Project Internal Control Assessment/Questionnaire (ICA/ICQ) Guide

November 2025

Table of Contents

Purpose of Internal Control Assessments/Internal Control Questionnaires

The purpose of the Internal Control Assessment/Internal Control Questionnaire (ICAs/ICQs) is to determine whether the partner has in place processes and tools to provide reasonable assurance about their capabilities to achieve project results:

- Operational — effective and efficient use of project resources to produce quality goods/services and to deliver results in a timely manner (outputs), including effectiveness in protecting the assets and resources of the partner.
- Compliance — compliance with policies, procedures, regulations, and institutional arrangements that are issued both by the government and the partner.
- Reporting — reasonable assurance on the reliability of financial, results, and regulatory reporting. Simply, UNHCR must ensure that partners have internal controls to track what is being provided to the forcibly displaced and stateless persons. This includes assurance that the partner has internal controls in place so that the resources it receives from UNHCR are used according to the partnership agreements and that no amount or quantity is diverted for other purposes.

The ICAs/ICQs[1] enable UNHCR to understand the risks of working with a particular partner and how to better mitigate the risks and assess how UNHCR can take advantage of strengths/opportunities identified where applicable.

---

[1] ICQ is different from the ICSAQ which is part of the FDY closing exercise, for further details on the ICSAQ refer to https://intranet.unhcr.org/en/support-services/financial-management/statement-of-internal-control---internal-control-self-assessment.html

Use of ICA/ICQ Results

The results of ICAs/ICQs should be used to:

- Determine the risk rating (low, medium/moderate, significant, or high) for the partner. The overall risk rating is used along with other available information to determine the type and frequency of assurance activities needed.

- Engage partners in discussion on internal control improvements required to comply with the partnership agreements.

- Consolidate the Internal Control Assessment (ICA) recommendations, to ensure they are reflected in the UNPP Integrity and Assurance Module (IAM). The detailed instructions can be found in the Standard Operating Procedures (SOP) on ICA and Audit Recommendations in the Integrity and Assurance Module of the UN Partner Portal (IAM/UNPP) available in the following.

- Insert any outstanding risks identified during the assessment within the Risk Register of the project workplan which is jointly developed with the partner via PROMS (follow PLAN-S9 3.docx for more details on the Project Reporting and Monitoring Solution (PROMS) process and access PROMS Software Tip-Workarounds for the workaround), implementing treatments as planned throughout implementation.

- Identify areas where UNHCR may provide support (e.g., training, additional project funding, mentoring) to strengthen the project management capacity of the partner.

- Identify the timing and nature of ongoing joint monitoring and project control activities for the projects with the partner.

Inquiries

For assistance or support in using this guidance note contact the Implementing Partnership Management Service at epartner@unhcr.org.

Assessing Internal Controls: The Importance of the Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control mechanism, providing discipline and structure. Control environment factors include:

- The integrity, ethical values, and competence of the people.
- Management's philosophy and operating style (tone at the top).
- The delegation of authority and responsibilities.
- Human resources policies and practices.
- Attention and direction provided by the Board of Directors (or applicable governance body).

Aspects of the control environment are often found in:

- Code of Conduct.
- Polices, especially personnel policies.
- Delegation of authority documents.

Remember that documentation is only a start—not the be-all and end-all. Try to understand the organization's attitude toward internal control. Is it a "necessary evil," or is it viewed as an integral part of the organization's management?

Background, Scope, and Methodology

Background

The project Internal Control Assessment/Questionnaire (ICA/ICQ) guide was developed, considering the harmonized ICA/ICQ with other UN agencies. However, the guide has been tailored to the specific UNHCR context. Therefore, some aspects of the Terms of Reference Professional Service -Macro Assessment have been considered in this guide.

Scope

The Internal Control Assessment/Questionnaire (ICA/ICQ) provides an overall assessment of the partner's programme, financial, Human Resources, and operations management policies, procedures, systems, and internal controls. It includes:

- A review of the partner's legal status, governance structures, and financial viability; programme management, organizational structure and staffing, accounting policies and procedures, assets and inventory, financial reporting and monitoring, and procurement.

- A focus on compliance with policies, procedures, regulations, and institutional arrangements issued by the Government and the partner.

Methodology

Through discussion with management, observation, and walk-through tests of transactions, UNHCR assesses the partner's internal control system with emphasis on:

- The effectiveness of the systems in providing the partner's management with accurate and timely information for the management of funds and assets in accordance with workplans and agreements with UNHCR.

- The general effectiveness of the internal control system in protecting the assets and resources of the partner. The ICA/ICQ results are discussed between UNHCR personnel and the partner before finalization of the report.

- The filled in matrix of ICA recommendations is downloaded from the UNPP IAM and is shared with the partner in PROMS, ensuring all MFT members are involved in follow up. The ICA recommendations process utilizes the "Document" and "Workflow" modules in Aconex, as outlined in PLAN-S9 3.docx.The link to PLAN provides more details.

PCOs and MFT members conduct the ICA/ICQ at the partner's office, including site visits if projects are being implemented (when applicable). The assessment primarily consists of interviews with partner personnel and a review of relevant documentation that is sufficient to complete the assessment questionnaire (please refer to the paragraph on ***"Steps on how to complete the Internal Control Assessment (ICA/ICQ) Template"***).

The ICA/ICQ provides an overall risk rating based on the four risk categories of the assessments below:

- **Low risk –** Indicates a well-developed financial management system and functioning internal control framework with a low likelihood of negative impact on the partner's ability to execute a project.

- **Medium/Moderate[2] risk** – Indicates a developed financial management system and internal control framework with medium/moderate likelihood of potential negative impact on the partner's ability to execute a project.

- **Significant risk** – Indicates an underdeveloped financial management system or internal control framework with a significant likelihood of potential negative impact on the partner's ability to execute a project.

- **High risk** – Indicates an underdeveloped financial management system and internal control framework with a high likelihood of potential negative impact on the partner's ability to execute a project.

The overall risk rating is used by UNHCR, along with other available information (e.g., history of engagement with the agency and previous assurance results), to determine the type and frequency of assurance activities as per the UNHCR Programme Handbook.

Using the ICA/ICQ Template during the assessment

There is no "one size fits all" system of internal control mechanisms for all organizations. A partner's organizational processes reflect a variety of factors, including: the level of maturity of the organization; operating environment; donor/funding agency requirements; and nature of the operation (e.g., legal services versus camp operations).

The description of the risk ratings to be used and the standard control activities outlined for each process may assist UNHCR PCOs in co-developing implementation monitoring recommendations ('issues' in PROMS) with the partner for joint follow-up and eventual closure.

---

[2] Throughout agencies' policies and systems, "moderate" and "medium" may be used interchangeably to describe the risk rating that falls between low and significant.

The filled in matrix of ICA recommendations is downloaded from the UNPP IAM and is shared with the partner in PROMS, ensuring all MFT members are involved for follow up. The ICA recommendations process utilizes the "Document" and "Workflow" modules in Aconex, as outlined in PLAN-S9 3.docx.The link to PLAN provides more details.

In addition, the potential high risk internal control processes specific to a project are discussed and entered jointly with the partner when developing the Project Workplan Risk Register via PROMS.

Steps on how to complete the Internal Control Assessment (ICA/ICQ) Template

The ICA/ICQ is divided into two parts (two Excel sheets/tabs) as follows:
The tab entitled "Information" is where the basic information about the partner is filled in as indicated. There is a hypothetical example provided in the ICA- ICQ Template.zip.

- *Information provided in this tab may be relevant for due diligence processes considering for example the disclosure of other sources of funding.*
- For row 17 of the tab "information" **Amount of UN funding by agency in last three years by":** This is an editable section where the UN donors and other non-UN donors are listed. **Below is the sample:**

Amount of UN and non-UN funding in last three years (in USD):	2023	2022	2021	
FAO				
UN Women				
UNDP				
UNFPA	600,000	500,000	450,000	
UNICEF	1,000,000			
WHO			125,000	
World Bank				
ECHO				
SDC				
Total	1,600,000	500,000	575,000	
Systems				

- ➢ **For a sample, please see above:** Programme and Technical Support Service (PTSS) would like to clarify that this section is editable. Non-UN agency donors, if known by the country operations, should also be listed with relative USD amounts.

