RISK MANAGEMENT MANUAL

IRMG
Internal Risk Management Group

INTERNAL RISK MANAGEMENT GROUP

(IRMG)

FOR NGOS IN UGANDA

NOVEMBER 2020

FOREWORD

In mid-2018, a group of INGO Country Directors in Uganda came to the shared realization that the only way to mitigate fraud, corruption and safeguarding cases is through sector wide collaboration, cooperation and exchange of information. However, due to the sensitivity of these cases and the reputational risk involved, there was little joint learning, reflection and sharing of experiences among the NGO community.

A founding group of country directors decided to form the "Internal Risk Management Group (IRMG)", a safe space for NGO leaders to share, learn and improve their management and mitigation of risk. As of November 2020, the IRMG consists of 62 NGO members, celebrating the diversity of Ugandan and International NGOs operating in the country. IRMG is further recognized as a one-stop-shop for Donors to engage the NGO community in questions around fraud, corruption and safeguarding.

Under phase 1, the Department for International Development of the UK government (DFID), generously funded the IRMG to conduct a benchmark and baseline study of NGO Risk Management and Accountability Practices in the country, as well as to tailor and run training for IRMG member agencies to improve their understanding and ability to respond to internal risk in Uganda. It is for this reason that a manual was developed and commissioned to provide additional tips, practices, principles and supporting information to guide with strengthening the internal risk management processes in members' respective organizations.

ABOUT THE IRMG:

The IRMG Steering Committee is made up of nine NGO members who are elected on a yearly basis. The IRMG is currently chaired by Catholic Relief Services, and co-chaired by Plan International. Mercy Corps is the current grant holder for the initiative, and has managed both the DFID (Phase 1) and Sida (Phase 2) grants related to this project. Other Steering Committee members include DanChurchAid, Care International, International Rescue Committee, Reach out Mbuya, Finn Church Aid and Farm Africa. The IRMG committee is made up of Country Directors of these NGOs, who meet monthly to set the strategic direction for the initiative.

Contact

Niek de Goeij - CRS (Chair)
Country Representative | Uganda
niek.degoeij@crs.org

Iveta Ouvry - Plan International (Co-chair)
Country Director | Uganda
Iveta.Ouvry@plan-international.org

Carron Beaumont - Mercy Corps (Grant Holder)
Deputy Country Director | Uganda
cbeaumont@mercycorps.org

Henry Owora - Mercy Corps (Grant Holder)
Project Manager | Uganda
howora@mercycorps.org

TABLE OF CONTENTS

THE NGO INTERNAL RISK MANAGEMENT GROUP

Non-governmental organizations (NGOs) in general, and also in Uganda, face significant risks related to corruption and fraud in their operations. They also face challenges in terms of safeguarding beneficiaries and their staff. To mitigate these risks NGOs have invested significant human and financial resources to put in place internal risk management systems and other mitigating measures in order to operate in these challenging environments.

In mid-2018, a group of international NGO Country Directors in Uganda came to the shared realization that the only way to mitigate fraud, corruption and safeguarding cases is through sector-wide collaboration, cooperation and exchange of information. However, due to the sensitivity of these cases and the reputational risk involved, there was little joint learning, reflection and sharing of experiences among the NGO community leading to the establishment of the Internal Risk Management Group (IRMG) as a safe space for learning, sharing and improving mitigation and management of risk.

Under phase 1 of the program, the Department for International Development of the UK government (DFID),generously funded the IRMG to conduct a benchmark and baseline study of NGO Risk Management and Accountability Practices in the country, as well as to tailor and run training for IRMG member agencies to improve their understanding and ability to respond to internal risk in Uganda.

Under phase 2, Swedish International Development Agency (Sida)has allocated funds to continue providing support to NGOs operating in Uganda that are working to address internal risk management issues such as fraud and corruption, as well as funds to improve how NGOs prevent, mitigate and manage safeguarding issues.

The program has three expected outcomes:

1. Improve organizational culture around dealing with fraud and corruption by implementing the recommendations from the year one assessment of best practices and gaps on fraud and corruption prevention, detection and management.

2. Improve the safeguarding practices and reduce the risks of Sexual Harassment Exploitation and Abuse (SHEA) and child abuse in NGO programs.

3. Leverage lessons learned and knowledge base of the IRMG to benefit the wider civil society sector in Uganda to improve management ofmisconduct, implement safeguarding practices and establish preventative measuresagainst fraud and corruption.

RISK MANAGEMENT VOCABULARY

This manual makes use of the vocabulary and definitions as set out in ISO Guide 73:2009 Risk management – Vocabulary. For ease of reference, the main vocabulary used and associated definitions are set out below in alphabetical order.

Risk: The effect of uncertainty on objectives.

Risk acceptance: An informed decision to take a particular risk.

Risk analysis: A process to comprehend the nature of risk and to determine the level of risk.

Risk appetite: The amount and type of risk an organization is prepared to pursue or take.

Risk assessment: The overall process of risk identification, risk analysis and risk evaluation.

Risk avoidance: The decision not to be involved in, or to withdraw form, an activity based on the level of risk.

Risk evaluation: Aprocess of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable.

Risk management: The coordinated activities to direct and control an organization with regard to risk.

Risk management framework: A set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continuously improving risk management processes throughout the organization.

Risk identification: A process of finding, recognizing and describing risks.

Risk management plan: A document with the risk management framework specifying the approach, the management components and resources to be applied to the management of risk.

Risk management policy:The overall intentions and direction of an organization related to risk management.

Risk management process: The systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, identifying, analyzing, evaluating, treating, monitoring and reviewing risk.

Risk tolerance: An organization's readiness to bear risk after risk treatments (see Section 4.4.) to achieve its objectives.

Risk treatment: Aprocess of developing, selecting and implementing controls.

1. INTRODUCTION

Uncertainty and risk are an integral part of NGO operations, not only in Uganda but everywhere that NGOs are delivering humanitarian and development interventions. Uncertainty and risk are closely related, and their relationship needs to be understood if risks are to be managed.

Uncertainty as it relates to NGO operations typically results from insufficient knowledge of potential risks, including as it relates to value systems, organizational culture and societal norms. Recognizing that these uncertainties exist allows us to put in place the necessary measures to detect change and take proactive steps to manage unexpected circumstances. Uncertainty may lead to positive or negative consequences. Risk is associated with negative consequences. Risk affects the ability of organizations to achieve their objectives and, if not controlled, can have negative strategic, operational, financial and reputational outcomes. Thus, risks are the effect of uncertainty on an organization's objectives.

It is important to keep this in mind: risks pose a threat to organizational objectives, i.e., your organization's ability to deliver critical humanitarian and development interventions. Too often risks are thought of only as those events that have the potential to cause reputational damage or jeopardize current or future funding. This is in part because of donors' high level of sensitivity to the potential impact of negative news on public opinion in their home countries.

As a result, internal risk management is frequently thought of mainly in terms of minimizing the risk of corruption, fraud, and sexual harassment, exploitation and abuse (SHEA). The IRMG commissioned Study of NGO Risk Management and Accountability Practices in Uganda (RMAPU)found that NGOs in Uganda face significant risks related to corruption and fraud. They also face challenges in terms of safeguarding beneficiaries and staff. The types of risks faced by NGOs in the Ugandan context was not found to be significantly different from those in similar contexts. However, the severity and pervasiveness of these risks were found to be higher in Uganda.

To mitigate these risks, NGOs have invested significant human and financial resources to put in place internal risk management systems and other mitigating measures to operate in these challenging environments. However, the RMAPU Study found that in many cases these measures are standalone and not part of a holistic approach to internal risk management. Yet all activities of an organization involve risks. Effective internal risk management supports decision-making by considering uncertainty and its effect on achieving objectives and assessing what, if any, actions are needed to mitigate risk. As such, risk management should be integral to all aspects of NGO operations, including strategic planning, decision-making, operational planning and resource allocation.

