CSO TOOLKIT

AGENTS FOR CITIZEN-DRIVEN TRANSFORMATION (ACT)

CSO RISK ASSESSMENT AND MANAGEMENT

Funded by the European Union

Implemented by the British Council

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This Toolkit is produced as a resource to support the organisational capacity development of the CSOs that are participating in the EU-funded Agents for Citizen-Driven Transformation (ACT) Programme in Nigeria. The content and materials used to develop the booklet were sourced from existing third-party, publicly available material; details provided in the Reference Section, which we would like to acknowledge and thank.

PURPOSE

This Toolkit has been developed to support CSOs[1] in Nigeria to manage their risk in order to plan and work effectively. It is not a Training Manual - but aims to support CSOs to stay on track, to refine their approach to identifying and mitigating potential risk, and to improve the validity and legitimacy of their CSO. Assessing potential risk should be integrated into governance, strategic planning, project planning and decision-making processes. The level of risk faced does not reflect the stage of development of a CSO; this Toolkit is therefore relevant for all CSOs from emerging to mature. The ACT Risk Assessment and Management Toolkit has been designed to support CSOs to plan and to prepare, as much as is possible, for potential risks within their own local context.

With increased levels of violence in conflict settings[1], due diligence requirements and regulations related to anti-corruption, money laundering and counter-terror efforts, CSOs contend with more risks to their staff and operations now than they have in the past. A CSO-wide risk management framework improves the ability of the CSO to be more adaptable and better prepared to deal with risky situations.

In line with ACT's commitment to Human Rights and Gender and Social Inclusion, and their impact on the sustainability of CSO project interventions, it is anticipated that CSOs' projects and plans demonstrate the mainstreaming of Gender and Social Inclusion and the adoption of a Rights-based Approach.

The ACT programme supports CSOs to collaborate through its Peer Learning Programme. This collaboration can help build trust, build a culture of shared learning and support, and together CSOs can better meet the resource challenges that face them. The ACT Toolkits provide further support with CSOs' organisational capacity development, and can help CSOs in Peer Learning groups to guide and support each other.
https://www.justice-security.ng/resources/toolkits

WHAT IS RISK?

Commonly risk is considered as a cause that might make something go wrong within a CSO's environment or its project(s). One definition of risk with regard to managing a development programme, provided by UNDP, is 'the effect of uncertainty on an organisation's objectives'. Potential risks come and go, or evolve, as a CSO's internal dynamics change, and as the external environment in which it operates changes. Keeping on top of the risks that may affect the CSO is an ongoing activity.

> "Strategic risk management can enhance - but never replace - a development decision-maker's knowledge, experience, cross-cultural skills, and other abilities."
>
> Managementforimpact.com

WHAT IS RISK ASSESSMENT AND MANAGEMENT?

Risk assessment aims, firstly, to anticipate possible risks and to assess the level of those risks. Then it aims to seek ways to prevent the risk from happening, or to manage and minimise the impact if the risk is not preventable.

Responding to risk will help the CSO to achieve its objectives, guarding against potential obstruction(s). Risk management must be part of the CSO's organisational and programme/project management, ie: in strategic planning, decision-making, operational planning, project planning, implementation and resource allocation. Risk management is good practice as it helps the CSO to guard against potential harm to its staff and to its beneficiaries, to improve its effectiveness and to use its resources efficiently.

A risk management system encompasses two key elements:

1. Risk management framework (including policy)
2. Risk management process and register

Risk is present at all levels of a CSO's operations. There are risks that may affect the CSO as a whole – such as risks to the CSO's reputation. There are also risks that may affect the safety and security of staff, financial risks, service delivery activities and those risks that may affect multiple areas. There are risks specific to every programme and project. So, what this means is that everyone in the CSO has some responsibility for managing risks.

[1] https://conflictandhealth.biomedcentral.com/articles/10.1186/s13031-021-00410-4
[2] For CSOs please read across the categories, ie: CBOs, CSOs, CS Networks and NGOs

CSO AND GOVERNANCE REQUIREMENTS

Risk management is an important element of good governance, so ongoing monitoring of how risk is being identified and managed is an essential role of the CSO's governing body and senior management. By managing risk, the CSO can guard against poor decision-making, complacency, potential exposure to the damaging consequences of its actions. Risk management can identify and consider how to mitigate against possible external forces that could affect progress (eg: related to security, politics, climate, or other external issues relevant to the CSO's context, sector and location).

