation to test whether a stolen card still operates.
2) **Partners**: submitting false or inflated invoices or purchase orders for funds to be paid by the NPO.
3) **Beneficiaries**: making fake grant applications or creating false or inflated numbers of beneficiaries, for claims and other forms of identity fraud.

NPOs working internationally may be exposed to particular risks inherent in the environment in which they operate. Risk associated with overseas NPOs include terrorist financing abuse, the NPO assisting an individual or entity that is subjected to Targeted Financial Sanctions to evade such sanctions as well as risk associated with these jurisdiction or entities linked to proliferation financing Breaches related to the sanction regime can also involve some indirect benefit to the designated person or entity. At all times NPOs should be aware who it is dealing with when funds are sent off island, what will those funds be used for and obtain evidence that funds have been used for the intended purpose.

It can be difficult to identify financial abuse as criminals may be adept at presenting their interests and activities as legitimate and lawful. Establishing the identity and legitimacy of any organisation the NPO works with can help reduce some of these risks. For example, without appropriate due diligence in high risk situations, controllers are not going to be able to identify whether a partner or beneficiary is designated or a proscribed organisation.

Working to these principles helps controllers ensure they comply with their legal duties and responsibilities to safeguard the NPO's funds and property. Following the principles will also enhance their NPO's transparency and accountability, which in turn will help build the trust and confidence of a NPO's donors, supporters, partners and beneficiaries.

Due diligence

Due diligence is the range of practical steps that need to be taken by controllers in order to be assured of the provenance of charitable funds and confident that they know the people and organisations the NPO works with, and able to identify and manage associated risks.
'Due diligence' is an important part of controller’s duty and is essential in safeguarding NPO assets. It means carrying out proper 'checks' on those individuals and organisations that give money to, or receive money from, the NPO, including partners and others that are contracted to work with it.

Monitoring

Where NPOs give money to partners and beneficiaries, especially large amounts of money or in high risk situations, it's vital to ensure that adequate 'monitoring' takes place. In short, controllers should take appropriate steps to verify that NPO funds or property reach their proper destinations and are used how the NPO intended. This will allow controllers to have clear oversight of how NPO funds are used across the full scope of its operation, whether nationally or internationally.

11. Why is identifying and assessing the specific risks important?

Risk to the NPO and its work directly affects what sort of due diligence, monitoring and action the controllers need to take to ensure the NPO's funds are used properly by the people they give them to.
It is vital that controllers identify and assess the risks to the NPO because the impact of these risks on the NPO's work directly affects:

- ❒ what sort of due diligence the NPO controllers need to carry out
- ❒ what organisations and individuals they need to carry this out on
- ❒ what monitoring procedures they need to have and apply
- ❒ what action they need to take to ensure charitable funds are used properly by the people they give them to

NPOs are required by law to file an annual return for which the controllers have legal responsibilities. Those NPOs that gross CI$250,000.00 per year and remit 30% (CI$70,000.00) are required to have a review done of their finances. This review should be conducted by a qualified accountant and a copy of that review report provided to the Registrar As a best practice, NPOs are encouraged to make a risk management statement in their review / financial statement as a matter of good practice.

How do controllers identify and assess the risks?

Controllers need to be aware that the risks that a NPO faces depend very much on the size, nature and complexity of the activities it undertakes, and also on its finances.

As a general rule, the larger and more complex or diverse a NPO's activities are, the more challenging it will be for the NPO to identify the major risks that it faces and put proper systems in place to manage them. This means that formal risk management processes may be necessary to help controllers and that these will need to be tailored to fit the circumstances of the individual NPO, focusing on identifying the major risks. In most cases, controllers of large, complex NPOs will need to explore risk more fully than smaller NPOs and in greater detail than given in this guidance. How controllers identify and assess risk and what tools they use to help them to do so is up to them.

NPOs are encouraged to identify and consider risk in the context of their day-to-day activities and incorporate it in their management processes and decision making.

Identifying and managing the possible and probable risks that a NPO may face is a key part of effective governance for NPOs of all sizes. Managing risk effectively is essential if NPO controllers are to achieve their key objectives and safeguard their NPO's funds and other assets. NPO controllers need to identify

risks that the NPO faces and decide whether the systems and procedures they have in place to address them are adequate, reasonable and proportionate.

Risks may take a number of forms, including for example:

1) Operational
2) Financial
3) Reputational
4) External
5) Compliance with the law and regulations in the Cayman Islands and, if applicable, internationally

In order to comply with their basic duties, NPO controllers should consider the full range of risks. How controllers identify and assess risk and what tools they use to help them to do so is up to them. Smaller NPOs with simple activities and facing low risks, may need to do nothing more than ensure they are aware of the risks and take them into account in decision making. However, in more complex situations, having a structured process or methodology may be helpful for ensuring key areas of risk arising from both internal and external factors are considered and identified and the controllers can demonstrate that this has been done.

Some NPOs find carrying out a formal written risk assessment, either relating to their work as a whole or to specific projects or work streams, helps controllers make informed decisions in relation to the NPO's operation. It also highlights any gaps where further scrutiny may be needed, and procedures developed. There are a number of models and frameworks which may be helpful. Some of these are referred to or provided as 'tools' for controllers.

The Registrar will always support NPOs to deliver legitimate humanitarian aid and other charitable services. The Registrar appreciates the challenges that some NPOs may face. This includes, for example, NPOs working in areas where corruption, violence, or serious or organized crime is common practice, or terrorists and other criminals are known to operate, perhaps where they have some degree of control over access to people in need. High risk activities require prudent risk management. Those NPOs that operate in high risk jurisdiction are encouraged to recruit board members with the requisite skill set and experience to assist with the desired governance. For other NPOs the risks are low. An example would be those NPOs whose operations are based solely in the Cayman Islands, their activities are straightforward, they raise store move and use cash in the Cayman Islands. This is why a risk-based and proportionate approach is important and more appropriate than a 'one-size-fits-all' approach.