- **How to deal with sensitive or confidential information;** It is possible to encounter situations where partners are not willing to share sensitive or confidential information. In such situations, UNHCR or the auditor will consider writing directly to the concerned section of the ICA/Q that the partner is not able to disclose such information and add reasons. This would be the preferred option because it will always be on the ICA, and no one will need to ask again what happened when reviewing the ICA. See below snapshot:

Location	Name of the City, Name of the Country			
Organisation				
Organisation type	Local NGO			
Key financial data for last three years as at financial year end:	2023	2022	2021	The partner did not share this info as it is confidential
Income (approx in US$)				
Expenditure (approx in US$)				
Income less expenditure (approx in US$)	0	0	0	
Net assets				
Number of physical offices in the country	2			
People				
Current number of employees	1150			
Activities				
Nature of activities	The partner is providing health services, distriputing CRIs, Shelter, and Multi-Sectoral Protection Assistance IDPs, Refugees, and Returnees.			
Locations of activities	The partner provides the activities in all Syria (14 governorates) through its own staff and sub-offices.			
Amount of UN and non-UN funding in last three years (in USD)	2023	2022	2021	
FAO				
UN Women				
UNDP				The partner did not share this info as it is confidential
UNFPA				
UNICEF				
WHO				
World Bank				
ECHO				
SDC				
Total	0	0	0	
Systems				

- ➤ It is further advisable to keep supporting documents such as email exchanges or NFFs that would further explain the background or context upon which the partner is not willing to share the information. Potential/current partner will be made aware that in absence of such information, UNHCR's ability to assess the capacity of the entity will be limited.

- The same applies to the tab "Questionnaire" example category A. Organization – question number 5 in row 10. If the partner is not willing to share minutes of the meeting, then this should be disclosed in column L, however, further alternative procedures could be performed, for example, if the assessment of the legitimacy of a partner is intended and they have the processes but cannot share the minutes. The partner could share at least proof of when the meetings take place (invitations to meetings), proof of participation, etc.

The information tab in the PDF version needs to be signed and dated by the auditors and partners. This means the auditors should submit the ICA in two copies to country operations: one signed, dated version in PDF and one in Excel that will be uploaded by UNHCR operation into IAM, using the ICA- ICQ Template.zip.

The tab entitled "Questionnaire" is where the following are the suggested steps to be followed in filling the ICA- ICQ Template.zip row by row.

- Columns A, B, C, and D – nothing to be filled in/changed as these are standard.

- Columns E, F, and G – please tick only one among the three options i.e., either "Yes" when the internal control in column C exists (positive), or "No" when the internal control in column C does not exist (negative). If the question in column C does not apply to a situation under review, then please tick "N/A" (not applicable) in column G.

- Columns H to K - please tick only one among the four options depending on the professional judgment based on the specific context being reviewed. Please refer to the paragraph below *(Annex 1: A sample ICA/ICQ Template)* for the contextual considerations while filling the ICA- ICQ Template.zip.

- Column L – this is where UNHCR/partner put comments (**Observation, Risk, Auditor Recommendation, Partner Response and UNHCR Response – refer to the snapshot below**) that would enable users of the ICA/ICQ, such as the partners, UNHCR - Operations, Regional Bureaux, HQ, Office of Internal Oversight Service (OIOS), United Nations Board of Auditors (UNBoA), project auditors and other relevant stakeholders, to understand how the rating conclusions were reached (low or medium/moderate or significant or high). Please refer to paragraph *(Methodology)* for the definitions. In all cases, UNHCR/partner should provide explanations even when column G has been ticked.

			Guidance	Yes	No	N/A	1 Low	2 Moderate	3 Significant	4 High	Comments
A. Organization											
General											
	1	Is the entity in compliance with national registration requirements?	*If the organization is a government entity, answer "N/A".* *For NGO / INGO / Other entity types, please record the legal status and date of registration in the country.*	✓					✓		Observation: Risk: Auditor/UNHCR Recommendation: Partner Response: UNHCR Response:
	2	Does an internet search indicate there have been no known cases of fraud, or other allegations of malpractice, concerning the entity or its staff in the last five years?	*The search should be performed using terms such as "fraud", "allegations", "abuse", and "criminal". When feasible this could include a search of public criminal databases depending on each country/state process for doing such a check etc. An example in Geneva: https://www.e-service.admin.ch/crex/cms/content/strafregister/strafregister_en*	✓					✓		Observation: Risk: Auditor/UNHCR Recommendation: Partner Response: UNHCR Response:

- Please note there are many different permutations in filling the ICA/ICQ Template based on the context and the collective judgement of UNHCR and the partner.

- An example of the Excel sheet Sample ICA - ICQ.xlsx that PTSS has taken from one of the completed ICA/ICQ conducted by an auditor where column L is properly completed in accordance with the structure shown in the above snapshot.

- For policy related questions throughout the ICA- ICQ Template.zip, ensure that a copy of the policy under review is obtained, briefly mention the topics covered in the policy, any topics that are not covered which should have been covered, if the policy is formally approved by the designated body and if the policy is being complied with.

- Please also avoid writing just – "No additional comments" or any other comments in column L of the questionnaire tab, that do not provide the reasons to justify the assessment rating (low or medium/moderate or significant or high or even N/A).

| | 3 | In the direction of confirming that there are no pending legal proceedings which may materially affecting the organization and its activities? | *To obtain and file the statement in writing, stating the name and position of the employee is higher than that of the doing, and the date on which it is made.* | ✓ | | | | | ✓ | | Observation - No additional commnets
Risk - n/a

Auditor recommendation - n/a

Partner Response - n/a

UNHCR Response - n/a |

- Writing only" See above" in column L of the questionnaire tab should be avoided as this is not a specific reference. In the questions assessed as (medium/moderate, significant, or high), full text should be inserted by copying and pasting the text from the row above. This will facilitate easy capturing of the recommendations in the IAM, hence facilitating the follow-up of such internal control-related recommendations as warranted. See the snapshot below:

| 5 | They are kept, the minutes of the meetings of the supervisory, examination of the plans and the timely follow-up? | | ✓ | | | ✓ | | | See above |
| 6 | The organization is structured in such a way as to allow for clear lines of communication, and assign specific areas of responsibility? | *To attach the organization chart of the organization.* | ✓ | | | ✓ | | | See above |

Note:

- If column G has been ticked, then leave the options available from columns H to K blank. The reason is, that if the situation is Not Applicable (N/A) then there is no need to provide a ranking (low, medium/moderate, significant, or high). However, it is good practice to comment in column L as to why the situation is N/A.

- To insert a tick/check mark (√) in columns E to K, UNHCR/partner can either copy and paste from the existing tick/check mark or click any of the cells and select from the dropdown menu. Furthermore, UNHCR/partner can select the cell and type the letter "a."

- If UNHCR/partner want to make any changes in columns E to K UNHCR/partner can also delete the inserted tick/check mark (√) by simply clicking delete.

After the ICA/ICQ Template which is available (in three different languages – English, French, or Spanish) is filled, then other reports will be automatically generated from the Integrity and Assurance Module (IAM). Please Refer to the below paragraph *"ICA/ICQ Reports from the Integrity and Assurance Module (IAM)"*

Further information on various aspects of ICA/ICQs based on input received from regional bureaus and the operations. Please refer to the webinar ICA/Q Deep-dive – PLAN 8 (pm/EN) ICAQ Deep-dive - PLAN 8 (PMEN)-20250617_151601-Meeting Recording.mp4 ICA/ICQ refresher session (Q&A) where various topics such as overview of the ICA/ICQ, presentation on procurement in ICA/ICQ, data Protection & Information Security, auditor's perspective on risks, IAM, ICA/ICQ in Aconex. The presentation also covers a subtopic - determining essential controls and the link with ICA/ICQ, please refer to the above the link where PTSS discusses about various scenarios (it starts from **1:28:12)** .

In addition, please find an example of an overview Flowchart -UNHCR - ICA – Process, that PTSS has obtained from an auditor.

Steps to follow to make sure that the ICA/ICQ is effectively completed

For the ICA/ICQ to be completed properly, correctly reflecting the true and fair views of the internal controls in place and the accurate assessment of risks (low, medium/ moderate, significant, or high), the following layers of processes should be considered:

1st Layer

1. The PCO should conduct meetings for individual partners under review to understand their processes and the process owners (if not yet known to the PCOs).

   - The PCO sends the ICA/ICQ template to the partner who will fill it out as a self-assessment. This is sent to the partner via Outlook email or using PROMS where the partner is registered in Aconex. The partner then sends back their completed ICA/ICQ.

