USAID FROM THE AMERICAN PEOPLE | PROgress PROTECTING GLOBAL RIGHTS | Freedom House

PROJECT RISK PLANNING

A WORKSHOP FACILITATION GUIDE

Cover Image:
Health workers learn to protect themselves and their patients from COVID-19 and other infections in Tanzania, in April 2020. (Credit: USAID)

Introduction

Who is this guide for and how can you use it?

This guide attempts to address some of the gaps in knowledge and project management practice identified through an assessment of existing USAID-funded programming by five implementing organizations. It outlines key concepts and group exercises for a half-day workshop, which can serve as a starting point for teams developing implementation plans for new projects or revising ongoing initiatives. Options for expansion are noted where relevant.

For maximum effectiveness, the workshop should focus on a specific project, so that the outputs immediately contribute to its planning and implementation. We recommend that this workshop take place during the inception period of a new project, or no later than the first 60 days post-award.

The participants should comprise the project team, including the assigned monitoring, evaluation, and learning (MEL), security, and compliance staff. For large, high-profile, or politically sensitive projects, and for portfolio-level analyses, a donor agency representative should also be invited. It is always a good idea to include local partners who will play a substantial role in project implementation to participate in the workshop. However, the size of the group should be limited, ideally to no more than 10–12 people, to ensure everyone has a chance to contribute.

The facilitator of the process should be someone external to the project team with expertise in program design and implementation. It does not matter whether the facilitator represents MEL, the Project Management Office, or another program team, but they should have a working understanding of the project management cycle and experience in facilitating adult learning.

As a basic tool, this guide captures only the fundamentals of risk management planning, as gleaned from the standards developed by the Project Management Institute and adapted by Freedom House. We encourage the users of this guide to explore additional resources and expand their own approaches to risk planning and management, documenting and sharing them for institutional and industry learning.

Methodological considerations

This guide first discusses some key concepts and overarching considerations for risk planning through the prism of the overall project management process. Then, information is broken down into three thematic, practical workshops—Process Overview, Risk Analysis, and Risk Responses—each including material and exercises to share with the participants. The facilitator can choose the presentation format and the specific portions of the background information to be shared based on the participants' baseline knowledge and available time.

To make this guide useful for distributed teams, it provides facilitation instructions for an online workshop, but it could easily be adapted for an in-person event. The appendices contain templates and visuals that can be shared (with minimum-to-no adaptation) via slides, flipcharts, or a whiteboard, depending on the workshop format.

Finally, the timing of each module is based on Freedom House's previous experience doing such workshops in-house and accounts for the discussion of theory and the group exercises. This guide does not include time considerations for technology testing, participant introductions, rule-setting, or practicing the use of virtual tools.

Definitions

Standardizing how we talk about risks in periodic reports helps collect comparable data, conduct analysis, and better prepare for managing risk in future projects. Through an assessment of implementers' project reports, Freedom House observed that project teams use a variety of terms to talk about risks, often conflating risk events, their impacts, and management strategies. For example, the word mitigation is often used to define any action in response to a risk event. Meanwhile, mitigation is only one of at least five risk management strategies. Similarly, we have observed that implementers extensively use the word challenge to describe both individual risk events and their impacts.

By using standardized lexicon on risk and risk management, project teams are better equipped to think about risk in a structured way and capture a full variety of possible and actual risks that projects are facing. This systematic approach is critical for planning response actions and allocating resources ahead of time, thus helping teams become more resilient in the increasingly complex and uncertain environment in which democracy, governance, and human rights (DRG) support programs operate.

The definitions used in this guide are adapted from the Project Management Institute's project management terms[1] and from Freedom House's internal practice.

Risk – an uncertain event or condition that, if occurs, has a positive or negative effect on one or more project objectives. Negative risks are called *threats* and positive risks, *opportunities*. Risks can be grouped into broader categories, usually based on their source, which can be individual to the project or generic across an entire organization. USAID, for example, groups risks into programmatic, fiduciary, reputational, legal, security, human capital, information technology, and operational.[2]

Risk source – a specific project process, document, actor, or external event from which individual risks may arise. Knowing the source of risk, and the level of control the project team has over it, allows teams to select and implement risk response strategies proactively and deliberately.

Risk impact – consequences of a realized risk on a project. Risk impact is specific to the project context and reflects the risk appetite and thresholds of the implementer and key stakeholders. Context- and partner-specific understandings of risk impact must be defined to interpret the applicability and/or level of influence of individual risk events on the project.

Risk response strategy – a strategy to respond to known risks, usually presented as a component of a project management plan that describes how risk management activities will be structured and performed. Risk response strategies for threats include avoiding, escalating, transferring, mitigating, and accepting. The response strategies for opportunities include exploiting, escalating, sharing, enhancing, and accepting.