Any approach to risk management is only as strong as its weakest link. NGOs that participated in the RMAPU Study almost all raised concerns as to whether implementing partners, who arecritical to the delivery of humanitarian and development interventions, have adequate systems to manage risks. Therefore, it is a major priority to strengthen the capacity of implementing partners contracted or sub-granted by grant holders on internal risk management.

To that end, this manual will provide guidance on how to put in place, as well as implement, a comprehensive approach to risk management. In doing so, this manual draws on *ISO 31000:2018 Risk management - Guidelines and IEC 31010:2019 Risk management — Risk assessment techniques. ISO 31000 provides the global standard for risk management while IEC 31010* provides guidance on the selection and application of techniques for assessing risk.

2. HOW TO USE THIS MANUAL

This manual is aimed at local and international NGOs in Uganda, regardless of whether they already have a comprehensive risk management system in place. If your organization does not yet have a comprehensive risk management system, this manual will guide you on how to design and implement one. For those that do, it provides a baseline against which to assess if your organization's risk management system meets global standards or if it requires further strengthening. This manual will provide staff within your organization with a solid understanding of the standards on risk management, techniques to improve how they approach it and its implications for operational and management decisions and actions.

For risk management to be effective it needs to be seen as and understood to be the responsibility of all staff within your organization. This manual should be understood by allstaff within your organization, not only management or those directly tasked with managing risk.

This manual is made up of three sections:

1. First, the principles for managing risk and the foundation and organizational arrangements that will allow you to effectively manage risk.

2. Second, the processes for managing risk, conducting risk assessment and implementing a risk treatment.

3. Third, suggested templates/tools and a list of resources and further readings if you wish to delve deeper into risk management and risk management techniques.

Recognizing that this manual will be used by a diverse range of NGOs with different levels of organizational and financial capacity, this manual is not prescriptive. What you choose to employ from this manual should match your capacity to successfully implement it.

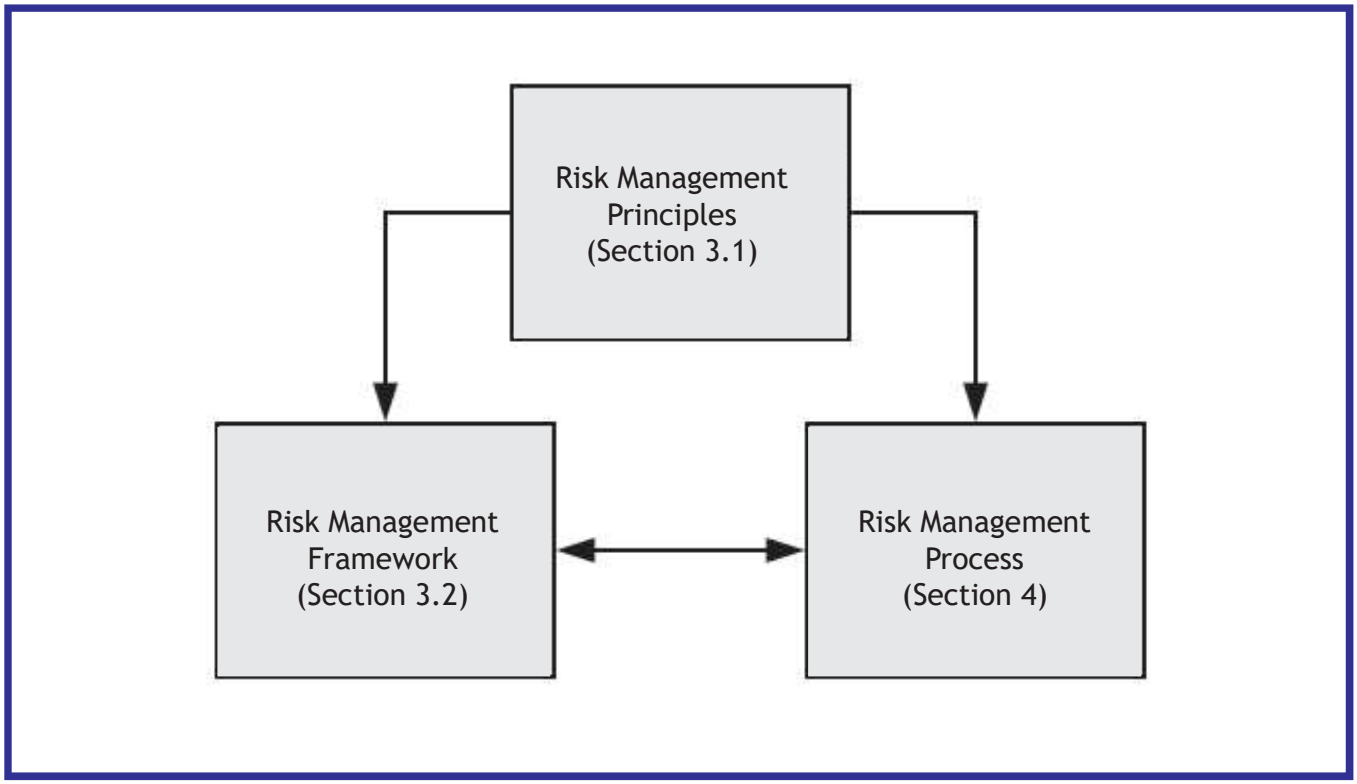
Also recognizing that several steps in the risk management resources could be costly for individual organizations, this manual highlights when relevant, where NGOs can draw on or pooled resources within the community.

3. WHAT IS RISK MANAGEMENT?

The purpose of risk management, in its broadest sense, is the creation and protection of value. The term value may be somewhat abstract in our context, but it is not value in an economic sense. For the purpose of this manual it should be understood to mean the humanitarian and development outcomes your organization is seeking to contribute to. If approached diligently, risk management helps improve performance and use of resources, encourages innovation and supports the achievement of organizational objectives. It will help in preventing poor decision-making, complacency and inadvertent exposure to potentially damaging consequences of your organization's activities. This, again, is why risk management should be part and parcel of all decision-making and operations.

As defined by *ISO 31000*, risk management consists of three interrelated components – principles, framework and process – as illustrated in Figure 1.

Figure 1: Components of Risk Management



While the underlying principles (covered in Section 3.1) of risk management should be expected to remain fairly constant, the risk management framework (covered in Section 3.2) and risk management process are likely to evolve as the nature of risks that your organization faces change an dlessons on what does and does not work are learned. Risk management is iterative and, if well implemented, will allow your organization to avoid risks increasing over time. This will happen through the interaction between the risk management framework and processes, when the framework has been designed to allow for continuous and incremental improvements.

While in many ways self-evident, it is worth setting out the expected benefits of putting in place a robust and comprehensive risk management system and associated risk management techniques. These benefits include:

- Establishing clear roles and accountabilities for managing risk of all staff in your organization.
- Providing structured information to support decisions and actions where there is uncertainty.
- Helping in setting realistic strategic and operational objectives.
- Determining risk criteria, including your organization's risk appetite.
- Taking risk into account when setting or reviewing priorities.
- Recognizing and identifying risk, including risks that could result in extreme outcomes.
- Understanding which uncertainties/risks matter most to your organization's objectives and providing a rationale for what should be done about them.
- Identifying effective and efficient measures to manage risk.
- Learning from success and failure to improve the way risk is managed within your organization.

While compliance may not be the most important aspect from the standpoint of achieving organizational objectives, remember that having a comprehensive risk management system in place is typically both a regulatory requirement and an expectation of your funding partners.