In addition, the principles of good governance dictate that those responsible for the management of a CSO have an obligation to protect, not just the CSO and its staff, but the interests of its constituents and to prepare to manage risk accordingly.

For these reasons, a risk management policy, its processes and activities need to be aligned with the CSO's strategy, policies and systems, in order to support the board members' and senior management's oversight role.

BENEFITS OF RISK MANAGEMENT

As well as contributing to good governance and compliance, effective risk management contributes to both strategic planning and operational planning within the CSO. It creates confidence that a CSO can deliver its objectives and achieve its planned outcomes, manage threats to an acceptable degree, and make informed decisions about opportunities.

Benefits of risk management include help to:

- Prepare to take action that would be effective in the face of an emergency arising
- Prepare for alternatives if an unexpected situation occurs
- Reduce the likelihood of possible costly and logistical surprises
- To plan for the 'what if...' in advance
- Prepare for challenging events to improve resilience
- Improve the quality of decision-making at all levels
- Improve planning processes
- Prioritise resources
- Increase performance
- Establish clear purpose, roles and accountabilities for all staff
- Improve stakeholder confidence in the CSO

CATEGORIES OF RISK

Risks can commonly be categorised into three broad inter-connected types:

1. **Contextual:** risks which are external and often outside the control of the CSO (eg: natural disaster, terrorist activity, political instability, lack of public infrastructure, climate change).

2. **Programmatic:** risks which are related to how the projects or programmes are designed and implemented, which may result in not meeting the needs of the constituents, and could even do harm (eg: weak situational/contextual analysis, lack of capacity, ineffective stakeholder analysis, poor participatory planning).

3. **Organisational:** risks which are internal to the CSO, and which may affect the security and safety of staff, security of information (Internet), and/or the reputation of the CSO (eg: financial and human resource management systems/processes)

RISK ASSESSMENT TOOL

It is very difficult to set up risk management systems if the CSO does not have a clear understanding of the threats it may face. The following is the first step in any strategy, new programme or project to ensure an understanding of the context.

BEFORE STARTING A PROGRAMME OR PROJECT[3]:

CONTEXT ANALYSIS AND ACTOR MAPPING

→ What is the context and who are the key stakeholders?

What impact will the CSO and programmes have on the context and key stakeholders?

↓

RISK ASSESSMENT

→ What are the threats/potential threats the CSO faces?

What are the CSO's vulnerabilities to those threats?

What is the level of probability and impact of the risks?

↓

(DIGITAL) SECURITY

→ What technology will the CSO need in this context to carry out its programme/project safely, effectively and securely?

What are the associated risks for the CSO, its, staff and constituents?

↓

STRATEGIES:

Reduce

Transfer

Accept

Avoid

→ Understanding the best approach, based on the type and level of risk (see 'Ways to deal with risk' details below).