What is the Risk Management Cycle and Where Does It Fit in the Project?

Projects are not implemented in vacuum; the context always presents a certain degree of uncertainty, which can vary over time. Risk planning and management are thus an integral part of the project management cycle. Steps to identify and analyze risks and to select and plan response strategies should be taken repeatedly throughout the project lifecycle (see Appendix A), and these activities should be planned and shared with the project stakeholders in advance—for example, through the annual workplan development process.

The frequency and format of risk management activities will differ depending on the project development approach, but the core recommendation applies uniformly to predictive (i.e., "waterfall"), adaptive (i.e., agile), and hybrid projects cycles:

1. Risks should be identified and analyzed before the project activities begin and periodically reviewed.
2. Strategies for risk response should be developed ahead of time and periodically reviewed.
3. Risk monitoring activities and responsibilities should be assigned clearly and enforced.
4. Retrospective reviews of actualized risks, responses, and lessons learned should happen regularly and result in documented actionable steps, which can be further incorporated into the risk management plan.

Risk Management Process

For example, a project-specific Risk Management Plan should be developed during the two-month project inception period and reviewed at logical stages in the project (e.g., quarterly, annually, or after specific milestones), depending on the predictability of the operating environment. Ongoing risk monitoring and review can be incorporated into standard project administration activities, such as a discussion item for project backstopping meetings or as a pre-requisite for each activity sprint. Finally, documenting lessons learned through risk responses should also happen at predictable moments in the project lifecycle, for instance, after each major activity milestone, annually, and at the end of the project.

Risk Management Plan

Project teams should develop and periodically revisit the Risk Management Plan—a fundamental project document that should, at the very least, include a description of the overall approach to risk management, project-specific risk impact definitions, a discussion of known project risks, an overview of risk response strategies and actions, the procedure for deploying resources available for risk responses, and the positions on the project team responsible for risk response ownership.

An actionable Risk Management Plan will also define decision-making authority of various project team members and other stakeholders, clearly specify the timeline for retrospective reviews and reassessments, and include project-specific standard operating procedures to manage high-probability, high-impact risks (for example, a secure communications protocol, a beneficiary vetting protocol, etc.).

Multiple team members can participate in the drafting of the plan; however, we recommend that project leads or specifically assigned senior team members own this task. For example, the project lead scopes the plan and presents the logic to the project team; the team and other stakeholders participate in the risk analysis process; and then the project lead incorporates the content into the plan with one more round of review. The plan should be reviewed and approved in accordance with organizational policy. In some cases, donor agencies will want to review and approve such plans as well.

Budgetary and Logistical Considerations

No matter how straightforward the project is, responding to predictable risks, as well as conducting iterative risk analysis and planning, requires dedication of project resources. If these allocations are not made for risk management, the project lead may need to make difficult decisions later to divert precious funds from activities or management functions for risk responses.

Budgetary and logistical implications should be considered as early as the cost design stage. After a preliminary risk

analysis is conducted, and highest priority risks are identified, the project design team should develop initial contingency plans and cost them out. Cost elements should be considered under every budget category, for example:

- **Personnel:** How will individual members' level of effort on the project change to manage this risk response, e.g., for increased daily communication and coordination with stakeholders?
- **Travel:** Will travel and lodging be required as part of the risk response, e.g., for temporary relocations?
- **Contractual:** Will there be any subawards associated with the risk response, e.g., to transfer the logistics and security of a particular event to a third party?
- **Other Direct Costs:** Will there be a change to office, security, or event costs, e.g., to cover losses in local exchange rates or beef up event security?

As a best practice, projects should have a dedicated *contingency reserve* specifically for responding to predictable, high impact risks. These reserves should only be tapped into if the identified risks are realized; they should be reallocated, in consultation with the donor, to other project needs if predictable risks are no longer likely. If budgets are too tight, contingency plans should include considerations of how project funds will be shifted to respond to realized risks.

For example, in some sensitive political contexts where human rights defenders constantly risk their physical security in the course of their work, Freedom House budgets for emergency relocations of the most vulnerable project partners in case they become targets for persecution. One such case can cost up to $10,000. Some donors provide guidance for the inclusion of contingency reserves in project budgets; for instance, projects funded by the EU External Action Service may include up to 5% of direct costs for contingency needs.[3]

For risks affecting multiple projects, response costs should be allocated proportionately to all of them. Unpredictable risks that are not specific to any given project are best addressed at the enterprise level with *management reserves*.