The next section will discuss the principles that need to underpin your organization's approach to risk management and the fundamentals of a risk management framework.

3.1. RISK MANAGEMENT PRINCIPLES

According to ISO 31000, the overall purpose and core principle of risk management is the creation and protection of value. It should not only help prevent or mitigate risk, but also improve organizational performance, encourage innovation and support the achievement of your organization's objectives.

Core principle: risk management must contribute to the creation and protection of value.

Risk management should help improve your decision-making processes and result in more efficient allocation of limited resources. Unfortunately, risk management systems can be viewed by staff as burdensome or an obstacle to getting their work done. If this is the perception,the risk management system is either not meeting the central principle (due to greater emphasis on protecting value at the expense of creation) or it has not been communicated well. In either instance, it should be a cause for concern and an immediate review of your approach to risk management.

Risk management should lead to the creation and protection of value – before moving on to the other principles if the exercise of managing risk is to be a meaningful one. This requires the continuous monitoring and review ofyour risk management system's performance, including soliciting the opinions of your beneficiaries, counterparts and staff.

The following principles should, as per ISO 31000, underpin your organization's approach to risk management:

- Risk management must be fully integrated: Risk management is not and should not be a standalone activity. It should be a central part of your organization's decision-making processes and help you in addressing uncertainty at all levels. It should be a shared responsibility among all staff and be aligned with other policies, procedures and standards within your organization.

- Risk management must be structured and comprehensive: Dealing with the uncertainty and risk your organization faces requires a structured, comprehensive and systematic approach. This will yield consistent and comparable results and will allow for the continuous improvement of your risk management system over time.

- Risk management must be customized to your organization's needs: This manual provides a comprehensive overview of what a risk management system could look like. However, not everything in this manual is applicable, or even suitable, to your organization's specific circumstances. Your approach to risk management must be customized and proportionate to your organization's external and internal context, risk profile and stated objectives. You must also ensure that you have the necessary human and financial resources to implement your risk management system, whatever shape it takes.

- Risk management must be inclusive: Your organization's ability to manage risk is dependent, to a great extent, on the range of views considered when assessing and treating risk. Ensuring the timely involvement of relevant stakeholders, from within and beyond your organization, will allow their knowledge and experience to be considered. This will lead to improved awareness and more informed risk management. It will also ensure greater awareness among stakeholders of your organization's approach to risk management.

- Risk management must be dynamic: The uncertainties and risks facing your organization will change over time. The risk management system you have in place today may not be appropriate for tomorrow. Because of this, your risk management system must be dynamic and able to identify and respond to change. It must also have a built-in capacity to improve over time through learning and experience.

- Risk management must be based on the best available information: If your organization's efforts to manage risk are based on incorrect or outdated information, it will be ineffective at best and counterproductive at worst. Inputs to manage risks must be based on the best available historical and current information, as well as projections for the future. Those responsible must be aware of and consider any limitations or shortcomings of this information when making decisions on managing risks. All relevant information should be made available to those involved in risk management (see inclusivity above).

- Risk management must consider human and cultural factors: Human behavior, culture and prevailing social norms are critical factors that shape the uncertainties and risksyour organization will face. They will influence how these uncertainties and risks are perceived and the ability of your organization to manage them. Your approach to risk management must be informed by a deep understanding of these factors and must consider theirpotential implications.

3.2. RISK MANAGEMENT FRAMEWORK

You need a risk management framework to help your organization integrate risk management into overall operations. As mentioned, for your approach to risk management to be effective it must be holistic and fully integrated into your organization's governance structure. Your organization's commitment to this and the principles outlined in Section 3.1. should be set out in your risk management policy. The risk management policy is an important tool for communicating your organization's intention and direction related to risk management.

The purpose of the risk management framework therefore is to lay out your organization's approach to and arrangements for managing risks. Your risk management framework will need to be customized to the needs of your organization. Also, it should be set out in a risk management plan which staff and relevant stakeholders should have access to and be familiar with. Again, the form of your framework document should suit the needs of your organization and could be more or less detailed. The larger the organization and the more complex the operations the more detailed the framework document should be.

What should go into your risk management plan? Before looking at the iterative aspects of the framework (i.e., how to design, implement, evaluate and improve our risk management processes) it is important to cover the fundamental aspects of leadership, commitment and the overall integration of risk management.

Leadership and commitment: The commitment of the leadership within your organization to take risk management seriously is essential if the risk management framework is to be successfully implemented. This commitment should be demonstrated through:

- Communicating the risk management framework to all relevant stakeholders and stressing the importance of it being adhered to. Management should reinforce this through leading by example. This means ensuring that uncertainties and risks are fully considered when setting organizational objectives and that appropriate measures are in place to manage risks and putting risk managementfront and center in management decision-making processes.

- Ensuring that there are necessary resources allocated to fully implement the risk management framework (too often risk management has failed due to insufficient resourcing, signaling that it is in fact not a priority for management).

- Assigning roles and responsibilities for overseeing and managing risks within the organization, while emphasizing risk management is the responsibility of all staff. Making contributions to risk management a part of staff performance assessments can be an effective way of driving home this point.

Integration: How risk management is integrated within your organization will depend on your organization's specific purpose, goals and complexity. As has been stressed, there is no one-size-fits-all solution. While the fundamentals should be the same, the actual implementation will differ depending on the needs of each organization. Your framework document must consider that:

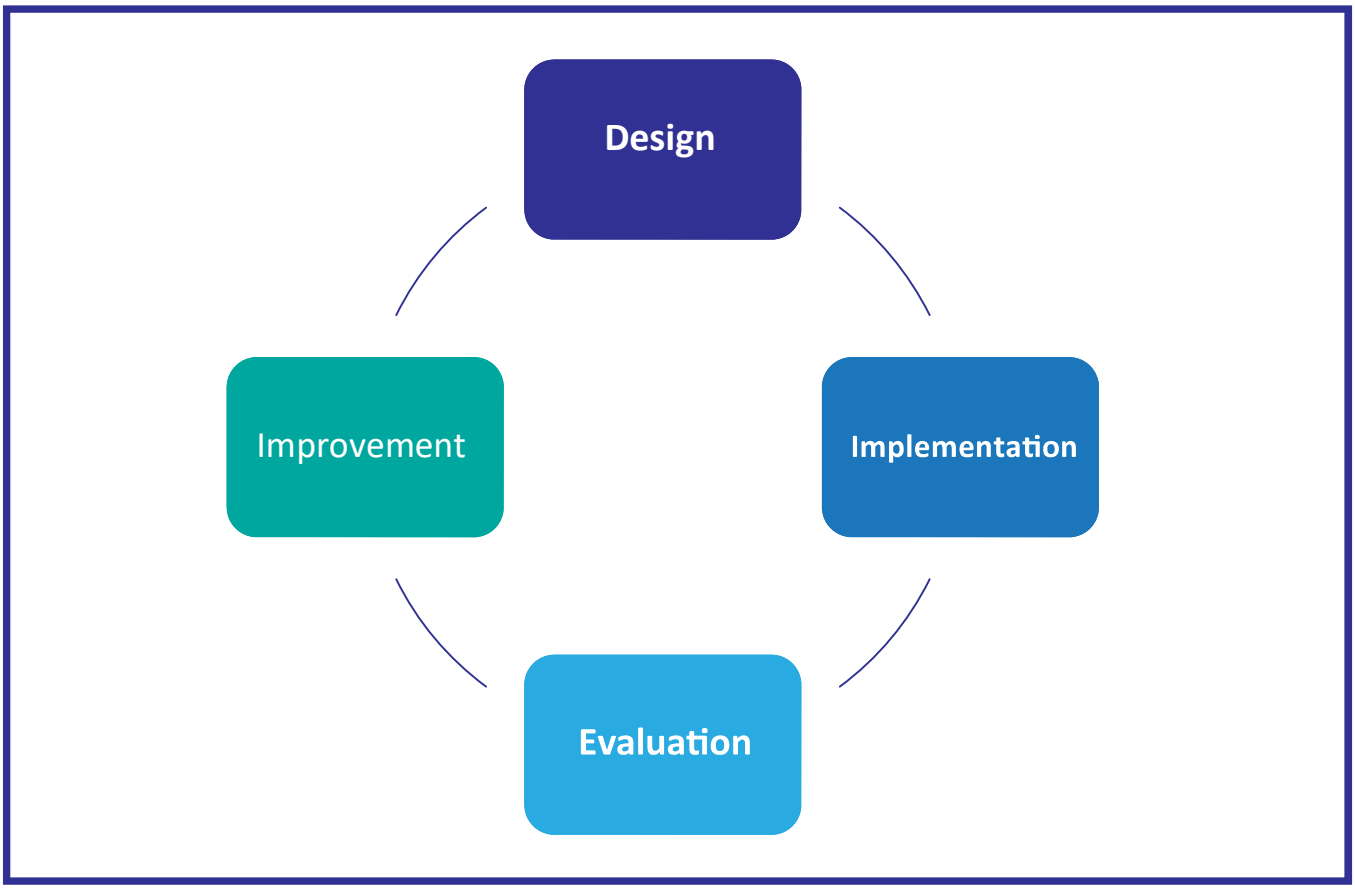
- Uncertainty and risk need to be managed at all levels and in all parts of your organization. Integrating risk management therefore requires a thorough understanding of your organization's structure and context.

