

TERMS OF REFERENCE (TOR)

Project:	“Biodiversity mainstreaming into Sectoral Policies and Practices and Strengthen Protection of Biodiversity Hot-spots in Montenegro”
Job title:	Partner capacity/micro assessment
Duration of assignment:	01st May 2024 – 31st May 2024
Location:	Home based, Montenegro

Objective and scope of the micro assessment

The partner capacity/ micro assessment is performed by a third party service provider and includes a site visit to the IP. The assessment primarily consists of interviews with IP personnel and a review of relevant documentation sufficient to complete the assessment questionnaire (Annex 2). The questionnaire provides an overall risk rating based on responses provided:

Low risk – Indicates a well-developed financial management system and functioning control framework with a low likelihood of negative impact on the IP’s ability to execute the programme in accordance with the work plan.

Moderate³ risk – Indicates a developed financial management system and control framework with moderate likelihood of potential negative impact on the IP’s ability to execute the programme in accordance with the work plan.

Significant risk – Indicates an underdeveloped financial management system or control framework with a significant likelihood of potential negative impact on the IP’s ability to execute the programme in accordance with the work plan.

High risk – Indicates an underdeveloped financial management system and control framework with a high likelihood of potential negative impact on the IP’s ability to execute the programme in accordance with the work plan.

The overall risk rating is used by the Ministry, along with other available information (e.g. history of engagement with the Ministry and previous assurance results), to determine the type and frequency of assurance activities as per each UN’s guidelines and can be taken into consideration when selecting the appropriate cash transfer modality for an IP, based on each UN’s business model (further detailed in section 8).

Logistics

The assessment should be completed (including the site visit and report issuance) within one month of engaging the third party service provider. Project manager in front of the Ministry will introduce the service provider to the IP and facilitate the site visit.

Ministry provide the following documentation to the service provider for review before starting fieldwork:

- Copy of the latest macro assessments performed for the country, as applicable;
- UN agency/ies’ work plan(s) and programme documents with the IP
- Copies of reports of any partner/ micro assessments or other relevant assessment previously performed on

³ Throughout UN's policies and systems, "moderate" and "medium" may be used interchangeably to describe the risk rating between low and significant".

the IP e.g. review of the IPs or Country's Public Procurement System to determine its compatibility with the UN's Procurement Rules and Regulations

- Copies of reports of any financial or internal control audits and spot checks previously performed on the IP; and IP and Programme information as per Annex 1
- Any other documentation that may help the service provider better understand the context from a Ministry perspective.

Procedures and deliverables

The third party service provider receives general information regarding the IP and the programme from the Project Manager in preparation for the assessment (see Annex 1 and Items to be provided above). The service provider reviews this documentation in advance of performing a site visit to the IP. The service provider should also provide the IP with an advance request of the documents and interviews they would like to have while on site, to ensure efficient use of time.

The third party service provider also completes the micro assessment questionnaire (Annex 2, with instructions) based on the procedures performed during the assessment period. The service provider discusses the results of the questionnaire with relevant IP personnel and the Project Manager before finalizing it. Upon finalization, the service provider delivers an executive summary, detailing the overall risk rating and specific identified risks, and the completed questionnaire.

The micro assessment report is to be delivered in the format given in Annex 3.

Qualifications of the third party service provider

The third party service provider must be experienced in performing assessments similar to a micro assessment and assessing risks related to organizational financial management capacity (i.e. accounting, reporting, procurement and internal controls). The service provider must also have knowledge of the United Nations system and the development sector.

CVs of all members of the assessment team should be provided to the Ministry and should include details on engagements carried out by relevant staff, including ongoing assignments indicating responsibilities assumed by them and their qualifications and experience in undertaking similar assessments.

Annex 1. IP and Programme Information

The following information should be completed at the start of the micro assessment and annexed to the report as per the format in Annex 4 of this RfP.

Implementing partner name:	
Implementing partner contact details (contact name, email address and telephone number):	
Main programmes implemented with the Ministry:	
Key Official in charge of the Ministry:	
Programme location(s):	
Location of records related to the Ministry:	
Currency of records maintained:	
Latest expenditures incurred/reported to Ministry (as applicable). Indicate the amount (in US\$) and the financial reporting period ;	
Current or latest cash transfer modality/ies used by the Ministry to the IP	
Intended start date of micro assessment:	
Number of days to be spent for visit to IP:	
Any special requests to be considered during the micro assessment:	

Annex 2: Micro Assessment Questionnaire

Please see separately provided Excel format for the questionnaire, with calculation formulae included, which has to be used.

Instructions

This questionnaire contains questions related to eight subject areas. Certain questions are classified as “key questions” indicating that they have a greater impact in assessing the effective functioning of the IP’s control framework.

1. Answer each question by selecting ‘Yes’, ‘No’ or ‘N/A’ (for ‘not applicable’) from the drop down menu in the appropriate column.
2. Use the Risk Assessment column to assign a risk rating (high, significant, moderate or low) for each question based on the response obtained. For example, if the question addresses an item that should ideally be marked ‘Yes’ but was marked ‘No’, it should be assessed for the level of risk it presents to the effective functioning of the IP’s control framework. Assigning risk ratings to each question requires judgment by the assessor as to how the response will impact the effectiveness of the IP’s control framework.