Module 1: Risk Management Process & Identifying Risks

Facilitator Note:

Use the first module as an opportunity to review or provide a broad overview of the risk management process throughout the project life cycle. Use Appendix A visualization in this module and throughout the workshop to point out which stage of the planning process you are in. Allow up to 20 minutes for this review; the amount of time spent on the theory will vary depending on the baseline knowledge of the participants.

Overview:

We often have conversations about project risks in the context of security—whether it is security of beneficiaries, security of staff, or organizational security. The concepts of risk and security are very closely related. *Risk* is an uncertainty that, if occurred, has an impact on project objectives. Risks can be positive (opportunities) and negative (threats). Each implementer has a different appetite for risks—they are willing to accept varying degrees of uncertainty in anticipation of a reward. *Security*, however, is the quality or state of being free from danger. Thus, when we talk about risks only through the prism of security, we limit ourselves only to the discussion of threats while missing out on considering opportunities.

No project exists free of risks; the question is, how do we respond to them? Better yet, how do we prepare for threats and opportunities in a way that maximizes our reward and minimizes the damage to the project? Risk planning and management procedures help us anticipate threats and opportunities far in advance, align resources to better navigate them, minimize response time, and streamline the learning process so that mistakes of the past do not occur in the future. Risk management is a continuous, never-ending process, which begins at project inception, continues throughout the project cycle, and ends only after project closeout (See *What is the Risk Management Cycle and Where Does It Fit in the Project?*). Like with any management process, risk planning and management must always be documented to expedite decision-making, streamline the project team's learning, and enable institutional knowledge transfer.

Risk Management Process:

The risk management process generally comprises five stages that recur in a cyclical pattern throughout the project.[4]

- **Plan risk management:** Project managers purposefully dedicate time to define their approach to risk management, establish timelines and the level of team engagement, and draft the scope of the *Risk Management Plan*.
- **Identify risks:** Project teams engage in a deliberate activity to identify real risks—both detrimental and beneficial—associated with a specific project. Teams can use brainstorming, document analysis, SWOT-analysis, expert interviews, root cause analysis, Crawford slip method, and many other tools to come up with a broad list of project-relevant risks.
- **Analyze risks:** Project teams perform qualitative and quantitative analyses of the identified risks. Qualitative analysis often involves assessing each risk's level of probability and impact on the project, along with other parameters, resulting in risk prioritization. Quantitative analysis is used to assign metric values to the most significant risks to determine the probability of achieving project goals or justify allocation of contingency reserves in large-scale, data-driven projects.[5]
- **Plan risk responses:** Project teams determine overall strategies and specific steps in response to the identified risks, determine the resources needed, and assign responsibilities for their execution.
- **Monitor and control risks:** Project teams implement the risk management plan and produce meaningful supporting documentation for record keeping and learning.

Risk Management Process

This workshop reviews step 1, risk management planning, and focuses on steps 2–4: identifying risk, analyzing them, and planning risk responses.

Next Step: Continue to *Exercise 1: Identifying Risks to Project.*

Exercise 1: Identifying Risks to Project

Duration:

Approx. 30 minutes

Tools:

A virtual board with multi-user functionality (consider Microsoft Teams Whiteboard, Miro, Google Jamboard, or a similar platform)

Objective:

Participants collectively determine as many known risks to the project as possible while exploring diverse interpretations of risk by each member of the team.

Knowledge prerequisites:

- Understanding of the concept of *risk* in the project context.
- Understanding of the risk management process.

Facilitator's guide:

Step (Duration)	Activity	Prompts	Notes
1 (2–3 min)	Review the specific project's goals and objectives.	Use project-specific materials.	- Save these points on a separate slide or corner of the virtual board for quick reference throughout the workshop.
2 (5 min)	Ask participants to brainstorm as many various risks as possible that can affect the specific project.	- *What risks can undermine the success of the project?*	- Participants write one idea per virtual sticky note or text box directly on the virtual board. - Participants work individually. No discussion at this stage.
3 (15 min)	Review the stickies with the participants and ask them to expand on their ideas.	- *Why is this a risk to the project?* - *Is this a positive or a negative risk?*	- Focus on the most repetitive ideas and those that appear unique. - Ask 4–5 volunteers to share. - Allow for discussion, agreement, or disagreement, aiming for clarity in logic.
4 (5–7 min)	Consolidate the ideas by adding or removing any stickies.	- *Is there anything you would like to add or remove from the board after this discussion?*	- Allow time for discussion if there are disagreements or concerns.