- Governance guides your organization and management structures translate governance directions into implementation. Determining where accountability and oversight for risk management rest within your organization is therefore an essential part of integration.

- Risk management should be adopted to your organizational culture and therefore part of its governance, management, strategy, objectives and operations.

While leadership and commitment, along with integration, should serve as the foundation for your risk management framework, it will also need to cover the actual steps of managing risk. This should consist of four steps: design, implementation, evaluation and improvement. As illustrated in Figure 2, these steps are not linear. They form part of a cycle where experience and lessons learned from implementation should feed into the continuous improvement of your organization's risk management system.

Figure 2: Steps of Risk Management Framework



Your organization's risk management system is unlikely to be effective unless sufficient attention is given to the design step. While an upfront investment and effort to get it right, your risk management system should, over time, yield a significant positive return. While details on the design step (as well as the subsequent three steps) will be covered in Section 4, overall your risk management framework should provide for:

- Examining your organization's external and internal context.
- Mapping out and assigning organizational roles, authorities and responsibilities.
- Determining the resources needed in terms of staff time, capacity development of staff, processes and procedures as well the associated funding requirements.
- Communication and consultation with staff and stakeholders so that your organization's approach to risk management is informed by a diverse a knowledge base, as well as ensuring broad awareness on your organization's approach to risk management.

Implementation: While the design phase is certainly critical, it is through implementation that the measures you have put in place will make the real difference. Your risk management framework should facilitate implementation through:

- Providing an implementation plan, including timelines and resources.
- Specifying where, when, how and by whom different types of decisions should be taken across your organization (including provisions for modifying decision-making processes when and if necessary).
- Ensuring that all staff and relevant stakeholders are aware of and understand your organization's risk management system, and that it should be practiced by everyone within the organization.

Evaluation: Only through rigorous and regular evaluation will it be possible for you to know whether your organization's risk management system is working as it should. Your organization's risk management framework should provide for regular evaluations of the performance of your organization's risk management system against its stated purpose, implementation plan and indicators (realistic and measurable criteria against which to measure progress). Based on these evaluations you will be able to determine whether the risk management system remains suitable for achieving your organization's objectives or if changes/improvements need to be made.

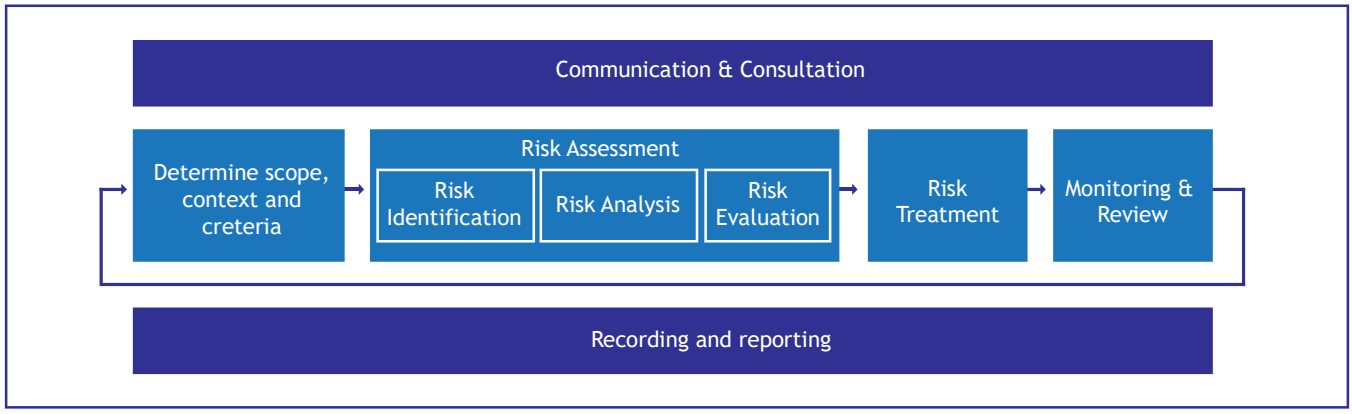
Improvement: Based on the findings of your regular evaluation, and considering internal and external changes, your organization's risk management system will need to have the flexibility to adapt and improve. A static risk management system will quickly become ineffective, so your framework needs to build in provisions to ensure that it can to be adaptive and continuously improved. This should include assigning responsibility for ensuring that measures to adapt and improve are fed into the (re)design phase and carried through to implementation.

4. WHAT DOES THE RISK MANAGEMENT PROCESS LOOK LIKE?

The risk management process allows us to recognize, understand and manage the uncertainties and risks that our organizations face. It is the comprehensive set of activities you will carry out to identify, assess, manage and monitor risk.

This section will cover the different steps of the risk management process, as illustrated in Figure 3. These steps can be applied at the strategic, program and project level. Like the framework, the risk management process is a cycle, with each step building on the previous one and through rigorous monitoring and review. While the steps are presented sequentially, they are to be applied iteratively. That is to say the practice of risk management involves moving back and forth between the different steps as circumstances may change and lessons are learned. In addition, communication and consultation as well as recording and reporting run throughout as crucial supporting steps to both inform and document the risk management process and its implementation.

Figure 3: Risk Management Process



The next section describes what each of the steps of the risk management process involves and covers techniques that your organization can use at each step.

4.1. COMMUNICATION AND CONSULTATION

Effective communication and consultation are critical to a well-functioning risk management process. Together they will ensure awareness, understanding and engagement in the process by internal and external stakeholders.

Your risk management process must not be treated as a closely guarded secret. There needs to be a concerted effort put forth to ensure that all staff within your organization are aware of the risk management process and the role they have to play in it. When relevant internal and external stakeholders have insight into what your organization's approach to risk management entails, they will know what to expect. If they lack this insight, there is a risk that they may become mistrustful of actions taken by your organization. This is a particular challenge in contexts such as Uganda, where corruption may be considered the norm rather than the exception and any action may be seen through that lens. Being aware of the process will allow your stakeholder to understand the reason behind decisions and actions taken.