2. It is considered good practice to utilize PROMS which documents the drafting and approval process, in case the partner is registered. The ICA/ICQ review process utilizes the "Document" and "Workflow" modules in PROMS. Click here for more details and here for the workaround process.

3. Alternatively, UNHCR would sit side by side with the partner and they would fill out the template together.

   - The PCO may request the partner to provide supporting documents/evidence as appropriate. A sample of the list of required ICA/ICQ supporting documents can be accessed through Sample of the list of required documents - ICA-ICQ.xlsx. However, the list is non-exhaustive, and depending on the interactions with the partner, more documents can be requested. Furthermore, it may depend on the modality upon which the partner maintained their supporting document, for example manually vs electronically.

2nd Layer

   - The PCO conducts additional checks on each category covered by the ICA/ICQ, paying attention to the questions (i.e., those highlighted in light blue) and the most vulnerable areas such as Personnel and Procurement. The Supply function leads the exercise surrounding procurement and warehouse management, while IT services lead the review of processes related to information security.

1. If required, and if already known to the operation, the PCO and Supply function would talk to former partner staff who have quit the organization and/or suppliers who have worked for the partner organization.

2. In operations where there is no dedicated Supply function, it is suggested that PCOs seek support or clearance on procurement-related processes review from the Regional Bureaux or MCOs. For HQ divisions, SMS could be contacted.

3rd Layer

- In some instances where there are inaccuracies detected in the ICA/ICQ; adjustments would be made based on a final meeting with the partner.

1. The draft ICA/ICQ is shared with partner for up to seven days for final comment ahead of finalization.

- The final ICA/ICQ report must be uploaded to the PROMS document register, document type 'Assessment Report,' selecting the drop-down label as Internal Control Assessment, for audit trail.

Furthermore, it is important that the partner receives the UNHCR draft ICA assessment, allowing further comment or additional supporting documentation before the finalization of the ICA. Moreover, the tab "information" within the ICA/ICQ Template should be used for listing the staff members involved in conducting the ICA. It is also used for signature by partner (signatory of the PW or a person delegated) and UNHCR. In general, for UNHCR, project control will sign as the preparer, and the direct supervisor (Representative or Deputy Representative) will sign as the approver.

Before submitting the finalized ICQ/ICA, the UNHCR Project Control or assigned auditor (as applicable) share the completed ICQ/ICA with the partner to acknowledgement the final assessment. The partner receives a specific deadline after which the Project Control or assigned auditor submits the report as final assessment.

A Sample ICA/ICQ Template

To be able to understand how to fill out the ICA/ICQ template, a Sample ICA - ICQ.xlsx is provided. It should be emphasized that this Sample ICA - ICQ.xlsx is one of so many possibilities for how the assessment/questionnaire can be completed. Please refer to the above paragraph "Steps on how to complete the Internal Control Assessment (ICA/ICQ) Template" on how column L should correctly be filled.

The exercise of filling out the Sample ICA - ICQ.xlsx is contextual which results in the possibility of having many permutations. The contextual matters relevant for each partner can be the operational environment in which the partner is operating (both internal and external context), objectives and activities, relevant stakeholders and how they may be affected by, or adding to the causes of risks, risks related to the management and operations plans and objectives and potential causes and consequences of risks. The Sample ICA - ICQ.xlsx can only show how the ratings have been determined in columns H to K i.e. (low or Medium/Moderate or Significant or high) based on the comments that are in column L. Depending on the partners' strengths and weaknesses and other factors noticed during the assessment, one would conclude on the appropriate rating.

Note: If the UN ICA/Q conducted uses a template that does not produce the same ratings and expected results, there will be a need to get a new ICA/ICQ completed using our harmonized template.

Quality Assurance (QA) of the ICAs (When conducted by UNHCR MFT)

As per the RASCI of regional bureaus, the Regional Controllers are responsible for ensuring that there are arrangements to conduct QA on ICAs of relevant countries of their region. The QA should be conducted as soon as the assessments are completed and uploaded into the IAM. RBs may conduct such QA following an MFT approach that may include other functions at the bureau such as controllers/project control, programme, risk advisors, supply, ICT, and others. RBs may consult or seek support from the relevant technical staff in HQ Divisions as required, such as DESS/SMS for supply DIST/ICT, and others, as necessary. The QA methodology can follow a risk-based approach that applies sampling from ICAs conducted throughout the region. For a sample size, the Regional Controller decides on the approach and the methodology to follow depending on the regional risk context. For example, in some locations at least 30% could be reasonable but it is up to the Regional Controller in the Bureau to decide.

PTSS has developed a QA checklist that shows the list of items to be checked during the ICA QA exercise. The QA checklist can be accessed through QA Checklist - Received ICA.docx The check list should be prepared for each ICA reviewed and properly uploaded in the PROMS document register for future reference and or audits.

The Regional Project Controller in coordination with the members of the MFT will determine the best timing to conduct the QA. However, if ICAs already uploaded into IAM need to be revised following the QA exercise, this will only require deleting the file already in IAM and uploading a revised ICA. Ideally, the QA on ICA should be conducted as soon as the ICAs are completed and uploaded into the IAM by the operations. This will enable the operation to promptly address any concerns that may be raised from the QA by the bureau.

If the QA identifies inconsistencies or errors in the ICA conducted/completed the ICA needs to be revised by the operations following the recommendations of the RB QA review MFT and the revised ICA will be uploaded to IAM again with a new issuance date. When the ICA has been revised, the date to be considered is the revision date of the ICA. PTSS can help remove the previously uploaded ICAs to allow operations to re-upload the revised ICAs.

The RB QA should aim to provide strategic oversight and ensure the consistency, reliability, and quality of the ICA process. Once the QA is completed, Operations must be promptly informed to address any identified weaknesses or areas for improvement. This allows for necessary adjustments, including updates to the ICA rating or the PW, to be implemented efficiently.   For reference, please consult the UNHCR Programme Handbook under the title "Internal Control Assessment".

When HQ divisions and entities conduct their ICAs, PTSS will undertake the QA of the ICAs from HQ. PTSS will provide guidance and support to RB QA MFT where needed.

PTSS will on a sample basis, select the QA Checklist - Received ICA.docx completed by RBs and perform the QA. TPSS will then share the results of the QA with the view of improving the quality of QA exercise.

For Information Technology (IT) related questions, the specific QA evaluation criteria have been developed, IT Related Questions ICA Guidelines in a (PowerPoint presentation) that provide details on how to go about reviewing the specific IT-related questions. The presentation can be accessed through ICA ICQ presentation - 18 Nov-2024 - IT Related Questions.pdf

Note: For ICQs conducted by auditors as part of audits, PTSS on a sample basis, will perform the QA of the ICQs. However, auditors may opt to conduct the QA using the QA Checklist - Received ICA.docx

 If the auditor decide to conduct the QA using the QA Checklist - Received ICA.docx, they may submit them during the review of QA of the KPI#2 – Audit Quality together with the Audit Working Papers (AWPs).

When the auditor conducts ICAs as part of the advisory, they may submit the QA Checklist to the UNHCR operations together with the final ICA-ICQ. It is recommended that the auditor(s) who perform the QA exercise, should be different from the one who prepares it to maintain segregation of duties hence independence in the QA review process.

Accepting of an ICQ from other UN agencies (or a micro assessment)

Where an operation proposes to accept an ICQ from other UN agencies (or a micro assessment), we propose to use the template Details from Micro assessments and ICQs from other UN Agencies - Template - 1st October 2024.xlsx, in order to see how the assessment report received compares with the UNHCR ICQ and also for PTSS to be able to reflect this within the tracking tools and the UNPP/IAM (tbc). This is a temporary solution as we continue to work with other UN agencies on how to share the audit certificates (including ICQs/micro assessments) via the UNPP.