Options:

- Instead of individual brainstorming, if time allows, the team could engage in a full SWOT analysis based on their in-depth understanding of the operating context. The *threats* and *opportunities* from the SWOT would then provide the basis for further analysis.
- If other sources of information from past experiences are available (e.g., lessons learned, stakeholder interviews, project assessments, etc.), the facilitator could share a list of risks that have previously occurred in similar contexts and ask for participant feedback.
- If desirable, the exercise can explicitly focus not just on *threats* but also *opportunities* for risk planning. In this case, Step 2 can be expanded to include the prompt *"What unpredicted factors can increase the success of the project?"*

Next step: Continue to *Module 2: Risk Analysis.*

Module 2: Risk Analysis

Facilitator Note:

Allow up to 20 minutes to review the content.

Overview:

After we identify a variety of possible project risks, the next step in the planning process is to perform qualitative analysis (see Appendix A for visualization). Qualitative analysis allows project teams to further describe and group risks according to different parameters, which then helps determine the priority of the response and the need for specialized resources. It also lets the project team learn over time what types of risks are more likely to occur in distinct contexts. The most common parameters for analysis include probability and impact, but complex analyses may also consider controllability, detectability, proximity (degrees of separation from the risk source), propinquity (perceived impact on individual stakeholders), and other parameters.[6]

Sources of Risk:

A most basic type of analysis is *categorization* of risks by source. In general, any taxonomy for sources can start at the highest level. Are the sources of risk internal or external to the project? Sources can then be narrowed down by broad categories, for example, legal, financial, technological, human, etc. In Freedom House's desk-review assessment of USAID-funded programs, almost one in three risks came from project partners or beneficiaries, followed by the political environment (about one in six cases) and global events (approximately one in eight cases). Other sources of risk often mentioned in DRG projects are local regulations, technology, internal rules and procedures, project scope, and travel requirements (see Appendix B for example).

Knowing the source is critical for risk management; depending on the level of control over the source, teams can choose an appropriate risk response strategy. Risk sources internal to the project and under a high degree of control, such as management structures or project scope, should be easier to predict and manage. The lower the level of control, the more likely it is that the risk cannot be avoided altogether, thus necessitating the planning for mitigation, acceptance, or transference as risk response strategies. The lower the level of control over a specific risk source, the higher the cost will be to influence this source (financial, human, or time). Teams should especially focus on mapping out management strategies and allocating resources for risks that project staff cannot influence—from lacking internet connectivity and travel visa denials to onerous local registration procedures and insurgency.

Impact and Probability:

Most organizations have a uniform approach to assessing *probability* using a consistent scale and definitions (for example, remote-low-moderate-high). However, the definition of *impact* should be developed for each project individually (see Appendix C for template). In Freedom House's analysis of program reports, the potential impact of specific risk events ranged widely, from misallocation of project resources or failure to accurately reflect local needs in activity design, to suspension of activities, and to a complete inability to achieve desired project outcomes. In a predictive project cycle, inability to implement project activities can have a high impact on the project; however, in an agile project cycle, this consequence would have a minor impact due to the adaptive nature of the design.

The Impact-Probability Matrix (see Appendix D for template) is the most used tool for determining the risk response priority based on these two parameters. In highly repressive or volatile environments, it may be helpful to weigh impacts heavier than probabilities, which acknowledges that certain risks, while less likely, could have devastating consequences on a project and should not be grouped with the risks that are highly likely but insignificant in their effects.

Impact-Probability Matrix

		IMPACT		
		High (6)	Medium (4)	Low (2)
Probability	High (4)	1st priority	3rd priority	later
	Moderate (3)	2nd priority	4th priority	later
	Low (2)	4th priority	later	later

Next Step: Continue to *Exercise 2: Analyzing Risks.*

Exercise 2: Analyzing Risks

Duration:

70 minutes

Tools:

- The virtual board with ideas from *Exercise 1: Identifying Risks to Project*
- A virtual table with the Impact-Probability Matrix in a separate section of the virtual board (see Appendix D)
- A virtual textbox with Risk Impact Definitions in a separate section of the virtual board or on a separate slide (see Appendix C)

Objective:

Participants collectively categorize identified risks by source and prioritize them based on an impact and probability assessment.

Knowledge prerequisites:

- Understanding of the concept of *risk* in the project context.
- Understanding of the risk management process.
- Review of the project risks identified during the previous exercise.

Facilitator's guide:

Step (Duration)	Activity	Prompts	Notes
1 (5 min)	Ask the participants to think about a concrete agent—source—of each risk and write it down on the stickies.	- *What person, document, event, or entity does the specific threat (or opportunity) originate from?*	- Remind the participants where you are in the Risk Management Planning process by referring to the process chart. You have gone through Identify Risks and are now in Analyze Risks. - Individual work; no discussion at this stage. - Participants add text directly to individual stickies on the virtual board. To add the risk source to each sticky, use a different font color or thickness or by adding text bubbles (depending on the functionality of the board).
2 (2–3 min)	Ask the participants to group the risks based on the identified sources.	- *Please work individually or as a group to group the risks according to their source.*	- Participants move stickies on the virtual board. - You can adjust stickies to make sure that all text is clearly visible.