Make your organization's risk management plan publicly available. It is highly unlikely to pose a security risk or be of assistance to anyone trying to hinder your efforts so the benefits of making it accessible greatly outweigh the risks. This should however not necessarily extend to the specific risks identified or the particulars of your risk treatment plans, as these could potentially negatively impact your relationship with external stakeholders who are themselves identified as risks or subject to risk treatment.

Broad consultations with relevant internal and external stakeholders as part of the development and implementation of your organization's risk management system will provide an expanded knowledge base and help to ensure:

- That different fields of expertise are brought together and heard at each step of the risk management process.
- That the views of different stakeholders are understood and considered when defining risk criteria and evaluating risks.
- That there is sufficient information to allow for effective risk oversight and decision-making.
- That there is a sense of common ownership among those affected by the risk identified.
- That there is buy-in to the overall process, as well as treatment plans, and the necessary resources will be available.

Given its importance, your organization may want to develop a strategy for consultation, along with a plan for communicating reliably, accurately and transparently to external stakeholders throughout the risk management process.

4.2. DETERMINING SCOPE, CONTEXT AND CRITERIA

For the risk management process and system to be effective,you must first determine the scope, context and criteria.

First, you will need to determine your organization's objectives, as risk is the effect of uncertainty on objectives. It's likely you already have your organization's objectives defined in your strategic or programmatic documents. If you do not, going through this step of the risk management process has the added benefit of prompting your organization to explicitly state its objectives. Your organization's objectives will change over time and you will need to take this into account when you iterate the risk management process.

Second, you will need to determine the stakeholders, internal and external, that are relevant to the risk management process. These should include:

- Stakeholders who have a role to play in managing risk.
- Stakeholders who may be affected by the risk.
- Stakeholders whose knowledge, information and views are relevant to the risk management process.

These are the stakeholders you should consult with throughout the risk management process, and with whom communications on the risk management process should be shared. (see Section 4.1.).

You will also want to identify the stakeholders that may be the cause of risk to your organization (e.g., potential sub-grantees that do not have sufficient internal controls). In some cases engaging with these stakeholders will be part of managing risk. In others, it is simply a matter of knowing who to monitor as you move forward with interventions and activities.

Next,establishing the scope of your risk management process should include defining the depth and level of detail in your risk assessment, explicitly stating what should be included. Whether your organization is laying the foundations of your risk management system or reviewing an existing risk management system your initial scope would likely be at the operational/programmatic level.

Once you have established the scope of your risk management process you will need to have a solid understanding of the context. This means that you need to thoroughlyunderstand the environment in which your organization seeks to achieve its objectives. The internal context (i.e., within your own organization) is as important as understanding the external context.

When seeking to understand the internal context you should consider:

When seeking to understand the internal context you should consider:

- Governance, organizational structure, roles and accountabilities.
- Organizational culture.
- Existing rules, regulations and guidelines.
- Organizational capability in terms of resources and knowledge, including staff, available budget, processes and systems.
- Relationships with internal and external stakeholders.
- Existing contracts, agreements and commitments.

When seeking to understand the external context you should consider:

- Social, cultural, political, security, legal, financial and environmental factors. In the Ugandan context this is not limited only to the national and local level. Changes in the region have the potential to have a tremendous impact (e.g., as a result of conflict and the resulting cross border movement of refugees). The international level should also be considered as it can impact on the availability of funding for your organization.
- Relationships of external stakeholders and what are the likely motivations driving their decisions.
- Existing networks and power structures within your area of operation.

Throughout your efforts to understand the internal and external context it is critical that you put the human aspect front and center. Ultimately, your organization's ability to manage risk will only be as strong as the commitment of those responsible for managing the risk. This is particularly important in the Ugandan context where the pervasiveness, and to some extent acceptance, of corrupt behavior may result in a greater acceptance of risk. Recognizing that norms and behaviors, as well as the organizational culture, internally and externally are critical elements of your operating context is crucial.

While it is inevitable that you will have to carry out the analysis of your organization's internal context, consider exploring opportunitiesto partner with other organizations to carry out the analysis of the external context. If other organizations have already carried out an analysis of the external context you can also request that they share them with you in order to avoid unnecessary duplication.

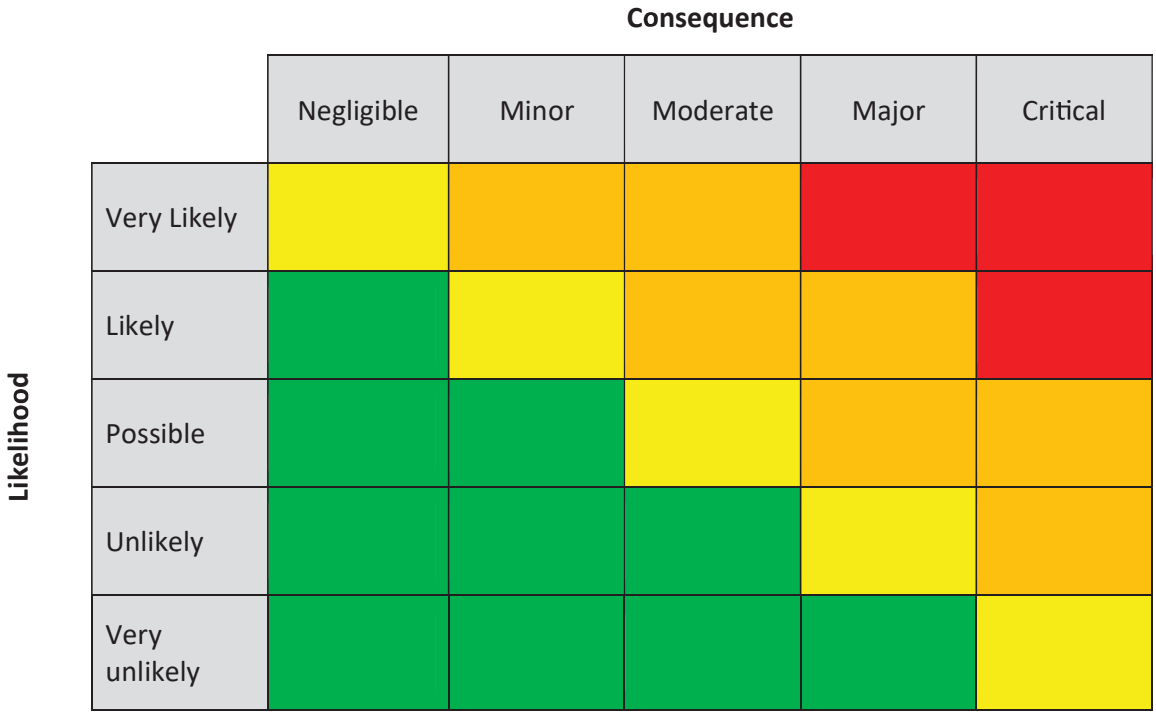
Finally, you will need todetermine risk criteria. Your organization will need to decide on the amount and type of risk that is considered acceptable given the objectives that you seek to achieve. By virtue of operating in the Ugandan context, your organization has already, knowingly or unknowingly, demonstrated a relatively high appetite for risk.Similarly, your organization's risk tolerance might also be assumed to be relatively high by others.

Nevertheless, there will be risk levels that are simply too high for both your organization's risk appetite and risk tolerance. Establishing risk criteria for your organization will allow you to recognize when that level has been exceeded. A consequence-likelihood matrix is a useful and straightforward tool that can help you determine whether a particular risk is at an acceptable level or not.