ICA/ICQ Reports from the Integrity and Assurance Module (IAM)

Once the completed soft/excel ICA/ICQ template is uploaded into IAM by Project Control or the UNHCR focal person following the guidelines provided in How to upload ICA in IAM.pdf, the **ICA Summary Report**, summarizing the results of the main eight ICA/ICQ processes found during the assessment, will be generated by clicking the Export ICA Data (please refer to the below screenshot), The report will be recorded and monitored in collaboration with the partner via PROMS.
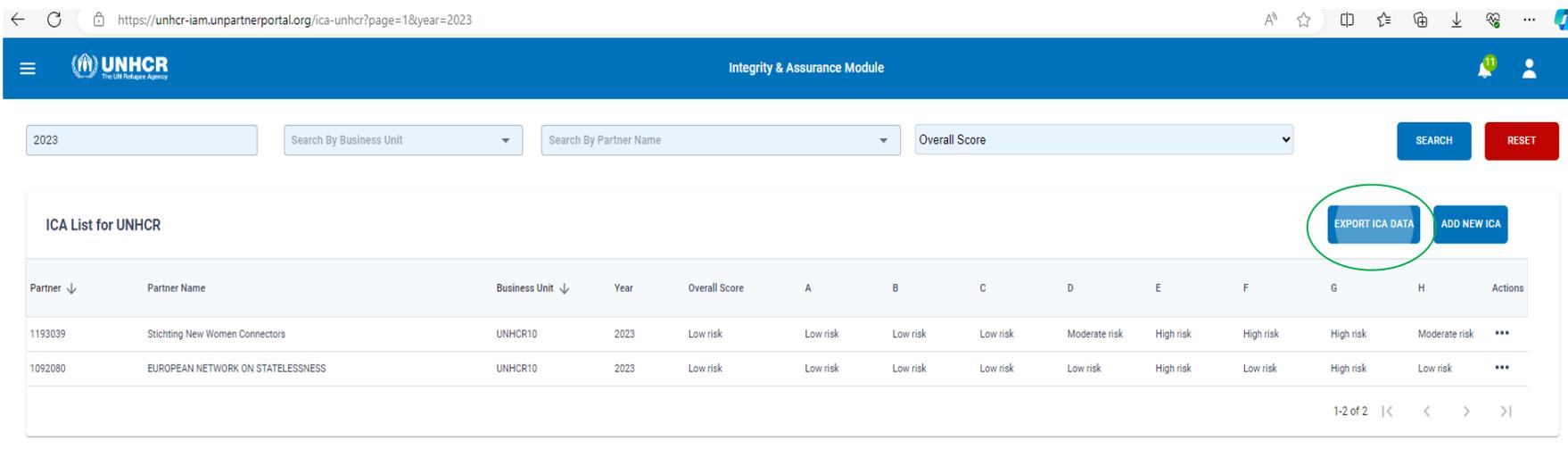
Note: Relevant supporting documents as evidence of the responses given by the partner will be uploaded and stored in PROMS, for future reference and accessibility by auditors, DEPS/PTSS, RBs, and country operations, as applicable. For the naming convention of such documents, an example is "ICA-2024-B9-Procurement Policy". It is important to reference the process that the supporting documents refer to, in this case, B9.

Which supporting documents should be stored in PROMS?
For archiving the supporting documents reviewed during the ICA process. The recommended approach includes considering, 1. Documents frequently requested from the partners, for example, the policies, manuals, certificates of incorporation, organograms, etc. 2, Procurement-related documents 3. Supporting documents for important findings, for example where processes are rated as medium/moderate, significant, or high risk.

ICA/ICQ Further guidance and examples

This section provides further guidance on how to use the ICA/ICQ Guide. It is divided into 3 major areas as follows:
- Assignment of points
- Risk assessment matrix
- Detail ICA/ICQ examples for each category

Assignment of Points

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

Note:
1. The same assignment is applied to all categories of the ICA/ICQ.
2. Key questions are those highlighted in light blue in the ICA/ICQ template.

Example of category A. Organization – determination of the category risk rating

There are 9 questions in Category A: Organization of the ICA/ICQ. There are 2 key questions which carry more weight than the remaining 7. The key questions are marked with an Asterisk symbol (*) in column A and they are highlighted in light blue. All key questions carry double the weighting of other questions except those with a low-risk rating. For example, if all 9 questions in Category A: Organization in column I are selected, then the first 2 questions (key questions) will each be multiplied by 2. The table above is "Assignment of points".

Risk assessment matrix

The risk assessment matrix provides an overview of how each question should be assessed and rated (refer to columns H to K of the ICA/ICQ template). Please see below an example of question B1 (i.e., the first question in Category B. People and behaviours) where different scenarios are provided, and the risk assessment matrix is used.

Question B.1: Is there an HR manual that covers key areas such as recruitment, employment, and personnel practices, and which is provided to all staff?

The user can select 1 out of 4 ratings (low or medium/moderate or significant or high in columns H to K of the ICA/ICQ template). This selection should be made after the user has selected/ticked either column E "Yes" or column F "No." No rating is required if column G "N/A" is selected/ticked.
In assessing this question (the same applies to all ICA/ICQ questions), one must consider the impact (potential consequences or damage that a problem can cause if it occurs) and probability (the likelihood of a potential risk occurring). Please refer to the matrix table below that shows how the severity of a risk is gauged using the qualitative values.

Please see below for examples of scenarios, related to question B.1, and the risk rating that would correspond to each scenario described.

Kindly note that these scenarios would have to be adapted to the specific context.

- **Scenario 1:** Lack of formal policies/SOPs or inadequate formal policies/SOPs covering HR best practices – ***High***

- **Scenario 2:** Existence of policies or SOPs that have not been formally approved or do not cover important HR elements, thus they are not capable of being consistently applied – *Significant*
- **Scenario 3:** Existence of policies or SOPs with some minor gaps in the provisions on HR best practices or they are inconsistently applied – Medium/*Moderate*
- **Scenario 4: All HR factors are covered and there is a consistent application of policies/SOPs (only limited situations of departure from policies/SOPs) – Low**

A risk assessment matrix is a qualitative method of risk analysis that helps define the severity of a risk/acceptability of a risk.

The severity of a risk = Probability x Impact

IMPACT				
Very High	Significant	High	High	High
High	Significant	Significant	High	High
Medium/Moderate	Medium/Moderate	Medium/Moderate	Significant	Significant
Low	Low	Low	Medium/Moderate	Medium/Moderate
	Rare	**Unlikely**	**Possible**	**Frequent**
	PROBABILITY			

Impact

- **High** – significant control weaknesses exist that could expose the organization to significant financial or other risks such as operational fraud. fiduciary etc. Occurrence can cause obstruction to the business hence not being able to achieve its main objectives.
- **Significant** – significant control weaknesses could expose the organization to unacceptable/inadequate levels of unmanaged risk. The achievement of main objectives will be hindered, considerable extra time and resources will be required.
- **Medium** – although a small number of control weaknesses exist, there are compensating controls and other mitigating factors in place to reduce the risk within the organization to acceptable levels. This implies that main objectives can be achieved, but not as well as planned and/or extra time resources will be required.
- **Low** – strong controls exist given the inherent business risks. This implies that main objectives can be achieved with small obstacles to overcome.

Probability

- **Rare** – likelihood of occurrence of an adverse event associated with the risk is rare or would only occur in exceptional circumstances.
- **Unlikely** – likelihood of occurrence of an adverse event associated with the risk might occur because the conditions for it exist, but controls are in place and are effective.
- **Possible** – it is likely that an adverse event associated with the risk will occur because the controls are inadequate or applied inconsistently.
- **Frequent** adverse events associated with the risk are expected to occur. There is certainty of occurrence because the controls do not exist or are ineffective.

Detailed examples per ICA/ICQ category

The tables below provide a selection of questions (all key questions and some non-key questions) from all categories of the ICA/ICQ template. For each question, there are examples of good practices, sources of evidence, and hypothetical scenarios with their recommended risk level. These tables can be used as a guide for filling out the ICA/ICQ template. It is suggested that when reading the examples below, one should consider the above risk assessment matrix as a guide for the consideration of other scenarios that could be relevant to the context.