3 (15 min)	Review and discuss the results as a group.	- *What do you observe? Is there anything surprising?* - *What major categories have emerged?* - *Is there consistency in how risks were grouped? Did you have any difficulty in rearranging the ideas? Why?* - *Which sources are under our control as a team? Under organization's control? Donor's control? Which can we influence? How?*	- Risks of different categories can originate from the same source. There may be alternative opinions about specific sources. - Note that knowing the source of risk—and the level of influence the project team and other stakeholders have on it—is important in the selection of risk management strategies. The less the control, the more likely you might try to avoid, escalate, or transfer the risk outside of the project (see *Sources of Risk*). - Note that there are no definite classifications of risks; they are individual to each project. One team can divide project risks into internal and external. Another can group them according to core project constraints (scope, budget, time). A third one yet may focus on operational (policies, procedures, resource availability) vs. human security (physical safety, mental and emotional well-being).
4 (5 min)	Review risk parameters: Impact and Probability.	See *Impact and Probability*.	- Note that gradations for each of these parameters can be unique for each project or standardized across the organization. - Ask if the participants have a standardized probability scale.
5 (15 min)	Ask the participants to define the various levels of impact that risks may have on their specific project and write them down.	- *How would you define the impact of risk on a specific project?* - *What exactly does it mean when we say that the impact is "high," "medium," or "low"?*	- Allow a couple minutes for the participants to brainstorm individually. - Remind the participants that risk impact should be reviewed through the prism of the project's goals and objectives. - Ask for volunteers to share their definitions and write them down on the online Risk Impact Definitions template (see Appendix C). - Facilitate the discussion until there is a cohesive agreement on the definitions among the group. - This activity can be extended if there are more nuanced gradations of impact than "high," "medium," and "low."
6 (5 min)	Present the Impact-Probability Matrix. Ask the participants to place the identified project risks on the Impact-Probability Matrix, using their definitions of risk impact.	- *Drag the stickies with the individual risks to the squares on the matrix where you think they belong.*	- Remind the participants to apply their newly developed definitions of impact. - Make sure that the online Impact-Probability chart is large enough for multiple stickies to fit without overlap, for everyone's visibility. - If needed, move stickies slightly to ensure everyone can read the text.

7 (20 min)	Review and discuss the placement of individual risks into the priority squares on the Matrix.	- *Does everyone agree with the placement of the identified risks on the matrix?* - *What makes you believe that this risk will have a high (medium, low) impact on your project based on your definitions?*	- Offer an opportunity to the participants to express alternative opinions as well as defend placements. - Facilitate the discussion until there is a general agreement over the placement of all stickies. Difference in views is good, and the objective is to achieve a shared view of risks. - Remind the participants that this analysis helps prioritize risk responses in times when multiple risks have materialized. - Conclude by reviewing the top-priority squares. - Remind the participants that this qualitative analysis can and should be performed periodically to capture changes in the context.

Options:

- The team could expand the discussion on categories of risks beyond their sources, if time allows, or skip it altogether.
- If time allows and the team is interested in analyzing *opportunities* in addition to *threats,* the facilitator can prompt them to discuss any observable trends in positive and negative risks by categories. For example: *Which sources generate more threats, and which generate opportunities? Why? What degree of control do we have over these sources?*
- If the team is interested and time allows, they could perform risk analysis around other parameters relevant to the project, such as detectability, dormancy, or the perceived impact on individual stakeholders (propinquity). However, multi-parameter risk analysis is not always warranted and may detract attention from planning responses to highest impact risks.

Next step: Continue to *Module 3: Risk Responses*

Module 3: Risk Responses

Facilitator Note:

Allow up to 25 minutes to review the content.

Overview:

After the team has identified known project risks and analyzed and prioritized them based on the combination of their potential impact and probability of occurrence, it is time to determine how individual risks will be handled. Planning risk responses is an important process; it allows a team to determine their—and, sometimes, other stakeholders'—behavior in preparation for, during, and after the occurrence of a risk event. Ultimately, knowing how your team is handling risks strengthens the ability of the project to weather the most dangerous—or most opportune—uncertainties, and significantly increases its resilience, especially in highly volatile operating conditions.

Risk Response Strategies:

There are, generally, five strategies to address negative risks, or *threats* (see Appendix E for visualization). The selection of a particular strategy depends on the risk appetite of the implementer, the level of control the team has over sources of risk, on the available resources, and on the severity of the potential risk impacts. Different teams may choose different strategies in the same situation.

