UNDP's Risk Management Framework for PVE Programmes: Quick Reference

The information below is summarized and adapted from: **The United Nations Development Programme's Framework - *Risk Management for Preventing Violent Extremism (PVE) Programmes: Guidance Note for Practitioners***

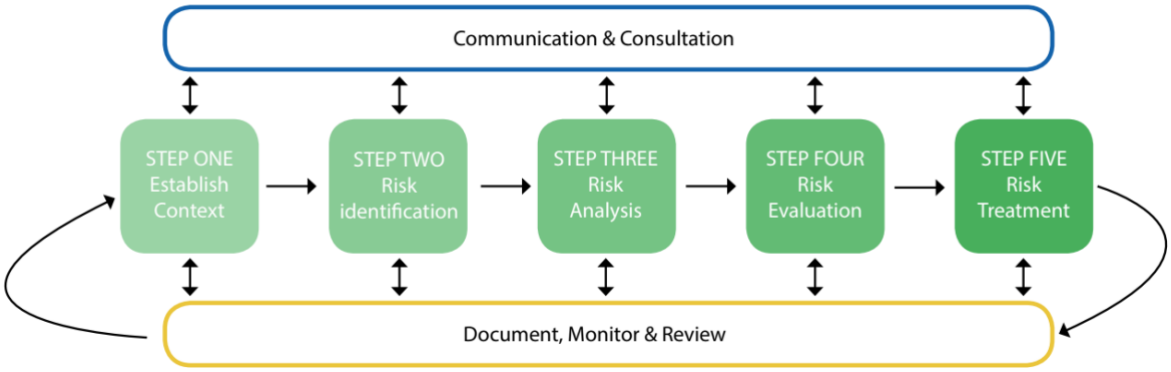
A project's Risk Management Strategy helps identify and manage PVE risks in a comprehensive manner and is underpinned by a risk management model built on:

1. Key '**principles'** that guide the creation of your risk management framework and help ensure that PVE programmes are as risk-sensitive as possible. UNDP defined the following key principles for PVE programming based on its research and experience: context analysis; conflict sensitivity and 'do no harm'; results-based management; and, human rights-based approaches.

> **TIP**: as UNDP recommends, you might revise these principles based on your own experiences and/or the context in which you work. For example, in this Guide, we introduce Positive Youth Development as a way to effectively involve youth in all stages of the project. Could PYD principles be valuable to you as you develop your Risk Management Strategy?

2. A '**framework'** that captures your overall approach to risk management. It consists of the policies and procedures put in place to implement the risk management process; this includes: the scope of the exercise; the human and financial resources that can be allocated both to the process and to the risk mitigation measures; the time you have available to complete the process; and, the level of risks – and in which areas – you are willing to accept and not accept.
3. The 'risk management **process'** (RM process) involves the systematic application of five key steps (establishing the context, identifying, analysing, evaluating, and treating PVE risks) combined with consistent communication with key stakeholders and regular monitoring. Lessons learned during the course of the RM process can feed back into the framework.

THE RISK MANAGEMENT PROCESS[27]



Step 1: Understanding the Context

The **internal context** includes: governance and organizational structures; accountability processes; relevant policies, overall objectives and culture. Establishing a clear, shared understanding of what your organization hopes to achieve with its PVE programmes is vital at this stage. The internal context should also include a discussion of the scope of the risk management activity; it is important to consider costs, resources (material and human), capabilities and whether additional capabilities are required, and what kind of documentation should be produced.	The **external context** comprises the broader context in which the PVE initiative/programme will take place, including the political, socio-economic, cultural, security, environmental, financial, religious and other dynamics. These dynamics may be at the local, national, regional or even global level, and the interaction between these different factors should be considered. External factors are generally outside the control of your organization or activity, and, therefore, constitute important risks to be considered when designing your risk management strategy.