A. Organization

Question	Good Practices (low risk)	Sources of evidence for good practices	Hypothetical scenario with the recommended risk level
Q1: Is the entity in compliance with national registration requirements?	There is a clear mandate through a legal act and/or other administrative decisions *(depending on the jurisdiction).*	Copies of the following: • Non-Governmental Organization Act. • Act of Parliament in case of a government entity. • Certificate of registration. • Renewal of mandate (if applicable).	The partner is set up by a Non-Governmental Organization Act. The actual setup and operationalization of the partner commenced in 2015 after obtaining the certificate of registration which is still valid to date. In such a scenario, the suggested risk rating is **Low.**

Question	Good Practices (low risk)	Sources of evidence for good practices	Hypothetical scenario with the recommended risk level
Q2: Does an internet search indicate there have been no known cases of fraud, or other allegations of malpractice, concerning the entity or its staff in the last five years?	• The partner has methods and approaches for information searching such as data mining or matching exercises. • The partner works to integrate the biometric National ID System with other agencies systems in efforts to ensure more effective service to the forcibly displaced and stateless persons.	• Internet search. • UN Resolution 1367. • Dow Jones. • Any other source relevant to the context.	From the internet search, there were no known cases of fraud implicating the partner and/or its staff. There was mention of the partner confiscating identity cards which some refugees and asylum seekers had obtained illegally and fraudulently. This indicates positive steps in standing against fraud and illegalities. In such a scenario, the suggested rating is **Low.**

B. People and behaviours

Question	Good Practices (low risk)	Sources of evidence for good practices	Hypothetical scenario with the recommended risk level
Q1: Is there an HR manual that covers key areas such as recruitment, employment, and personnel practices, and which is provided to all staff?	• Complete and adequate HR manual exists and is updated, as necessary. The procedures and manual cover all HR key activities including recruitment, employment, and personnel practices. • In case HR activities are outsourced, procedures and arrangements are in place to effectively monitor and supervise the delegated tasks, including reporting mechanisms.	• Copy of the HR manual. • Sample of personnel recruitment. • Contracts for outsourced activities (if relevant).	The HR manual exists but does not adequately cover direct staff promotions. However, the management confirmed that the recruitment procedures and practices embraced transparency and competition. Partner lacks clear criteria for promotions. In such a scenario, the suggested rating is **Significant.**

Question	Good Practices (low risk)	Sources of evidence for good practices	Hypothetical scenario with the recommended risk level
Q7: Does the finance team contain a sufficient number of suitably experienced staff, so that team members are competent to perform the tasks assigned for them and with sufficient segregation of duties?	There is a segregation of duties between authorization, custodianship, and recording of transactions.	• Copy of the finance manual. • Copy of the finance organogram. • Sample of financial transactions. • Copies of the finance teamwork plans.	The finance function is headed by a Principal Accountant (PA), who reports to the Chief Executive Director. The PA is assisted by 1 Senior Accountant and 2 Accountants, moreover, there are 2 Assistant Accountants. The authorization, custodianship, and recording of individual transactions are performed by different staff within the finance team. In such a scenario, the suggested rating is **Low.**

Question	Good Practices (low risk)	Sources of evidence for good practices	Hypothetical scenario with the recommended risk level
Q10: Does the organization have a clear set of policies concerning the expected conduct of its staff, and procedures to follow up on allegations of misconduct?	• Staff understand the standards of conduct required and their personal responsibility in preventing fraud, corruption, and conflict of interests. • Staff participate in training and awareness-raising activities on tackling fraud, corruption, and conflicts of interest. • There are internal and external whistle-blowing procedures in place. • Partner staff understand the importance of controls, where and how they should report suspicions of fraudulent behavior, corruption, conflict of interest, or control weaknesses.	• Copies of evidence of fraud awareness training conducted. • Copies of a signed declaration of independence, non-disclosure of confidential information, and elimination of conflicts of interest. • Copy of the description of the methods available for reporting on allegations.	All staff are guided by the written policies on the prevention of fraud, corruption, and conflicts of interest. Further, the written policies provide guidelines on reporting fraud and misuse of resources. The policies have provisions for protecting whistleblowers from retaliation and victimization. Management indicated that they had advised staff on the provisions of the policies with respect to reporting on fraud, waste, and misuse of resources. The members of staff are advised to report to the committee in confidence if they suspect any fraudulent activities. Systematic trainings are in place to ensure consistent knowledge of the policy across the organization. In such a scenario, the suggested rating is **Low.**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q11: Does the organization have an anti-fraud and anti-corruption policy that is readily accessible to all staff?	• The partner has up-to-date anti-fraud policies (clearly and fully covering all the necessary elements of measures to prevent and detect conflicts of interest), implementation plans, and manuals in place.	• Copy of an up-to-date written policy covering all necessary elements of fraud. • Adequate explanations of the defined arrangements for tracking the elements of fraud. • A register tracking the fraud allegations.	**Same as above for Q10:** All staff are guided by the written policies on the prevention of fraud, corruption, and conflicts of interest. Further, the written policies provide guidelines on reporting fraud and misuse of resources. The policies have provisions for protecting whistleblowers from retaliation and victimization. Management indicated that they had advised staff on the provisions of the policies with

• In cases not specified in the anti-fraud policies, partners have defined arrangements for tackling fraud, corruption, and conflicts of interest with the support of senior management and allocation of appropriate resources.	respect to reporting on fraud, waste, and misuse of resources. The members of staff are advised to report to the committee in confidence if they suspect any fraudulent activities.
• Staff understand the standards of conduct required and their personal responsibility in preventing fraud, corruption, and conflicts of interest.	In such a scenario, the suggested rating is **Low,**

C. Activities

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q1: Does the organization have and use sufficiently detailed written policies, procedures, and other tools to develop and manage programmes and plans?	• The partner has adequate controls in place to track project results. • The partner does monitor their own activities, and those of sub-partners, properly to ensure that the project is progressing as planned.	• Acts and regulations in the case of a government partner. • Partner strategic plans. • Annual work plans. • Annual performance reports.	• The partner had a clear mandate in its programming activities, guided by the Act and its Regulations and the Strategic Plan (SP) for 2019 - 2024. • The annual work plans were derived from the SP, and these were prepared for every financial year. In such a scenario, the suggested rating is **Low.**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q4: Does the organization identify the potential risks for achieving its objectives and programme delivery and mechanisms to mitigate them?	The partner has established the mechanisms and tools to manage the overall risk management of programme delivery and mechanisms to mitigate them.	• Risk register • Business continuing plan. • Programme procedural Manual	The potential risks for program delivery and mechanisms to mitigate them were not clearly identified in the Strategic Plan and the partner had no matrix of the program risks and the mitigation measures. In such scenario the suggested rating is **High.**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q7: Does the organization have and use sufficiently detailed policies, procedures, guidelines, and other tools for monitoring and evaluation?	Effective procedures are in place to ensure monitoring and follow-up of the recommendations and corrective measures resulting from oversight and substantive testing.	• Monitoring and evaluation guidelines • Tools for monitoring and evaluation • Templates to track the progress of activities undertaken. • Staff trainings	• The partner had monitoring and evaluation guidelines for its programs. It developed specific tools for monitoring and evaluation of its work based on donor requirements. • The partner had templates to track the progress of the activities being undertaken. On this, there is a Monitoring and Evaluation Officer (MEO) who works together with partners and uses various forms that guide the officer in undertaking the work. In such scenario the suggested rating is **Low.**

D. Reporting and Accountability

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q1: Is there a finance manual, or similar, that clearly sets out the main policies and procedures to be followed?	Partner has up-to-date finance manual clearly and fully covering all the necessary elements such as cash disbursements, - (cheque authorization, bank reconciliations, purchases, payroll, and taxes therefrom, travel expenses, consultants). Others including, administration expenses capital equipment, budget, maintenance of books of accounts, adequate segregation of duties etc.	• Copy of an up-to-date finance manual • Review of sample of expenditure transactions	The partner has a finance manual in place, and the test of the transactions revealed that policies and procedures are adequately followed. The finance manual has not been updated for the past 3 years to accommodate some few changes that have occurred there since. However, the changes are not significant. In such scenario, the suggested rating is **Medium /Moderate.**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q2: Has the organization complied with its statutory reporting requirements for the last three years?	• Statutory deductions such as Pay-as-you-Earn (PAYE), are submitted before the deadlines to the relevant authorities. • Other reporting requirements to the regulatory bodies covering areas such as environmental requirements are timely submitted.	• Copies of the correspondence from the regulatory bodies. • Copies of payment vouchers on statutory deductions • Copies of certificates from the regulatory bodies • Copies of fines paid to the regulatory bodies for late submissions.	Through test of transactions and documents, meetings with the management. The partner had submitted all the required reports and statutory deductions. In such scenario the suggested rating is **Low.**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q4: Has the organization received UN audit reports, or other assurance activities commissioned by UN organizations, which report a good control environment, and without significant amounts of unsupported expenditure being identified?	• The audits are performed in accordance with the last updated audit strategy, are based on a clearly described audit methodology including a proper risk analysis and consider the internationally accepted auditing standards. • Control systems in place give the necessary assurances that the funds were managed in accordance with all applicable rules; and used for the intended purpose as defined in the PW.	• Copies of the audited financial statements and management letters. • Copy of the unmodified opinion • Copy of the Internal Control Questionnaire/Assessment (ICA/ICQ)	The management did not provide the audited financial statements and the management letters during the review. In such scenario the suggested rating is **High.**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q11: Are budgets prepared in sufficient detail so that they can be used as a meaningful monitoring and control tool?	Budgets are prepared for all activities in sufficient detail to provide a meaningful tool for monitoring subsequent performance.	• Minutes of the meetings where budgetary issues are discussed by all stakeholders. • Copy of the budgets. • Copy of the budget preparation policy and procedures including stated budget ceiling. • Copy of the minutes board of directors/trustees.	For the UNHCR funded activities budget was prepared in a participatory approach, all relevant stakeholders (MFT) were involved led by the Programme Manager, and thereafter a consolidated budget with sufficient details to provide a meaningful tool for monitoring subsequent performance. In such scenario the suggested rating is **Low.** An example of assessing entities budgeting processes with no UNHCR funding history should be captured here.