Acceptance normally acknowledges the existence of a certain threat but deems it so insignificant that no proactive action is taken, and no contingency reserves are allocated. This strategy is best applied to low-impact, lower probability risks. For example, the project team may expect variations in currency exchange rates, but their analysis shows that the variations will be so small that the budget can absorb them without any negative impact on the project. The team does not take any steps to address this risk; it accepts it.

Avoidance implies that the threat can be potentially so damaging that the probability of its occurrence should be eliminated. Avoidance responses usually involve changing an aspect of the project, such as activity design, timeline, or budget. For example, a particular project partner repeatedly delivers delayed, or subpar contributions to the project, forcing the implementer to allocate additional resources to correcting errors and undermining the reputation of the overall initiative in the host country. In this case, the project team may opt to partner with another organization with similar capacities to avoid these risks.

Escalation leads to engaging stakeholders outside of and more senior than the project team—either within the organization or externally, such as the community of peer organizations, a professional association, or donors. This strategy is best applied to the risks that cannot be managed by the project team alone. For example, a project is facing significant delays and souring relationships with local partners because of the lengthy subgrant procurement procedures. The project team escalates the risk to the grants and compliance team with constructive recommendations, which results in the development of a more streamlined subgrant procurement policy at the organizational—not project—level. Escalation is also utilized when certain political risks cannot be navigated by one organization alone but require targeted policy advocacy through coalitions.

Mitigation involves actions meant to reduce the probability of risk occurrence and/or to reduce the impact of the threat; this strategy is deployed when avoiding the risk altogether is impossible. For example, connectivity issues can limit the ability of participants to see and interact with webinar content, thereby jeopardizing their commitment to the workshop or the achievement of learning objectives. In a real-life example, a team chose to mitigate this risk by providing the affected participants with downloadable content ahead of time and then conducted the webinar in an audio-only format.

Transference involves shifting ownership of a risk to a third party to both manage the risk and bear its impact if it occurs; transference usually comes with a premium cost. For example, an implementer can choose to hire a logistics company to organize a major event—and thus transfer the ownership of risks associated with finding a perfect venue, arranging travel or interpretation, or payment transfers, to a third party. Similarly, if an implementer faces exposure as a direct supporter of a local civil society organization in a repressive country (a potentially devastating risk), it may choose to transfer the risk of exposure by contracting an intermediary organization.

In Freedom House's analysis of implementers' reports, in nearly half of all examples, teams were deploying mitigation activities where damage had already occurred in order to limit the severity of impact. In many cases, risks that result in the need for damage control (mitigation) can in fact be avoided altogether with proper advanced planning. Escalation and transference can be powerful solutions to deal with threats that are outside of the scope of the project but require thoughtful analysis of sources of risk, as well as courage and determination of project leadership to engage stakeholders outside of the project team.

For a supplemental discussion of risk response strategies for *opportunities*, please see Appendix F.[7]

The selection of risk response strategies is the last major step in risk planning, but the process does not stop there. As teams go through the planning process, they should document their identified risks, their assigned priority levels, risks response strategies (and, ideally, specific response actions), and assign the "owner" of each risk—the person on the team who will be responsible for managing the individual threat. It is also a good practice to proactively determine response timelines for risks that do occur and decision-making responsibilities. The resulting plan of action becomes an integral part of the Risk Management Plan (see Appendix G for template).

Risk Response Plan

Threat	Source	Priority	Impact Scenario	Response strategy	Response actions	Response timeline	Risk owner	Decision authority
Staff emails are hacked	*Government-sanctioned actors in country XYZ*	*2*	*Names of staff, partners become known to nefarious actors, resulting in a smear campaign or direct threats*	*Avoid*	*Develop custom email protocol:* • *use separate email addresses for each activity/partner* • *use two-factor authentication* • *delete emails with sensitive info after securely archiving (etc.)*	*Two weeks post-award*	*Senior project officer*	*Project director*

Next step: Continue to *Exercise 3: Planning Risk Responses*

Exercise 3: Planning Risk Responses

Duration:

50+ minutes

Tools:

- Slide: Risk Response Strategies (see Appendix E, F)
- Shared spreadsheet template: Risk Response Plan (see Appendix G)

Objective:

Participants collectively determine risk response strategies to high-priority project risks.

Knowledge prerequisites:

- Understanding of the concept of *risk* in the project context.
- Understanding of the risk management process.
- Completion of the Impact-Probability Matrix in the previous exercise.