A consequence-likelihood matrix (also known as a risk matrix) is designed to allow you to determine the likelihood of a risk occurring and how serious the consequences will be if it does. As shown in the example of a consequence-likelihood matrix in Figure 4, the seriousness of the consequences of a risk occurring increase along the x-axis, and the likelihood of the risk occurring increases along the y-axis. It is up to you to decide how many levels you want to include on each axis, but consider making use of the following levels/categories:

In our context, assessing the consequence and likelihood of a risk occurring is not an exact science. The data that will inform your assessment is more likely to be qualitative than quantitative. As such, a certain level of subjectivity is unavoidable. It is necessary to provide a narrative description of what each level/category entails and ensure that all those involved in carrying out the risk assessment have a shared understanding of these categories.

Figure 4: Example of Consequence-Likelihood Matrix



The colors in Figure 4 represent the overall level of risk (i.e., consequence + likelihood), with red indicating extreme risk, orange indicating high risk, yellow indicating medium risk and green indicating low risk. The example in Figure 4 would be reflective of an organization with a relatively high level of risk appetite. If your organization instead has a medium to low level of risk appetite there would be more red squares and fewer green. Your organization will also need to establish criteria on what actions need to be taken depending on the overall level of risk, including risk treatment (see Section 4.4.) and escalation (see Section 4.3.).

Recommended techniques for establishing scope, context and criteria for your risk management process include internal brainstorming, workshops and interviews that include external stakeholders and, if relevant, surveys. You should also survey existing research and materials. This would include exploring whether other organizations have carried out analysis of the external context that you can use.
In all these steps, it is inevitable that a certain level of subjectivity will creep in. It is important to keep an eye out for potential biases resulting from group think or over-confidence in one's knowledge about the context or risks. Expert opinions and the inputs of staff from within your own organization should be complemented to the extent possible by other sources of evidence and data. This is again, why it is so important to conduct consultations with a wide range of stakeholders, in order to gain as broad a perspective as possible.

4.3. RISK ASSESSMENT

With the scope, context and criteria established, you are ready to move ahead with the next step of the risk management process – the risk assessment. The risk assessment consists of the identification, analysis and evaluation of risk. Throughout the risk assessment step, it is important that you apply a systematic, iterative and collaborative approach. With your internal and external stakeholders in place, you'll need to make use of all the information that you have available. If this is not sufficient you will need to supplement it with further inquiry.

4.3.1. RISK IDENTIFICATION

The first step of your risk assessment is to identify the risks your organization is facing. This means identifying, recognizing and describing the risks that potentially stand in the way of your organization achieving its objectives. The main questions to consider when identifying potential risk are:

- What uncertainty exists in your organization's context and what might its effect be?
- What occurrences or issues could have negative consequences for your organization?
- What sources of risk exist (that you are already aware of) and which may develop?
- What controls or treatments does your organization already have in place?
- What is your organization's past experience and what lessons might it hold for the future?
- What are the human and organizational factors that you need to consider (think norms, behaviors, values and culture)?

The questions listed above do not only draw on your organization's past experience but also seek to identify new and emerging uncertainties and risks. Known risks or those you can anticipate based on past experience need to be managed but you are likely already taking measures to mitigate them. New risks on the other hand have the potential to catch your organization off guard. This is why having a forward-looking perspective is such an important part of your risk identification efforts. The questions listed above can form the basis of a checklist that can be utilized when identifying potential risks.

In identifying risks there can be a tendency to focus on the risks that, to at least some extent, are within the control of your organization. This must be avoided as you need to identify all potential risks. If these risks are beyond the control of your organization, it is particularly important that you are aware of them in your decision-making and planning process.

The context your organization operates in is dynamic (hence the need to be forward-looking), which means that you may not identify all risks initially or new ones may emerge after you have completed your risk identification. You need to be continuously scanning for potential emerging risks through monitoring and review of your risk management process (see Section 4.5.) and recording and reporting (see Section 4.6.).

In answering the questions above, you may wish to divide up the potential areas of risk to make the process more manageable. While the categories you select may differ, consider the following as a starting point, taking the Ugandan context into account:

- Contextual risks:Risks that are external to your organization, and typically outside of your organization's control. These will be identifiedby thoroughly analyzing the external context (see Section 4.2.). While they may be outside of your organization's control, you will still need to understand and prepare for them. These could include the possibility of conflict in a neighboring country resulting in the displacement of populations or severe drought causing food insecurity.

- Programmatic risks:Risks that have the potential to impact on the delivery of your organization's programs, projects and activities (falling somewhere in between contextual and organizational risks). While not always fully within your organization's control, these risks would be managed through strong situational awareness, robust operating procedures, clear accountabilities and effective oversight.

- Organizational risks:Risks that are internal to your organization with the potential to cause damage to the health and safety of your staff, the reputation of your organization, or loss of funding. These risks are very much within the control of your organization to manage and should be treated with robust oversight, finance and human resource management mechanisms.

After identifying all the potential risks, you need to identify and assess your organization's existing risk management controls. In assessing their effectiveness, you should consider the following:

- How are existing controls meant to modify risk?

- Are the controls in place working as intended and achieving the expected results?

- Are there shortcomings in how your controls are designed or applied?

- Are there gaps in your organization's existing risk management controls?

- Do the controls that your organization has in place function independently or do they need to function together to be effective?

- Are there conditions, vulnerabilities or circumstances that have the potential to reduce the effectiveness of your organization's risk management controls?

- Could existing risk management controls themselves result in the emergence of new risks?

Assessing the effectiveness of your organization's existing risk management controls can be a potentially sensitive exercise, with internal stakeholders holding on to old ways of doing things or feeling that their performance is being questioned. Here, management needs to play a role in creating an environment where stakeholders feel comfortable to have a frank and honest discussion. Let the questions above serve as a checklist to guide this conversation.

Make sure that you have put in place a systematic and detailed methodology for capturing the results of your risk identification exercise. With this in place, you will be able to move ahead to the next step of analyzing the risks you have identified.

4.3.2. RISK ANALYSIS

You have now identified the risks that may have an impact on your organization, you have categorized the risks and you have a good understanding of your organization's existing risk management controls. Now you must analyzeeach risk.

While risk analysis can be a highly technical discipline, you should keep in mind that our analysis will be based primarily on qualitative data. Try to keep your analysis as simple as possible, seeking to determine:

- The likelihood of the risk occurring.
- The potential consequences should the risk occur.
- The effectiveness of existing controls in managing the risk identified.

Having determined the likelihood and potential consequence of a risk occurring you will be able to plot your organization's risks into your consequence-likelihood matrix, determining your organization's overall risk profile. Your risk analysis will serve as a basis for your risk evaluation, as well as decisions on whether a risk needs to be treated or not, and what the most appropriate risk treatment would be.

Given the type of data that will serve as the foundation for your risk analysis, there is a risk of subjectivity, including underestimating or overestimating the level of risk. To mitigate this, consider sharing your risk analysis with peer organizations to get their unbiased feedback on whether you have gotten it right or not.

4.3.3. RISK EVALUATION

Having identified and analyzed the risks facing your organization, you will now need to evaluate the risks. This will allow you to make decisions on which risks require treatment, which do not, and those risks that fall outside the scope of your organization's risk appetite whether they are treated or not.

Based on your analysis you will have plotted the risks you have identified in the consequence likelihood matrix (see Figure 4). Depending on how you have determined your organization's appetite for risk (see Section 4.2.) you will know whether the level of risk is extreme, high, medium or low. Based on this you will need to decide whether to:

- Do nothing further, i.e., no actions are needed to control the risk.
- Consider possible risk treatment options, when there are no controls in place or existing controls are not sufficient.
- Carry out further analysis, where the risk is not yet fully understood.
- Maintain existing controls, i.e., the residual risk with existing controls is at an acceptable level.
- Reconsider your organization's objectives, interventions or activities where the risk is simply too high.