E. Assets and Inventory

Fixed Assets

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q1: Does the organization maintain a comprehensive and up to date fixed asset register, that records all relevant details (such as purchase date, cost, condition, location, tag number, serial number, and owner) for each asset held?	• A fixed asset register is maintained for tracking and storing assets information; either online or on a spreadsheet depending on the size of an organization. • The register should contain various details such as the asset name, tag number, condition of each asset, date of purchase, custodian of the asset, the last service date (if relevant), disposal date, etc.	• . Asset card(s). • Fixed assets register. • General ledger for the maintenance of expenses.	The organization does not have a fixed asset register and not even a list of assets. In such a scenario, the suggested rating is **High.**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q2. Are there sufficient measures and procedures in place to protect assets from theft, damage, or misuse?	Policies or SOPs on: • Asset management. • Warehouse management. • Guidance on asset and warehouse management.	• Existing policies, SOPs, or guidelines.	Evidence of the existence of assets and periodical monitoring reports, asset physical verification reports In such a scenario, the suggested rating is **Low.**

Insurance

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q3. Are significant assets either insured, or can otherwise be readily replaced, in the event of theft or damage?	• Facilities/Office Insurance • Warehouse Insurance • Transportation Insurance • Existence of policies/SOPs on handling damaged/stolen assets	• Evidence of insurance policies.	The facilities/office and warehouse are insured by a commercial insurance service provider. However, the partner has not provided evidence of transportation insurance. In such a scenario, the suggested rating is **Significant.**

Verification

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q4. Are assets subject to at least annual physical verifications?	• Mandatory physical verification of operational assets at least once a year. • Regular inventory check of assets in storage.	• Guidelines/SOPs for verifications and scope of stock count. • Evidence of past verification exercises Refer to the ICA /ICQ Template	Mandatory physical verification of operational assets is conducted annually. Moreover, there are regular inventory checks of assets conducted at least twice a year. In such a scenario, the suggested rating is **Low.**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q5. Are the physical verifications performed by the person other than responsible one (segregation of responsibilities) than one person, and are the	• Records of discrepancies from verifications are archived. • The partner performs root cause analyses for recurrent discrepancies.	• Verification guidelines/SOPs. • Verification reports.	Physical verifications are conducted at least twice a year but only by the Stores Clerk. The necessary adjustments are carried out but not appropriately documented and approved. In such a scenario, the suggested rating is **Significant.**

Question	Good Practices (low risk)			

results, and any necessary adjustments, appropriately documented and approved?	• Records of remedial measures for discrepancies are archived.		

Inventory

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q6: Is inventory managed through a computerized system that provides an up-to-date picture of items held?	• The partner has SOPs in place with segregation of duties (i.e. (I) incoming and outgoing approver and (ii) warehouse management roles are assigned to different persons). • Either by using software, or a simpler computerized tool, all the items held in stock are appropriately recorded, and the stock balances are updated on time when confirming the inventory transactions. The process should facilitate monitoring the stock by status (ready to be used, damaged, on hold, etc.).	• SOPs for inventory activities. • Stock balance position by item, status, and date. • Bin/stock card • Inventory Records (Purchase Order documents, waybill, receipt note, issuing note). • Software used for inventory management.	**High / significant Risk:** Partner does not have a computerized system to manage the inventory, tools are manual, there are no SOPs, and no segregation of duties can be ensured, resulting in unreliable data, lack of accuracy of the records and inaccurate stock status and quantities, affecting the capacity to respond relying on inventory items. **Medium/Moderate Risk:** The partner does not have a computerized system or software that records the levels of stock and enables automated and electronic monitoring and recording of inventory transactions. However, the partner has manual records and has standard operating procedures for inventories in place, showing appropriate internal organization to manage and record inventory transactions. Despite having SOPs, it is recommended to enhance the systems, especially if the quantities and value of inventory goods are large, as manual processes can jeopardize accuracy of records and result in unreliable stock status and quantities.

			Low Risk: The partner has clear SOPs for inventory management, detailing a segregation of roles, and uses a software or computerized tool enabling appropriate monitoring of inventory transactions, and efficiently supporting responses and decisions based on reliable data about inventory items.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q7: Are physical verifications of inventory items reconciled to the records held on a sufficiently frequent basis, and the results, and any necessary adjustments, documented and approved?	• The partner regularly defines an inventory verification calendar of activities. The frequency is determined by the operational context, the rotation and type of goods stored, and the performance results of previous verifications. As a minimum, one annual physical verification is to be conducted. In the case of big warehouses, the cycle counts are to be implemented. • There are instructions to perform physical verifications detailing a) the roles of each actor (inventory manager, counting team, and verification team), b) preparation activities (work plan, warehouse freeze, warehouse preparation), c) reconciliation and update of pending transactions, d) counting process, identification of	• Inventory verification calendar of activities. • Physical verification reconciliation report. • Inventory Count Sheets. • Baseline Stock Reports. • Records of Discrepancies Records for Adjustments.	**High Risk:** The partner consistently fails to plan and implement the defined physical verification schedule, and there are no detailed instructions on how to perform and reconcile the physical verification of inventories. Adjustments are overlooked and mistakes are not corrected. Additionally, there is no segregation of roles during the verification process and timelines are not respected, resulting in poor and inaccurate inventory data. **Low Risk:** The partner operates with an inventory verification calendar of activities, determining regular inventory verifications in compliance with the minimum annual requirements. Instructions on how to conduct the physical verification, including roles, reports to be used, and tools to record the reconciliation results are appropriately described in internal guidance documents. The partner ensures these documents are accessible and guides all personnel involved in inventory management verification activities.

	discrepancies, resolution, and adjustment.		

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q8: Are items with a limited shelf-life sufficiently monitored to ensure they do not expire prior to issue?	Items are managed using the First in First Out (FIFO) approach, considering for the First in Date, the date that the items were received by the partner in any location and not just in the warehouse that currently stores those items. Reference to the UNHCR Intranet is https://intranet.unhcr.org/en/about/unhcr-manual/a-content-page/ch08-supply-chain-management/glossary-of-supply-terms.html. • For perishable products, the First Expired First Out (FEFO) approach is used. • A consolidated list of items by warehouse with the shelf-life status is regularly reviewed and updated with main stakeholders. • Good warehouse conditions ensure proper storage of the goods, including cold-chain or controlled temperature facilities or equipment (I.e., tags to indicate temperature deviations)	• Lot information of the items under inventory. • Packing list for Purchase orders. • Shelf-life information of the item as per the Product technical sheet. • SOP for inventory and warehouse management. • Goods receiving notes issued at different warehouse locations to validate the First in date.	**Significant Risk:** The partner does not use the FIFO approach adequately resulting in dispatching and delivering expired items or goods with short shelf-life that might not be useful or safe for consumption. The required warehouse conditions are not properly maintained so the goods may be damaged before their expiry date and hence not useful anymore affecting distribution and responses. In both cases, goods may not meet the conditions to be safely used and distributed,