Facilitator's guide:

Step (Duration)	Activity	Prompts	Notes
1 (10 min)	Review and discuss the slide: Risk Response Strategies.	- *Which sources of risk can we control on the project team? In our department? In our organization?* - *Can you think of examples from your experience that would fall into each of these response categories?*	- Note that the more control the team has over the source of risk, the easier it is to deploy a*voidance* or *mitigation* strategies. - Note that this exercise is focused on responses to negative risks (threats). The response strategies to positive risks (opportunities) are slightly different.
2 (5 min)	Review and discuss the template: Risk Management Plan.	- *Which of these parameters would be most/least useful in your work? Why?*	- The template can be augmented to include or exclude certain parameters, depending on project needs. - Certain parameters (e.g., risk category) could be preferable to capture for MEL purposes but may otherwise be unnecessary for an individual project.

3 (2–3 min)	Revisit the Impact-Probability Matrix and review the top priority risks.	- *Which risks have we identified as top priority based on the combination of their probability and potential impact?*	- The focus on the top priority options is only for the sake of time. Ideally, all identified risks should be addressed in this exercise, in order of their priority.
4 (15+ min)	Split the participants into small working groups (2-3 people max) and assign each group to develop a response plan to one of the selected risks.	- *Take one risk and walk through each item in the risk response plan. Note the priority level, impact scenarios, desirable response strategy and brainstorm key response actions as part of that strategy.*	- Each group should fill out a separate line in a shared doc for their specific risk. - If time allows, assign more risks per group. - Participants may find that one risk can have multiple response strategies. Ask them to determine which will be the best for the project. If time allows, participants can prioritize multiples response strategies for one risk (e.g., avoid-mitigate-escalate), but they should determine when and why they would switch from one strategy to the next.
5 (25+ min)	Bring small groups back to the plenary for their presentations.	- *Please share with the group your results: which risk you worked on, what priority it is (if multiple), what response strategy you selected, why, and what specific risk management steps you propose.*	- After each presentation, allow the rest of the participants to critique their peers. Encourage constructive explanations for alternative opinions. - Ask the group which *role* on the team (position, not a person) should "own" each risk. - Note that the participants are developing a plan for future action. If a specific risk is realized, it should be documented, triggering the implementation of risk response steps. - Allocate approximately five minutes per risk. Expand the duration of this step as needed to review all identified risks if time allows.

Options:

- The facilitator can assign "homework" to the project team to repeat the process for all identified project risks to complete the risk response plan. Alternatively, teams can undertake a longer workshop, or multiple sessions, to work through each identified risk as a group with a facilitator.
- The teams may choose to work on both threats and opportunities. In this case, the workshop should be extended, or the exercise can otherwise be reconfigured to include a discussion of select threats and opportunities.

About this Guide

This guide was developed under the Human Rights Support Mechanism (HRSM), a USAID-funded and Freedom House-led Leader with Associates cooperative agreement. HRSM is implemented by the PROGRESS Consortium, a group of five organizations that support and implement human rights programming. Freedom House developed this guide as a resource for the Consortium and other DRG implementers.

In spring and summer 2021, Freedom House conducted a random-sample analysis of HRSM narrative project reports to examine how Consortium partners managed and reported on risks. As a benchmark, the evaluation team used the core concepts and principles of risk management from the Global Standard for Project Management (ANSI/PMI 99-001-2021).

The desk-review assessment revealed that, at the time, there was no evidence that the HRSM partners managed project risks using standardized and cohesive processes. Risk analysis was, for the most part, performed after the fact and in a rudimentary form, indicating an absence of either the systematic anticipation of risks at project inception or the reevaluation of previously developed risk management plans. Moreover, the observed risk response strategies largely focused on controlling the negative impacts of threats that had already occurred. A lack of uniform terminology across the sample underscored the missing theoretical knowledge among report writers and further complicated comparative analysis.

Ultimately, this toolkit serves as a practical step to address some gaps in the implementers' practices in analyzing, planning, managing, and reporting project risks.

Endnotes

1 *A Guide to the Project Management Body of Knowledge* (*PMBOK Guide*). Seventh Edition. Project Management Institute, 2021.

2 *USAID Risk Appetite Statement: A Mandatory Reference for ADS Chapter 596*. New edition date: 08/22/2022. https://www.usaid.gov/sites/default/agency-policy/596mad.pdf.

3 *Practical Guide on Contract Procedures for European Union External Action* (*ePRAG*). Chapter 6: Grants. https://wikis.ec.europa.eu/display/ExactExternalWiki/6.+Grants.

4 Adapted from Pritchard, Carl. *Risk Management: Concepts and Guidance*. Fifth Edition. CRC Press, 2015.

5 Given the complex and resource-consuming nature of quantitative risk analysis, which is often impractical for smaller-scale democracy, human rights, and governance projects, this guide does not review this step.