Depending on your organization's risk appetite and considering whether the benefits of a particular course of action outweigh the risks (i.e., a cost-benefit analysis) you will need to decide what is the right course action for different risk levels. Consider the following to help guide you:

- Extreme level of risk: Take immediate action to manage risk and limit exposure. This level of risk would generally not be accepted or retained.
- High level of risk: Carry out a cost-benefit analysis to determine whether to treat the risk. Typically, this level of risk would only be accepted or retained when there is a significant potential benefit of moving forward.
- Medium level of risk: Apply treatment and carry out continuous monitoring of the treatment to ensure that the risk is kept at an acceptable level.
- Low level of risk: Manage through regular processes and procedures as the risk is not sufficient to warrant the investment of additional resources.

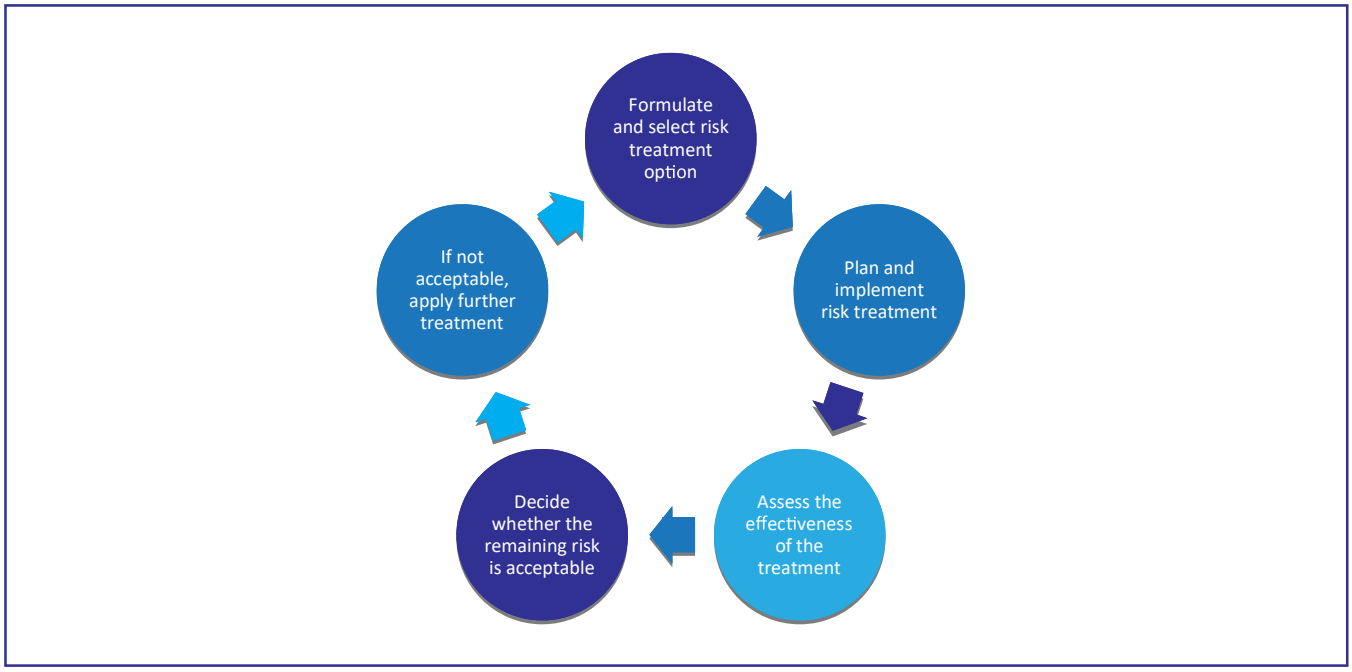
Regardless of your decision on whether to accept or retain a risk and if treatment is needed, all risks should be documented with a rationale for the decision.

In Annex 1 you will find a suggested template for a risk register. You will likely wish to enter the suggested fields into an excel sheet for simple entry. This risk register template (or any other risk register template your organization may utilize) will allow you to document your organization's risk assessment process, track developments over time, as well as ensure that your risk treatment measures (as detailed in the next section) are proportionate to the risks identified.

4.4. RISK TREATMENT

When a risk is considered to be at an unacceptable level you will need to apply a risk treatment. The risk treatment process, like the other steps in the risk management process, is not linear. You likely have to revisit your risk treatment multiple times, either because it has not sufficiently reduced the risk or the risk itself has changed. Figure 5 shows the five steps (the first two will be covered in detail) of the risk treatment process and how they relate to each other.

Figure 5: Risk Treatment Process



Selection of risk treatment options: Selecting one or more risk treatments (sometimes one will not be sufficient) involves weighing the potential benefits of an intervention against the cost of implementing it and the implications if itdoes not sufficiently mitigate the risk. Possible options for treating risk include:

- Avoiding the risk by not going ahead with the planned intervention or activity that gives rise to the risk.An example of this would be to not proceed with an intervention that would require direct transfers to a host government institution where the risk of corruption is thought to be significant.

- Accepting the risk after determining that the potential benefits of proceeding with the intervention or activity far outweigh itsnegative impacts.An example of this would be delivering life-saving humanitarian aid despite the risk of some of it being diverted by rogue actors.

- Removing the source or cause of the risk.An example of this would be moving to electronic moneytransfers if there is a risk of fraud when making cash payments to beneficiaries.

- Reducing the likelihood of the risk occurring.An example of this would be introducing a policy of preventing SHEA, raising awareness among all relevant stakeholders on the policy, and introducing a hotline to report incidences of SHEA.

- Sharing the risk with another party or parties.Typically this would be understood to be insurance, but in our context another example could include shared risk of entering into a contract with a funding partner if your organization will be implementing an activity with known risk at the request of the funding partner.

From the examples above you can imagine how some of the risk treatment options may be complementary. For example, your organization may decide to proceed with delivering life-saving humanitarian aid because of the perceived benefits and because the risk is shared with a funding partner.

While risk treatment is often determined by economic consideration in the private sector (i.e., the impact on the profit margin), this is less of a concern in our context. It is more important that the risk treatment isaligned with your organization's objectives, risk criteria and available resources. It is worth restating that the cost of the risk treatment needs to be weighed against the benefits it is likely to deliver, i.e., will it help your organization deliver on its objectives while mitigating risks at a manageable cost. You should also consider the following when selecting the most suitable risk treatment options:

- The cost, financial and otherwise, of implementing the risk treatment.

- The feasibility of implementing the risk treatment and how likely it is to mitigate the risk.

- The potential impact of the treatment on your stakeholders' values, perceptions and interests as some risk treatments may be more acceptable to your stakeholders than others – refer to Section 4.1., communication and consultation with your stakeholders will help in guiding you on this.

- Whether the risk treatment is in conflict with legal, regulatory or other obligations your organization may have.

- The possible unintended consequences of the risk treatment itself may have an impact on other existing risks or may give rise to new (secondary) risks.

Plan and implement risk treatment: The purpose of a risk treatment plan is to detail how the risk treatment will be implemented and how its progress can be monitored. Thismust be understood by all those involved. As with other aspects of the risk management process, your organization's risk management plans should be integrated into the overall management and decision-making processes.

Your risk treatment should include the following:

- The risk being treated and the risk treatment(s) chosen to mitigate it.
- The rationale for choosing the risk treatment(s).
- Which individuals will be accountable and responsible for approving and implementing the treatment plan.
- The proposed actions to be taken, including timelines and the sequence in which actions should occur.
- All resources required to implement the treatment plan.
- How the implementation and effectiveness of the risk treatment is to be measured, i.e., performance measures.
- Requirements in terms of reporting and monitoring on the implementation of the risk treatment plan.

Annex 2 provides a template for what a risk treatment plan could look like. You may also wish to consult with other organizations on what template they use and, if it better suits your needs, borrow it.