Two important points to keep in mind during step 1:

- Invariably, the lines between internal and external factors may be blurred or inter-related; it is helpful, therefore, to brainstorm the two at the same time.
- Part of understanding the context includes developing your risk criteria (see Box 1), which is based on an understanding of your organization's risk appetite. Risk appetite can be defined as the balance between the potential benefits of embracing risk and the threats associated with such risks; knowing in advance what kind of balance your organization wishes to strike helps to guide you during the elaboration of this strategy and helps ensure consistency. Step 3 includes more details.

Box 1

Risk criteria can be thought of as a combination of 'red lines'/'no go areas' on the one hand, and areas where you have more leeway to 'push the boundaries' on the other. For example, your organization may decide that it will not take any fiduciary risks (e.g. risk of inadvertently funding individuals/CSOs with links to violent extremist groups), and the willingness to accept such risks, therefore will be low. However, your willingness to accept certain political risks may be high (e.g. insistence on engaging with 'returnees' despite government labelling them as 'terrorists'), since this aspect of the programme may be vital for achieving your goals, despite potential resistance.

Step 2: risk identification

What?

When identifying PVE risks, it is important to ask series of fundamental questions related to your activities that may positively or negatively impact upon the achievement of your objectives or outcomes. Risks may arise as a result of both internal and external factors, so it is important to explore and identify vulnerabilities, and potentialities, related to the context, the institution and the programme.

Who?

The identification of PVE risks should be undertaken in participatory manner – by bringing together certain stakeholders together in one room, and by implementing tailored engagement strategies for other stakeholders as and where necessary.

How?

It is helpful to 'walk through' each aspect of the programme you are assessing with relevant stakeholders. You should consider how each aspect of the programme will relate to both the context and the institution, and how the interaction between these elements may impact the programme and vice versa. Brainstorming, surveys, scenarios and focus groups could be strategies used to identify risks. It is helpful to ask the 'what, where why, who, when and how' questions. When trying to understand a risk you've identified, ask yourself the following:

- Sources of risk – "Risk From": What kind of risks could arise from the context, the programme or the institution?
- Risk type – "Risk of": What will the nature of this risk be?
  - Resource Risks (insufficient funds), Fiduciary Risks (loss of money for example as a result of fraud), Principles Risk (violates organization's or donor's principles), Political Risks (resistance of the plan from major actors), Security Risks (physical harm), Operational Risks (disruption to the smooth running of operations).
- Risk target – "Risk to": is this a risk to your reputation, your ability to deliver, or your staff, partners and beneficiaries?

Step 3: Risk analysis

This means 'unpacking' everything you know about the risks you have identified and using both quantitative and qualitative methods to determine the risk level. There are four central questions to be answered during the risk analysis phase for each of the risks you have identified:

1. What is the likelihood (or probability) of this event/or risk occurring? This is measured as a combination of whether the event is expected to occur and how often – measured on a scale of 'very likely' to 'rare'

Likelihood	Very Likely	Likely	Possible	Unlikely	Rare
Occurrence	The event is expected to occur in most circumstances	The event will probably occur in most circumstances	The event may occur at some time	The event could occur at some time	The event may occur in exceptional circumstances

2. What will the consequence (or impact) of this event/risk be on the programme? This is measured on a scale of 'extreme' to 'insignificant'

Consequence	Extreme	Major	Moderate	Minor	Insignificant
Occurrence	An event leading to massive or irreplaceable damage or disruption	An event leading to critical damage or disruption	An event leading to serious damage or disruption	An event leading to some degree of damage or disruption	An event leading to limited damage or disruption

3. What is the risk level? This involves a risk matrix, which is used to combine the scale for measuring likelihood/probability and the scale for measuring consequence/impact into one generic 5x5 table, numerated to make the analysis more efficient.