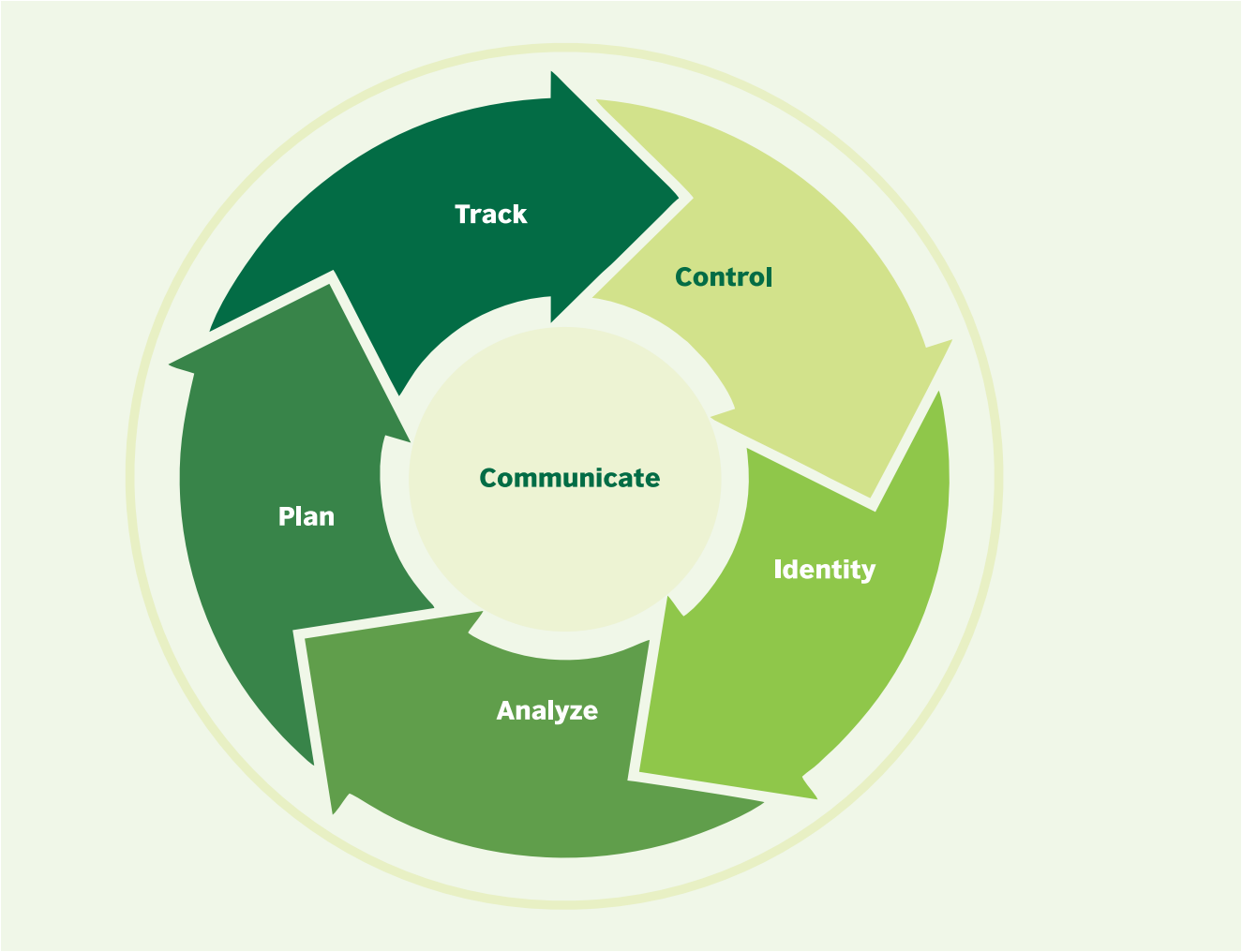
Understanding your organisational approach: what strategies do you use generally and in this context in particular?

[3] Adapted from: https://gisf.ngo/wp-content/uploads/2020/04/EISF_Security-to-go_guide_2020_Module-3.pdf

OVERVIEW OF A RISK MANAGEMENT FRAMEWORK

The risk management framework can be used to assess risk across each of the following areas:

- Governance, strategy, financial management, and planning
- Operational and staff management, fundraising, work plans and activities
- Internal and external reporting processes and communications mechanisms
- Policies, procedures, values and culture



Larger CSOs may have a more extensive Risk Management Framework document, whereas smaller CSOs may have a briefer document simply stating the understanding of the CSO's broad approach to risk management. Either way, consider the following steps.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

1. Identification

Write down all the potential and actual risks and threats – and ask other staff/volunteers/ board members/stakeholders to contribute.

2. Analyse/Assess

Together evaluate each risk by determining the likelihood of it happening and the level of impact it would have if it did happen.

3. Mitigation/Plan

Consider how the CSO might mitigate against / reduce the impact of each potential risk and develop a response plan against each risk, should it happen.

4. Monitoring/Tracking

Review the progress of the plan regularly, to check - if a risk has occurred but was missed, if all of the risks remain relevant, if the level of individual risks remains the same or if there are any new potential risks to be added - this is the responsibility of the CSO's senior management, together with the board members.

5. Control/Report

Share the details of the risk plan with stakeholders, including donors, to keep them engaged, and keep them updated with risks arising, or amendments to the plan.