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q9: Are the warehouse facilities sufficiently secure, providing suitable conditions for the items held, with adequate protection against environmental factors?	• A feasibility study to design the partner´s warehouses has been used, including at least the following considerations: a) political, environmental, and operational considerations, b) delivery of goods, c) location, and d) another special requirement related to the storage of goods under inventory. Partner's warehouses consider the development of internal protocols containing information on the warehouse access controls (including management of keys). This includes security measures, such as a logbook to conduct routine checks and record security incidents. Such internal protocols should include an evacuation plan as well. Partner's warehouses comply with fire safety precautions, to ensure that facilities comply with Fire Safety standards.	• SOP /guidelines on physical inspections • Results of the warehouse Feasibility Study or similar assessment. • Copies of Security protocols, and evidence of compliance with Fire Safety standards. • External assessments or inspections conducted by public authorities e.g., Fire Safety authorities. • Quality Certificates for ISO standards, or similar certificates on warehouse management. • Internal Protocols on access to the warehouse.	**High Risk:** The warehouses are not located in adequate facilities following appropriate feasibility studies, and they are not managed in accordance with minimum safety standards and measures. This means that goods stored may be stolen or damaged.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q10: Are warehouse items maintained in a way that allows authorized persons safe and ready access to them?	• Partner's warehouses consider the development of internal protocols containing information on the warehouse access controls, including security measures, such as the use of a logbook to conduct routine checks and record security incidents. • Access to the warehouse during working hours is restricted to the main entrance of the building and limited to those staff whose duties require it. The custody of keys is controlled. • In the warehouse, there is a list containing the names and numbers of personnel accessing the facilities, to assist the headcounts of personnel in case of an emergency. • Partners ensure that only authorized personnel will be permitted to enter the warehouse or to receive items to be stored in the warehouse.	• SOP /guidelines on physical inspections. • List of authorized personnel. • Internal Protocols on access to the warehouse.	**Significant Risk:** The warehouses do not have appropriate protocols or documentation defining the warehouse access controls. Therefore, the facilities could be accessed by unauthorized personnel, hence exposing the facilities and the goods stored to damage, theft, or inappropriate distribution.

F. Procurement

(All questions related to procurement have been considered below (refer to column C and D rows 98 to 108)

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q1: Does the Organization have written procurement policies and procedures, which facilitate competition, transparency and obtaining value for money?	The partner has written procurement policies and procedures reflecting the best international standard, like the UN Procurement Manual.	• Procurement Manuals. • Guidelines / SOPs • Templates for different types of tenders. • Templates for evaluation reports. • Templates for contracts. • Procurement Plan template. • Vendor Performance Review template. • Other relevant templates for successful procurement management.	**Low risk scenario (also described in ICA/ICQ Template):** The Partner has procurement policies and regulations which meet the best international standards, for example UN Procurement Manual. All procurement actions are fully and transparently documented. Well-designed procurement forms reflect each step of the procurement process and allow for the effective management of procurement activities including procurement planning processes of the Organization. Complete and adequate documentation exists to serve as the basis for vendor accountability and will be required in case of disputes or claims, as well as for an audit trial and lessons learned. In addition, the Partner proactively pursues Sustainable Procurement. The procurement manual/practices have been reviewed and updated. **High risk scenario:** There is no clearly defined procurement policy within the organization, or the found policies introduce a substantial risk, jeopardizing the effectiveness and transparency in handling procurement and vendor interactions. This deficiency increases the probability of spontaneous purchase decisions, potential budgetary excesses, irregular supplier oversight, and the absence of standardized processes. Such shortcomings have the potential to result in financial inefficacies, non-compliance concerns, and a compromised capacity to achieve strategic objectives.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q2: Do the procurement policies specify appropriate thresholds at which points different procurement procedures apply?	The Organization uses well-defined and easily understandable criteria when determining whether to use informal or formal solicitation methods, without affecting the provision related to the waiver of competitive bidding. When the Organization conducts procurement with UNHCR funds, the threshold that prompts the use of formal solicitation methods should closely align with the thresholds that are widely recognized as good international practice by UNHCR for the specific region.	• Procurement Manuals. • Guidelines / SOPs. • Other relevant templates for successful procurement management.	**High risk scenario:** The partner exercises discretion without employing clear and explicit thresholds for determining the use of informal and formal solicitation methods. When the partner engages in procurement with UNHCR funds, there are no predefined thresholds to initiate formal solicitation methods, and the partner does not conform to any standards regarded as good international practice, acceptable to UNHCR in the specific region.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q3: Are all procurements authorized through documented approval from an appropriate member of staff?	Clear delegation of authority system exists in the Organization, supported by relevant templates and forms (digital or offline), and is continuously followed.	• Procurement Manuals. • Guidelines / SOPs. • Contracts and TORs of relevant staff. • Templates and archived documentation demonstrating staff authorities.	**Low risk scenario:** A clear and efficient delegation of authority system is firmly in place, supported by relevant templates and forms, available in digital and/or offline formats. This system ensures that roles and responsibilities are clearly defined and distributed across various levels and/or departments. **High risk scenario:** The delegation of authority system does not exist or is unclear and inefficient, lacking any relevant templates or forms. Roles and responsibilities are not defined or vaguely defined and not distributed consistently across various levels or departments.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q4: Is there adequate segregation of duties in the procurement process?	Segregation of duties is adequately reflected in the regulations and is continuously followed.	• Procurement Manuals. • Guidelines / SOPs. • Contracts and TORs of relevant staff. • Templates and archived documentation demonstrating segregation of duties.	**Low risk scenario (also described in ICA/ICQ Template):** The Partner's regulations reflect the principle of segregation of duties between requisitioning and procurement entities by specifying their separate and distinct functions within the overall procurement process and finally between the entity that executes the payment. **High risk scenario:** The Partner's regulations fail to establish a clear segregation of duties between requisitioning and procurement entities, as they do not specify separate and distinct functions within the overall procurement process, nor do they differentiate between the entity responsible for payment execution.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q5: Is there a stated basis for the assessment of bids, and is this followed in practice and documented?	The Organization evaluates offers promptly after the deadline, using well- defined evaluation rules and templates, and engaging adequate staff with appropriate knowledge.	• Procurement Manuals. • Guidelines / SOPs • Templates for evaluation reports. • Examples of evaluation reports.	**Low risk scenario:** The Partner organizes a systematic and impartial assessment of submitted offers in a transparent and objective manner. A well-defined set of evaluation criteria tailored to the project's specific requirements is being used. Evaluation teams, composed of subject matter experts review and score each offer based on these criteria. Additionally, a clear process of weighing the criteria to reflect their relative importance and a rigorous scoring methodology ensures fairness and consistency. Open communication and documentation of the evaluation process and results contribute to maintaining transparency and accountability. The selection of the contractor is based on a thorough and unbiased

analysis of all offers, fostering trust and confidence in the procurement process.

High risk scenario: The Partner conducts evaluations that compromise transparency, fairness, and objectivity of the process. These may involve a lack of transparency in criteria and process communication, allowing bias, changing criteria midway, non-compliance with procurement rules, insufficient documentation, conflicts of interest, lack of objectivity, incomplete due diligence, unrealistic expectations, and inadequate subject knowledge, all of which can lead to questionable contract awards, reduced competition, and legal challenges, ultimately undermining the integrity and efficiency of the procurement process.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q6: Does the organization have a policy that sets out how any exceptions to the stated procurement procedures are to be implemented and managed, along with appropriate approval requirements?	The Organization has defined procurement cases where exceptions would apply and provides detailed explanation of instances for waiver and approval processes.	• Procurement Manuals. • Guidelines / SOPs. • Procurement approval templates.	**Low risk scenario:** The Partner defines specific conditions and criteria under which waivers can be considered, such as emergencies, government monopoly, or other compelling reasons. These instances are clearly outlined within the regulations, with stringent justification and documentation requirements to prevent misuse. Attention is given to transparency in the waiver process, involving multiple stakeholders for review and approval to ensure accountability and prevent favoritism or abuse. Additionally, there are mechanisms for reporting and post-waiver evaluation to assess the impact and uphold accountability and integrity within the procurement framework.