NB: THE APPROPRIATE RISK ASSESSMENT OR “NOT APPLICABLE” MUST BE SELECTED FOR EACH QUESTION. IF THERE ARE QUESTIONS CONTAINING “ERROR” THE RISK RATING FOR THE CATEGORY AND OVERALL WILL BE WRONGLY CALCULATED!

3. The risk ratings to be used are:
 - **High** – Response to question indicates a risk to the effective functioning of the IP’s control framework that has a high likelihood of a potential negative impact on the IP’s ability to execute the programme in accordance with the work plan and stated objectives;
 - **Significant** – Response to question indicates a risk to the effective functioning of the IP’s control framework that has a significant likelihood of a potential negative impact on the IP’s ability to execute the programme in accordance with the work plan and stated objectives;
 - **Moderate** – Response to question indicates a risk to the effective functioning of the IP’s control framework that has a moderate likelihood of a potential negative impact on the IP’s ability to execute the programme in accordance with the work plan and stated objectives; or
 - **Low** – Response to question indicates a low risk to the effective functioning of the IP’s control framework and a low likelihood of a potential negative impact on the IP’s ability to execute the programme in accordance with the work plan and stated objectives.
 - **N/A** – *The specific question is not applicable for the IP and therefore no risk rating is assigned. It is not expected to be used regularly.*
4. The risk points column automatically assigns the points to each question based on the response given.
5. Points are assigned as follows:

Risk rating	Points: non-key questions	Points: key questions
High risk	4 points	8 points
Significant risk	3 points	6 points
Moderate risk	2 points	4 points
Low risk	1 point	1 point

6. Use the 'Comments' column next to each question to provide details of the basis for your assessment, and to highlight any important matters. This document will be referenced subsequently by the agency when performing additional assurance activities related to the IP. Sufficient details should be provided in this document for the agency to understand the rationale for your assessment.

Calculation of risk ratings per subject area section

For each individual subject area, as well as the overall rating, the risk points are totaled together to provide a score that then fits within one of the bandings for the risk ratings. The banding calculation method is that a low risk rating will be assigned to any sections or overall rating where the risk score is less than or equal to the lowest possible score (based on the number of applicable questions), plus 15% of the difference between the minimum and maximum possible scores. Moderate ratings are given on the same basis, but from more than 15% up to 30% of the range, then significant up to 50%, and anything over 50% is high risk. An example is set out in Note 1, below.

Note 1 – Method of assigning risk ratings to risk scores

As per paragraph 5, key questions are assigned double the risk points if the answer is other than “low” risk. Therefore, the risk rating assigned to the key questions has twice the weight in determining the risk rating for the section.

The Excel spreadsheet automatically assigns the risk rating by using the following algorithm:

1. Only the applicable questions are taken into consideration
2. The minimum possible points for the subject area are calculated, that is, if all questions are assigned low risk rating
3. The maximum possible points for the subject area are calculated, that is, if all questions are assigned high risk rating
4. The ranges for each risk rating banding are set out below:

Low risk	Minimum possible score plus 15% of the remaining available risk points
Moderate risk	Minimum possible score plus 30% of the remaining available risk points
Significant risk	Minimum possible score plus 50% of the remaining available risk points
High risk	Anything greater than 50% of the remaining available risk points

5. The actual risk points are matched with one of the four risk ranges to determine the overall risk category.

The same algorithm is applied when calculated the overall risk rating for the IP.

Assume the following two scenarios with the same risk rating for the questions.

1. Scenario 1: There are four non-key questions having equal weight
2. Scenario 2: The first question is key and the remaining three questions are non-key

Scenario 1	Risk Rating	Points
Question 1	Significant	3
Question 2	Moderate	2
Question 3	Low	1
Question 4	Low	1
Total Risk Points:		7
Min score	= 4 * 1	4
Max score	= 4 * 4	16
Low risk band (15%)	= 4 + ((16 - 4) * 0.15)	5.80
Moderate risk band (30%)	= 4 + ((16 - 4) * 0.30)	7.60
Significant risk band (50%)	= 4 + ((16 - 4) * 0.50)	10.00
High risk band (>50%)		= > 10.00
Overall risk	Moderate	7.00

Scenario 2	Risk Rating	Points
Key question 1	Significant	6
Question 2	Moderate	2
Question 3	Low	1
Question 4	Low	1
Total Risk Points:		10
Min score	= 4 * 1	4
Max score	= 4 * 4	16
Low risk band (15%)	= 4 + ((16 - 4) * 0.15)	5.80
Moderate risk band (30%)	= 4 + ((16 - 4) * 0.30)	7.60
Significant risk band (50%)	= 4 + ((16 - 4) * 0.50)	10.00
High risk band (>50%)		= > 10.00
Overall risk	Significant	10.00