It is important for all CSOs to understand their 'threshold' for acceptable risk for the CSO, for its staff/volunteers, for its constituents, partners and other key stakeholders. Some CSOs may have the experience and capacity to work in moderate to high risk environments, while others may only have the capacity to work in low to moderate risk areas. It is important to understand the ability of the CSO to manage risk.

Risk management must be responsive to change – both within the CSO and in the external environment. Therefore, monitoring and reviewing the Risk Register must be on-going.

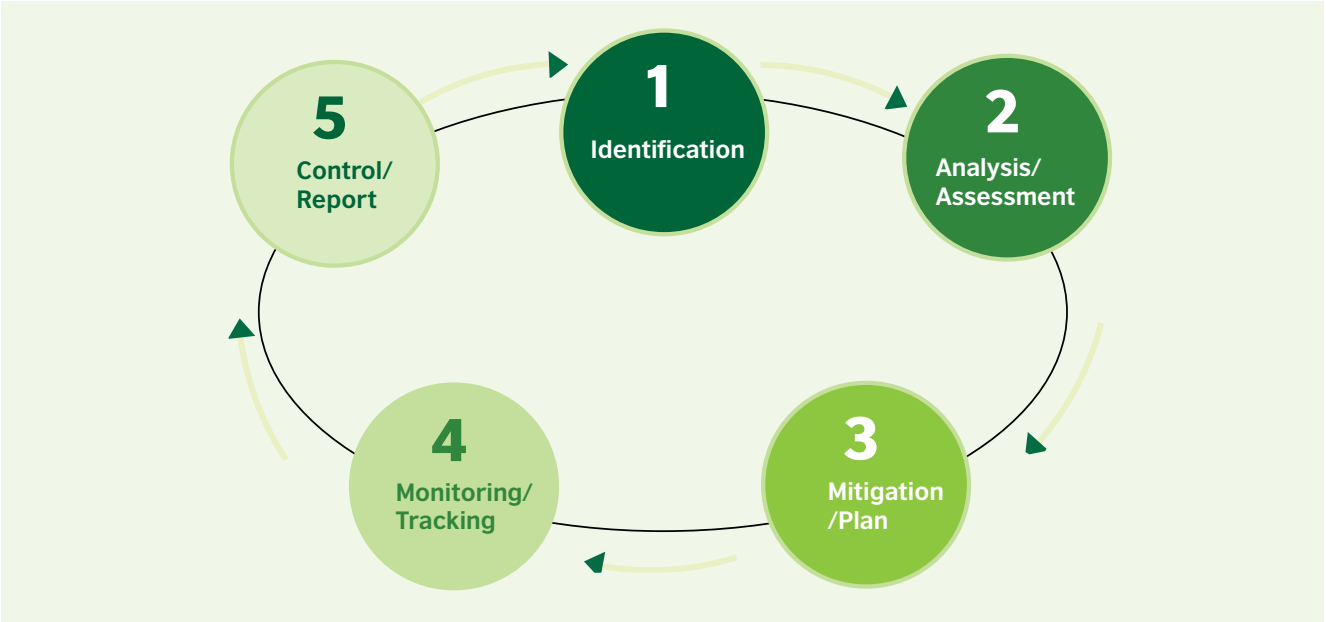
By monitoring risks, controls and plans, you can ensure that the risks are being managed in accordance with the Risk Management Policy and Framework. Monitoring is part of continual improvement and will enhance the CSO's value.

Formal review would look something like this:

- On a six-monthly basis, review the CSO's organisational Risk Management Policy, Framework and risk assessment criteria.
- On a six-monthly or quarterly basis (linked to your Board cycle), report to the Board with an update on the Risk Register, particularly for extreme or high risks.
- On a monthly basis (or whenever the senior management team meet) review risks and risk treatment plans, against the risk register.

Developing a list of stakeholders can help a CSO to:

- Identify those who will need to be involved in the identification, analysis and mitigation against risks
- Determine what information is shared with whom, and who should be consulted on which issues.