6 For more on parameters for qualitative risk analysis, see *The Standard for Risk Management in Portfolios, Programs, and Projects.* Project Management Institute, 2019.

7 For more details on risk response strategies, see *A Guide to the Project Management Body of Knowledge* (*PMBOK Guide*). Sixth Edition. Project Management Institute, 2017, and other resources in the library at www.pmi.org.

Appendix

Appendix A:

Appendix B:

Control over Sources of Risk (example)

Risk sources	Low control	Medium control	High control
Internal to project		Project scope	Management
Internal to organization		Implementer's procedures	
External	• Technology • Travel requirements • Global events • Political environment • Local regulations	Partners	

Appendix C:

Risk Impact Definitions (template)

Impact	Definition in relation to the project	Weight?
High		
Medium		
Low		

Appendix D:

Impact-Probability Matrix, Weighted (template)

		IMPACT		
		High (6)	Medium (4)	Low (2)
Probability	High (4)	1st priority	3rd priority	later
	Moderate (3)	2nd priority	4th priority	later
	Low (2)	4th priority	later	later

Appendix E:

Risk Response Strategies

Accept

- Low probability, low impact
- No proactive steps or a contingency reserve

Avoid

- Sources of risk easier to control
- Change some aspect of project, management, objective to reduce risk probability to zero

Escalate

- Threat is outside the scope of the project
- Move risk response out of the project and onto higher authority in the organization or further out

Mitigate

- High probability
- Action to reduce probability of occurrence or severity of impact
- Damage control after threat occurred

Transfer

- Sources of risk hard to control
- Shift ownership of threat to a third party to manage risk and bear impact (at a premium)

Appendix F:

Risk Response Strategies for Opportunities

Just like with threats, positive risks, or opportunities, can be navigated using a variety of strategies. The selection of a particular strategy depends on the risk appetite of the implementer, the level of control the team has over sources of risk, the available resources, and the severity of the potential risk impacts. Different teams may choose different strategies in the same situation.

Acceptance normally acknowledges the existence of a certain opportunity but deems it so low priority that no proactive action is taken. It is good to monitor such opportunities in case their potential impact or probability of occurrence changes.

Enhancement implies that the potential benefit of an opportunity is so high that the team takes action to increase the probability or the impact of this positive risk. Understanding the source of the opportunity, and the level of control the project team has over it, helps focus efforts to increase its probability of occurrence. The impact of an opportunity can also be increased by changing the allocation of resources, environment, or culture around it. An example of opportunity enhancement can be the decision to organize an advocacy campaign in support of a desirable legislative proposal, to increase its chances of passing.

Escalation leads to engaging stakeholders outside of and more senior than the project team—either within the organization or externally, such as the community of peer organizations, a professional association, or donors. Just like with threat escalation, this strategy is best applied to the opportunities that cannot be managed by the project team alone. The ownership of risk also has to be transferred outside the project team, and it is critical that the higher-level stakeholder accept it. Once opportunities are escalated, project teams no longer need to monitor them.

Exploitation involves actions to increase the probability of a favorable opportunity to 100% and is usually applied to manage high-impact risks that are just too positive to ignore. In many cases, exploitation is used as a strategy to improve the organization's or project team's position in a competitive environment, or as a thought leader, or to improve its capacity to implement certain activities. For example, a project team may decide to exploit the availability of new data security technology to improve its data management protocols in politically sensitive environments and acquire a competitive edge over peer organizations.

Sharing involves increasing the chances that the opportunity will occur by transferring ownership to a third party. Just like with negative risk transference, shifting risk ownership comes with a premium cost. A very common example of opportunity sharing is when several implementing organizations form consortia and distribute roles as primes and subs, with corresponding budget and management responsibilities, to increase the probability of winning a competitive bid for a new funding opportunity.

Appendix G:

Risk Response Plan (template)

Threat	Source	Priority	Impact Scenario	Response strategy	Response actions	Response timeline	Risk owner	Decision authority
Staff emails are hacked	Government-sanctioned actors in country XYZ	2	Names of staff, partners become known to nefarious actors, resulting in a smear campaign or direct threats	Avoid	Develop custom email protocol: • use separate email addresses for each activity/partner • use two-factor authentication • delete emails with sensitive info after securely archiving (etc.)	Two weeks post-award	Senior project officer	roject director

Freedom House

Freedom House is a nonprofit, nonpartisan organization that works to create a world where all are free. We inform the world about threats to freedom, mobilize global action, and support democracy's defenders.

1850 M Street NW, 11th Floor
Washington, DC 20036

freedomhouse.org
facebook.com/FreedomHouseDC
@FreedomHouse
info@freedomhouse.org
202.296.5101