		Consequence				
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Likelihood	Very Likely (5)	Medium (5)	High (10)	High (15)	Very High (20)	Very High (25)
	Likely (4)	Medium (4)	Medium (8)	High (12)	High (16)	Very High (20)
	Possible (3)	Low (3)	Medium (6)	High (9)	High (12)	High (15)
	Unlikely (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	High (10)
	Rare (1)	Low (1)	Low (2)	Medium (3)	Medium (4)	High (5)

4. What does this analysis mean for my organization? i.e. What kind of decision-making processes or actions will be triggered by these risk levels, when, how and by whom? You should decide collectively what needs to happen as a result of each of the risk levels identified. The actions to be triggered are tied to your organization's risk criteria [see step 1].

Step four: Risk evaluation

Having analysed each of the PVE risks, you now need to evaluate them against the risk criteria established. At this point, you will need to initiate a discussion with key stakeholders concerning whether the risks are acceptable, manageable, unacceptable, etc. For each risk you should consider the benefits (tangible/intangible) of proceeding against the potential harm (including unintended consequences).

At this point, you may like to bring together your work into one table or 'risk register'. The Risk Register allows you to:

- Categorize risks according to whether they originate from the context (local, regional, global), the programme or the institution;
- To identify the risk type (e.g. resource risks, political risk, principles risk) and the risk target (e.g. reputation, ability to deliver, staff/beneficiaries/partners);
- Add in the likelihood and consequence score;
- Calculate the combined risk level score;
- Describe what type of controls you have in place already to manage the risk;
- Identify the indicator(s) you can use to assess whether or not the risk is realized;
- Indicate what risk treatment you intend to provide (see step 5); and,
- Indicate who the 'risk owner' will be. Risk owners are individuals within the organization responsible for monitoring a particular PVE risk. Their job is to keep track of changes in the context and/or programmes and the impact these changes have on the risk 'materialising'. The risk owner is responsible for ensuring that the risk treatment process in place is working and/or to initiative the

required risk treatment process as and where necessary. By ensuring that each risk has an 'owner', you are ensuring that the risk management process remains dynamic and adaptable.

Step five: Risk treatment

The risk treatment phase involves deciding (collectively!) how you will approach and mitigate the risks you have identified. There are four options available:

- Option 1 - Tolerate the risk: Tolerating a risk means accepting that the event may occur. You may decide to tolerate the risk because:
    - existing controls to mitigate against any negative impact are sufficient;
    - the risk level is within the organization's risk tolerance; and/or
    - additional measures are not worth the effort.
- Option 2 - Treat the risk: There are three ways risks can be treated, with the goal of reducing the 'residual risk level' i.e. the level of risks once the additional measures are in place:
    - Reduce the likelihood/probability: These mitigation measures are designed to reduce the likelihood/probability of an event occurring.
    - Reduce the consequence/impact: These mitigation measures are designed to reduce the consequence/impact of the event should it occur.
    - A combination of a. and b. depending on the nature of the risk in question.
- Option 3 - Transfer the risk: Transferring the risk means engaging a third-party to take responsibility for the risk and/or to distribute liability for the risk; this decision may be taken in contexts where other actors are likely to have different and/or reduced risks.
- Option 4 - Terminate the risk: This option should be considered if the costs involved in treating the risk outweighs the potential benefits, or if they are simply too high. In this case, the organization terminates the activity/engagement that is generating the risk.

As you go through these 5 steps, make sure you integrate two elements throughout the Risk Management Process:

1 *Communication and consultation*	**2** *Monitor and Review*
The risk management process should begin with communication and consultation, and these efforts should continue at each stage of the process. You will identify all the relevant internal and external stakeholders during phase one. You may then decide to design a stakeholder engagement strategy, detailing how and where at each stage of the process you intend to promote communication and consultation. This can enhance accountability, transparency and, therefore, the effectiveness of your risk management process.	Monitoring and reviewing the context, the risks identified and the processes put in place to manage them is an integral and systematic part of the risk management process. It ensures that our whole risk management framework remains 'fit for purpose'. Indeed, the risk management strategy must remain a 'living document'. Monitoring and review, however, should take place at each of the above steps as a change in internal or external context could require a whole revision of the risk management strategy underway, underscoring the importance of continued context analysis, monitoring and review.