Typical CSO stakeholders may include:

- Board members
- Staff and Volunteers
- Constituents
- Funders/Donors
- CS partners
- Government Agencies (local/State/Federal)
- Community members
- Other locally based CBOs, CSOs, Networks, Associations, Unions
- Traditional Leaders
- Religious Leaders
- G&SI should be a key focus when engaging with stakeholders to ensure the risks facing the most marginalised people are given equal consideration

Steps to address risk management include the following:

- A deep understanding of the CSO's purpose, its constituents and context
- Develop a Risk Management Policy (see sample: Appendix I)
- Establish accountabilities (who is responsible for what)
- Integrate Risk Management into the CSO's processes, culture and values
- Involve the staff/volunteers so that they have ownership and buy-in which are essential to creating the culture
- Update/amend the Risk Management Framework, based on on-going learning, regularly

WAYS TO DEAL WITH RISK

(See the Risk Register section to plan actions to mitigate against risk.)

REDUCE

Reducing risk is possible by considering carefully the effects of a risk and planning actions that can be taken to mitigate against the effects of that risk. If it's not possible to reduce the probability of the risk, then focus on reducing its impact. Larger risks can become smaller risks, eg: by installing a fire or burglar alarm; by observing the speed limit and wearing seat belts. A CSO can reduce the risk of corruption through processes of due diligence.

TRANSFER

Transferring risk may be possible through taking out an insurance policy against a specific risk, eg: accidental damage. Working in partnership with others may also share the full impact of the risk.

ACCEPT

Acceptance acknowledges the inevitability of certain risks, and planning around the effects of the risk, by accepting full responsibility if there is no way it can be mitigated against. Accepting the risk is the most suitable approach when the potential severity of a loss is low, or if the cost of insuring the risk would be higher over time than the potential loss. Risk acceptance/retention is not the best strategy if the potential severity of the risk is high, particularly if it leads to unnecessary stress and worry if the CSO doesn't know whether it could absorb the potential effect.

AVOID

Avoidance may mean making a decision not to participate in activities that could harm the CSO in any way, as a result of a specific risk related to those activities. The problem is that whenever a risk is avoided, the opportunity to benefit from participating in the activity may also be missed, so this needs to be weighed up carefully. Also, not all risks can be completely avoided, such as climate change or natural disaster.

TYPES OF RISK[4]

CSOs have their own ways of categorizing and grouping types of risk. Below is the generic categorisation used for the NGOs and Risk study:

Risk Area	Definition	Examples
Security	Violence or crime	Kidnapping Armed attack on facilities
Safety	Accident or illness	Road accidents Fire in office COVID-19
Fiduciary	Resources not used as intended (fraud/theft/bribery)	Diversion of project materials Bribery of local officials
Information	Data loss, breach, or misuse	Theft of confidential financial information Breach of personnel data or other sensitive information Inappropriate communications by staff on social media
Legal/compliance	Violation of laws/regulations	Violations of employment or CSO regulations Violations of sanctions or counter-terror restrictions
Reputational	Action, information or perceptions damaging the CSO's integrity or credibility	Negative media stories Negative public statements or litigation by staff, ex-staff or stakeholders
Operational	Inability to achieve planned objectives	Human error Capacity gaps Financial management processes Resource gaps
Safeguarding	Putting children or vulnerable adults in danger	Power relations Sexual misconduct Inadequate duty of care
Ethical	Unfair and unequal practice	Nepotism Unequal opportunities for staff development or promotion Conflict of interest

[4]https://www.humanitarianoutcomes.org/sites/default/files/publications/ngo-risk_handbook.pdf

RISK REGISTER

A risk register builds a picture of the risks facing the CSO at a given time. It should be built from the project level upwards, through programmes projects, communications, management, legal requirements, financial/due diligence requirements, governance – to identify and rank potential risks within all categories.

These will inform the risk register, which is compiled at least once per year, and monitored closely (on a regular basis).

Once the risks are identified and prioritised (ranked), the process involves developing strategies to mitigate them, including outlining ways that procedures and practices may need to be adjusted.