Once the implementation of your organization's risk treatment plans isunderway you will need to revisit them regularly to monitor and review progress (see Section 4.5.) and to determine whether they are achieving the intended results. You should expect that there will be a need to revisit and adjust your risk treatment plans on multiple occasions as the context within which you are operating changes.

4.5. MONITORING AND REVIEW

As has been noted throughout this manual, risk management cannot and should not be static, as the risks your organization faces will change over time. Unless your response to risk includes mechanisms that allow it to adapt to changing circumstances, it will quickly become outdated, ineffective, and hinder your ability to assess the performance of your risk management process. Avoid this by building in rigorous and regular monitoring and review of your organization's process.

Monitoring and review will allow your organization to maintain and improve the quality and effectiveness of all stages of your risk management process. While necessary to consistently review the overall performance of your risk management system, it holds particular relevance for the risk assessment stage of the process as monitoring and review will allow for:

- Comparing actual outcomes with the results that you had predicted at the risk assessment stage, allowing for improved assessments in the future.
- Gathering data that you can use to gain a better understanding of risk.
- Scanning for new risks and unexpected changes that would indicate that you need to update your risk assessment.

Monitoring and review of the risk management process must also be built into your organization's overall performance management, measurement and reporting activities. As such, it is part of the responsibility of those within your organization performing the monitoring and evaluation function. The results should also inform the thinking of your organization's senior management in the overall planning and decision-making processes.

While each organization will have to determine the regularity with which the risk management process is reviewed, it is necessary to brief management with regular up-to-date information on risks and the implementation of risk treatment plans. At minimum (although it could be more frequent given the specific circumstances of your organization's risk profile) consider:

- Reviewing your organization's risk management framework and plan on an annual basis.
- Reviewing your organization's risk register and risk treatment plans on a quarterly basis.

4.6. RECORDING AND REPORTING

Given its iterative nature, it is necessary that you put in place mechanisms to document and report on your organization's risk management process and its outcomes. Recording and reporting will allow you to:

- Communicate on your risk management activities and outcomes across your organization.
- Ensure management is fully informed of the risk management process and provided the necessary information for decision-making.
- Monitor, review and improve risk management activities (see Section 4.5.).
- Help you in communicating and interacting with relevant external stakeholders (see Section 4.1.).

Your risk treatment should include the following:

- The risk being treated and the risk treatment(s) chosen to mitigate it.
- The rationale for choosing the risk treatment(s).
- Which individuals will be accountable and responsible for approving and implementing the treatment plan.
- The proposed actions to be taken, including timelines and the sequence in which actions should occur.
- All resources required to implement the treatment plan.
- How the implementation and effectiveness of the risk treatment is to be measured, i.e., performance measures.
- Requirements in terms of reporting and monitoring on the implementation of the risk treatment plan.

Annex 2 provides a template for what a risk treatment plan could look like. You may also wish to consult with other organizations on what template they use and, if it better suits your needs, borrow it.

Once the implementation of your organization's risk treatment plans isunderway you will need to revisit them regularly to monitor and review progress (see Section 4.5.) and to determine whether they are achieving the intended results. You should expect that there will be a need to revisit and adjust your risk treatment plans on multiple occasions as the context within which you are operating changes.

4.5. MONITORING AND REVIEW

As has been noted throughout this manual, risk management cannot and should not be static, as the risks your organization faces will change over time. Unless your response to risk includes mechanisms that allow it to adapt to changing circumstances, it will quickly become outdated, ineffective, and hinder your ability to assess the performance of your risk management process. Avoid this by building in rigorous and regular monitoring and review of your organization's process.

The tools for recording your risk management process, activities and outcomes have been covered in the preceding sections and include:

- Your organization's risk management policy and plan.
- Your organization's risk treatment plans.
- Your organization's consequence-likelihood matrix.

In line with your communication plan (see Section 4.1.), you will need to set out a plan for reporting, which includes how to report, to whom and with what frequency.

ANNEX 2: RISK TREATMENT PLAN TEMPLATE

Risk #	Risk description	Risk category	Controls in place	Likelihood	Consequence	Risk level (likelihood + consequence)
	Provide a description of the risk identified.	*Assign a category to the risk identified (in accordance with the categories that your organization has determined).*	*Provide a description of current controls in place to manage the risk.*	*Assign a value for the likelihood of the risk occurring (using the categories set out in Section 4.2.).*	*Assign a value for the consequence should the risk occur (using the categories set out in Section 4.2., if found appropriate to your organization's context).*	*Assign the overall risk level for the untreated risk (making use of the risk levels as defined in your organization's consequence-likelihood matrix (see Figure 4).*

Column 8-14:

Primary risk owner	Secondary risk owner	Mitigating actions (treatment plan)	Residual likelihood	Residual consequence	Residual risk level (likelihood + consequence)	Additional actions
Identify who has the main accountability for the risk.	*Identify who should be consulted on the risk (if considered necessary).*	*Provide a description of the mitigating actions decided on for the risk (as per the risk treatment plan – see Annex 2).*	*Assign a value for the likelihood of the risk occurring (using the categories set out in Section 4.2., if found appropriate to your organization's context).*	*Assign a value for the consequence should the risk occur (using the categories set out in Section 4.2., if found appropriate to your organization's context).*	*Assign the residual risk level for the treated risk (making use of the risk levels as defined in your organization's consequence-likelihood matrix (see Figure 4).*	*Depending on residual risk level, determine what further actions need to be taken/ whether risk needs to be escalated (consider escalation criteria at end of Section 4.3).*

ANNEX 2: RISK TREATMENT PLAN TEMPLATE

Risk #:	*Same as Column 1 in the Risk Register.*
Treatment #:	*Assign identifier for the risk treatment.*
Risk description:	*Provide description of the risk, as per Column 2 in the Risk Register.*
Priority:	*Specify the level of urgency with which the risk needs to be treated (to allow for prioritization of risk treatment plans).*
Treatment plan:	*Provide description of the treatment plan (to be reflected in Column 10 of the Risk Register).*
Treatment plan objectives:	*Specify what will be achieved through the treatment plan, along with indicators against which progress can be measured.*
Actions:	*Specify what actions/activities will be taken/implemented under the treatment plan, along with timeline.*
Resources:	*Specify what resources are required to implement treatment plan (including staff time, financial requirements, etc.).*
Person(s) responsible:	*Specify the person(s) responsible for implementing the treatment plan.*
Monitoring:	*Specify how progress on implementation will be monitored, along with reporting requirements.*
Date:	*Specify the date the treatment plan was completed and approved.*
Version:	*As the treatment plan may need to be amended over time, specify the version that is the most current treatment plan (and ensure that previous versions are systematically filed).*

ANNEX 3: FURTHER READING

IEC. 2019. IEC 31010:2019 Risk management — Risk assessment techniques (behind paywall)

https://www.iso.org/standard/72140.html

This manual provides guidance on the selection and application of techniques for assessing risk in a wide range of situations.

ISO. 2018. ISO 31000:2018 Risk management — Guidelines (behind paywall)

https://www.iso.org/standard/65694.html

ISO 31000:2018 provides guidelines on managing risk faced by organizations, according to international standards.

Transparency International. 2014. Preventing Corruption in Humanitarian Operations: Handbook of Good Practices

https://images.transparencycdn.org/images/2014_Humanitarian_Handbook_EN.pdf

A comprehensive handbook providing guidance in how to diagnose corruption risks specific to humanitarian operations and to develop a set of good practices aimed at mitigating those risks.

U4 Anti-Corruption Resource Centre. 2011. Developing an NGO corruption risk management system: Considerations for donors

https://www.u4.no/publications/developing-an-ngo- corruption-risk-management-system -considerations-for-donors.pdf

The report provides and overview of what a corruption risk management system could consist of and issues to take into consideration when designing such a system.