Example:

Nature of Risk or Uncertainty	Likelihood: High/ Medium Low	Likelihood: High/ Medium Low	Scoring of Overall Impact High/ Medium/ Low	Actions required and who will take responsibility to manage the risk
The LGA feels suspicious of local CSOs and communities engaged in the project	M	H	H	Engagement with LGA during planning, monitoring and learning sessions to ensure engagement, collaboration and ownership throughout the project's lifespan.
Natural disaster - flooding	L	H	H	(This is largely unpreventable so focus on what can be done to reduce the impact.) Eg: Invest in flood doors and flood barriers for the CSO office. Plan for community meetings/ Town Hall Meetings to take place during the dry season.
Political insurgence	M	H	H	Engage with CS Networks to access early warning systems. Ensure an effective communication system to highlight potential danger with staff and key stakeholders.
Road accidents	M	H	H	Prevention strategies – such as driver training; regular vehicle checks, servicing; use of seat belts in front and rear, etc.
Health epidemic/ pandemic	M	H	H	Consider alternative ways of working/engaging within the CSO and at community level

GLOSSARY

Funder/Donor:

An individual or organisation that provides a CSO with funding. In this guide, the term "donor" generally refers to institutional donor agencies (eg: the EC, USAID, FCDO) or Foundations (eg: Macarthur) which advertise a 'call for proposals', review grant applications and select grant recipients. They each have their own development objectives to achieve, and CSO grantees can support them to achieve these. It is important to ensure that a CSO is not at risk of compromising on its own focus in order to fit with those of the donor.

Gender and Social Inclusion (G&SI):

A concept that addresses improved equal access for all, including women, girls, youth, poor people, people with disabilities, ethnic minority groups, older people, children, LGBTQI+, etc – those people who are traditionally excluded from development initiatives. G&SI supports inclusive policies and mindsets, and increases voice and influence by all.

Programme:

A programme can be defined as a group of related projects managed in a coordinated way towards the achievement of a CSO's Goal and Objectives. A programme is usually long term and comprises of a framework of related projects, that will contribute to its wider goal, outcome and objectives.

Project:

A (usually temporary and time-bound) set of activities, developed with the CSO's constituent group, to meet agreed objectives and deliver tangible outputs and outcomes that align with a wider programme and strategy, with agreed resources and monitoring plan.

Risk:

The likelihood and potential impact of encountering a threat.

Risk definitions:

Security risk: Physical risk to individuals and assets from acts of terrorism, violence and crime

Fiduciary risk: The risk that money or materials are not used for their intended purposes (eg: fraud, theft, corruption)

Legal/compliance risk: Technical or human error to comply with state regulation processes, or the CSO's constitution.

Operational risk: The risk of technical or human error, or capacity gaps, that lead to operational failure to manage the systems and processes within the CSO, its programmes or its projects, in line with its strategic plan – this can include mis-managing financial activities.

Informational risk: The risk of confidentiality breaches or data loss/theft.

Reputational risk: Damage to the CSO's image or reputation that results in future harm, losses or lack of support.

Ethical risk: The risk of harm caused by unethical behaviour, including unfair practice in relation to recruitment and selection, unequal opportunities for promotion, sexual misconduct, inadequate duty of care (staff or constituents), insufficient consideration of the CSO's values, actions that are not in line with organisational policies (eg: HR policy, Gender and Social Inclusion Policy, Safeguarding Policy, Conflict of Interest Policy, etc).

Risk management:	A formalized system for forecasting, weighing, and preparing for possible risks in order to minimize their impact.
Threat:	A danger or potential source of harm or loss.
Strategy:	The overarching CSO concept (Vision, Mission, Values, Goal and Objectives) under which their programmes/projects affiliated activities are designed, implemented and monitored.
Sustainability:	The potential for the impact created by the project to be sustained after the end of the project, typically without dependency on the CSO for further funding.

REFERENCES/SOURCES OF INFORMATION

Conflict and Health:
https://conflictandhealth.biomedcentral.com/articles/10.1186/s13031-021-00410-4

GISF NGO:
https://gisf.ngo/wp-content/uploads/2020/04/EISF_Security-to-go_guide_2020_Module-3.pdf

Humanitarian Outcomes:
https://www.humanitarianoutcomes.org/sites/default/files/publications/ngo-risk_handbook.pdf

Interaction.org:
https://www.interaction.org/wp-content/uploads/2019/03/Risk-Global-Study.pdf
https://www.juliantalbot.com/post/example-of-a-risk-management-policy

Management for Impact.com

Online Pictures:
Risk Mgmt: by unknown author is licensed under CC BY-SA
Risk Assessment by unknown author is licensed under CC BY-NC
Risk Management Framework by unknown author is licensed under CC BY-NC-ND
Ways to deal with risk by unknown author is licensed under CC-BY-SA-NC

Software advice:
https://www.softwareadvice.com/resources/5-steps-of-the-risk-management-process/

APPENDIX I

Policy documents should be concise –

> "A policy is a deliberate system of principles to guide decisions and achieve rational outcomes. A policy is a statement of intent, and is implemented as a procedure or protocol."
>
> Wikipedia

SAMPLE RISK MANAGEMENT POLICY:

(This document provides guidance only. As an example, It can be modified based on the CSO's needs.)

Overview

(Name of CSO) recognises that it is exposed to certain risks due to the nature of its activities and the environment in which it operates. The key to *(Name of CSO)'s* success is the effective management of risk to ensure its organisational objectives are achieved.

Risks arise due to *(Name of CSO)*'s operational undertakings and from external sources. Risks occur in numerous ways and have the potential to impact financial performance, reputation, health and safety, community and the overall performance of the organisation.

Policy

In order to fully understand such risks, *(Name of CSO)* has established a Risk Management Policy which provides the framework for how risk will be managed within the CSO. The Risk Management Policy forms part of the governance framework of the CSO. It also integrates with the strategic planning process. The Policy addresses both strategic and operational risks.

(Name of CSO) will use its skills and expertise to identify risks across the organisation and will also identify operational controls with which to manage risk.

(Name of CSO) will assess the size or degree of risk by taking into consideration the potential impact to its operations. Risks will be ranked in a common and consistent manner and a Risk Register will be maintained containing potential risks to the CSO.

Risk treatment/planned mitigation actions will be developed for risks which are unacceptable to the CSO. Risks, and the effectiveness of the risk management system, will be monitored on a regular basis and *(Name of CSO)* will communicate and consult with relevant stakeholders on its approach to managing risk.

Risk Tolerance

(Name of CSO)'s tolerance for adverse risks will be used to determine which risks are treated through the development of risk treatment/mitigation actions to manage risks to an acceptable level. During this process *(Name of CSO)* will consider additional control measures to manage the risks to acceptable levels, and these actions will be noted, monitored and modified as necessary in the Risk Register.

Integration with Governance and Strategic Planning

The Risk Management Policy forms part of the governance framework and integrates with strategic planning. The Policy addresses both strategic and operational risks and the requirement of *(Name of CSO)* to operate in its regulatory environment. Risk Management will be a key activity in all programme and project development and monitoring.

Accountability

Ownership of risks and risk treatment actions will be assigned to relevant roles within the organisation. *(Name of CSO)* has incorporated risk management accountability in executive, management and supervisory roles which are required to report on risks and risk treatment actions.

Risk Management Oversight

(Name of CSO)'s Board members and senior management will oversee the Risk Management Policy and the CSO's exposure to risk. Oversight of the effectiveness of the risk management processes and activities will provide assurance to the Board and stakeholders, and will support the CSO's commitment to continuous organisational improvement.

Reporting, Monitoring and Review

(Name of CSO) will monitor risks and mitigation actions on an ongoing basis. Performance of the risk management system and outstanding risk mitigation actions will be reported to the Board on a regular basis. Formal reviews of both the Risk Management system and the Risk Register will take place on an annual basis and the Board will assess the effectiveness of the Risk Management Policy annually; Project Risk Assessment and Risk Register

monitoring may take place at each Board meeting, or by Senior Management staff on a regular basis with reports to the Board, and in response to M&E reporting requirements.

Communication and Consultation

(Name of CSO) will communicate and consult with its stakeholders (internal and external) on its approach to risk management.

(Name and Signature)

ED/CEO

(Name and Signature)

Chair

Date Risk Assessment established:

Find out more
Agents for Citizens Driven Transformation (ACT)
ACT@ng.britishcouncil.org
www.justice-security.ng

Key contacts
National Programme Manager: Damilare Babalola@ng.britishcouncil.org)
Operations Manager: Maxwell Anyaegbu@ng.britishcouncil.org)

The Agents for Citizen-driven Transformation (ACT) programme works with civil society organisations (CSOs) to enable them to be credible and effective drivers of change for sustainable development in Nigeria. The four-year programme (2019-23) is funded by the European Union and implemented by the British Council.