High risk scenario: The Partner has vague, open-ended language in the regulations, allowing for broad discretionary powers without clear guidelines or accountability. There is frequent, undocumented use of waivers without valid justification or proper review, resulting in a lack of transparency and increased potential for favoritism, corruption, or misuse of these exceptions, undermining the integrity of the procurement process and public trust.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q7: Does the organization have adequate policies to ensure staff consider and document whether they have any conflicts of interest with potential suppliers?	The Organization has adequate policies for addressing conflicts of interest and instances containing potential risks of fraud, corruption, and favoritism.	• Procurement Manuals. • Guidelines / SOPs. • Tender Evaluation Reports. • Code of Conduct for personnel.	**Low-risk scenario (also described in ICA/ICQ Template): Procurement is conducted ethically, with total impartiality and without any preferential treatment.** The Partner has a zero-tolerance policy on fraud and corruption. The Partner does not condone corrupt and fraudulent practices or any other form of misconduct including conflict of interest. The partner complies with this approach and ensures it has systems in place which prevent and detect fraud, report unethical behavior, and corrupt practices to foster a culture of integrity and accountability. The Partner commits to maintaining the highest possible standards and to immediately identify, address, mitigate, and report all instances in which these are compromised. Partner demonstrates Code of Conduct for employees addressing ethical principles mentioned above. **High risk scenario:** The Partner's procurement process lacks ethical integrity, exhibiting partiality,

			preferential treatment, and a high tolerance for fraud, corruption, and other misconduct, including conflicts of interest. The Partner does not have robust systems to prevent or detect fraud and unethical behavior, and there is no clear commitment to maintaining high ethical standards. There is a culture that tolerates compromised integrity, and instances of ethical violations go unaddressed and unreported, potentially resulting in a lack of accountability and damaged reputation. The absence of a Code of Conduct for employees addressing ethical principles further contributes to this bad practice.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q8: If a conflict is identified, is it evident that the staff member concerned is required to recuse themselves from any procurement process in which that entity is involved?	The Organization has clearly established rules on how and when the staff should recuse from procurement process. Those rules are regularly followed.	• Procurement Manuals. • Guidelines / SOPs. • Recusal reports. • Tender Evaluation Reports. • Code of Conduct for personnel.	**Low risk scenario:** The Partner demonstrates continuous use of appropriate methods to address conflicts of interest and implements the recusal mechanisms. The Partner displays instances of recusal in various stages of the procurement process. **High risk scenario:** The Partner consistently fails to effectively manage conflicts of interest and overlooks the implementation of recusal mechanisms. They do not showcase any instances where conflicts were appropriately handled at different stages of the procurement process.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q9: Are background checks performed on suppliers to ensure there are no publicly known cases of fraud or other malpractice?	The Organization uses available mechanisms to check the suppliers' background, portfolio, and credentials to avoid contracting ineligible vendors.	• Procurement Manuals. • Available local and international platforms. • Databases of suppliers, contracts where suppliers are also reflected or implemented projects etc. • Reference mechanisms for checking the background of suppliers. • Industry publications.	**Low risk scenario:** The Partner established a comprehensive due diligence process that examines suppliers' financial history, legal records, and past performance. The Partner utilizes reputable sources and databases to cross-reference information and consider seeking references or conducting interviews with previous clients. Additionally, the Partner monitors news and industry publications for any reported irregularities or legal issues involving the suppliers and collaborates with relevant regulatory agencies and industry associations to gather information and stay informed about any potential red flags. **High risk scenario:** The Partner shows a lack of due diligence and oversight, resulting in an inadequate or superficial examination of supplier backgrounds. This might include solely relying on informal sources or neglecting to update and revisit checks periodically, leading to outdated or incomplete information. There is a lack of transparency in the process or failing to document the findings, making it challenging to justify supplier selections or identify potential risks. Additionally, the Partner disregards legal and regulatory requirements, or makes decisions based on personal biases rather than objective criteria.

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q10: Does the organization have policies in relation to contract management?	The Organization employs specific mechanisms for contract management, which are reflected in the rules and regulations.	• Procurement Manuals. • Guidelines / SOPs. • Contracts. • Vendor Performance Reviews. • Vendor payment documents.	**Low risk scenario (also described in ICA/ICQ Template):** The Partner covers areas such as monitoring contract expiration, performance securities, and contract risk management procedures. The monitoring entails monitoring of performance against contract requirements over time, which consists of measuring, analyzing, and managing vendors' ability to comply with their contractual obligations. This is part of contract management for which the Partner concerned is expected to have a proper system, methodology and procedure in place. **High risk scenario:** The Partner neglects to monitor contract expiration, performance securities or contract risk management procedures. The Partner demonstrates a lack of attention to contract management, failing to track performance against contract requirements, and not implementing any structured systems or methodologies to ensure that vendors fulfil their contractual obligations. Important deadlines are continuously missed.
Question	**Good Practices (low risk)**	**Source of evidence for good practices**	**Hypothetical scenario with the recommended risk level**
Q11: Does the organization require its suppliers to uphold high ethical standards at all times?	Ethical standards are communicated to all suppliers and the Organization monitors vendors' behavior and performance.	• Procurement Manuals. • Guidelines / SOPs. • Examples of Vendor Performance Reviews. • Code of Conduct for suppliers.	**Low risk scenario:** The Partner established a comprehensive set of ethical guidelines and codes of conduct, explicitly outlining expectations regarding issues such as fair labour practices, environmental responsibility, anti-corruption measures, and quality standards. These guidelines are integrated into contractual agreements, with clear clauses specifying the commitment to ethical standards and potential consequences for non-compliance. Regular supplier audits, assessments, and due diligence are conducted

			to monitor and verify adherence to these standards. Additionally, fostering open communication channels, providing ethical training, and promoting a culture of transparency and accountability is exercised to incentivize suppliers to maintain high ethical standards throughout their engagement with the Partner.
			High risk scenario:
			Lack of clear ethical guidelines and codes of conduct, leaving room for ethical misconduct. Infrequent or superficial audits and assessments of supplier behavior, resulting in limited oversight and potential ethical violations going unchecked. The Partner neglects to enforce consequences for non-compliance and fails to promote ethical awareness and accountability within the organization and its supply chain which might lead to ethical lapses, reputational damage, and potential legal and financial repercussions.

G. Sub- Partners

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q1: Are sub-partners selected based on standard procedures, such as pre-award assessments, to ensure they are appropriately registered, suitably qualified to perform the role to be assigned, have adequate internal control systems, and that there are not significant ethical or reputational concerns?	There is an adequate due process performed prior to engaging a sub partner. The due process involves all stages and or activities as indicated in the Question and description column.	Guidelines / SOPs	**Explanation** should be provided into column L row 113 of ICA/ICQ - the partner has not engaged sub-partners. In such a scenario the suggested rating is **– N/A with no further rating.**

H. Systems

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q6: *Accounting system* - Do appropriate procedures and controls exist to ensure that the same or similar level of oversight is maintained even if staff are not physically present in the office?	Control activities are the policies and procedures that help ensure management directives are carried out even if staff are not physically in the office.	• Copy of authorized personnel who have access to the IFMS and or other systems. • Secured internet connections. • Use of usernames and passwords • Use of Multi Factor authentication (MFA)	Access to IFMIS was through usernames and passwords. Access to IFMIS was granted only to authorized personnel. The system is accessible even if the authorized staff are not in the office and have secure internet connection. Once a transaction is initiated, the reviewer and the approver get an email notification to act on their part. In such scenario the suggested rating is **low**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q8: **Banking** - Does the organization perform bank reconciliations on at least a monthly basis?	• Bank reconciliations are prepared at least monthly, independently reviewed, approved, and documented, as an essential internal control tool necessary in preventing and detecting fraud. • They also help identify accounting and bank errors by providing explanations for the differences between the accounting record's cash balances and the bank balance position per the bank statement.	• General ledger account balance being reconciled. • Bank statement. • List of unpresented cheques • Signed bank reconciliation statement. • Deposits recorded in the general ledger account, which have not yet been received and recorded by the bank.	Bank reconciliations are prepared by an Assistant Accountant, reviewed, and approved by the Senior Accountant. However, the bank statements were not prepared on time. In such scenario the suggested rating is **Significant**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q11: **Payments** - Are payments subject to a clear approval process with adequate segregation of duties?	• There is a clear segregation of duties between approval, custodianship, and reporting of payments transactions. • Online payments are subject to adequate IT controls.	• Payment vouchers • Invoices and Purchase Orders • Source documents contain pertinent information about the transaction, such as the date, the amounts, the involved parties, and the purpose of the transaction. • Receipts that represent proof of a financial transaction or purchase.	There is an authorization matrix defining approval thresholds. The partner's payments were authorized by the Directors as indicated in the authorization matrix. In such scenario the suggested rating is **Low**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q15: *Payments* - Is there a stated and reasonable limit for the amount that can be paid in cash?	• Generally, the cash assets must be kept in a bank account and their monetary transactions must be carried out in a bank account. • Laws seeking to limit and minimize the use of cash between different jurisdictions must be observed. • When unavoidable to use cash payments, proper approval should be sought and documented.	• Payment vouchers • Receipts that represent proof of a financial transaction or purchase. • Cash payments limit procedures and reporting.	No cash payments were made by the partner. In such a scenario the suggested rating is **– N/A with no further rating.**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q19: *Payments* Are supporting documents stamped as "Paid" and marked with the donor or project name after payment has been made, or does the accounting system otherwise have inbuilt controls to ensure payments cannot be made more than once or claimed against more than one funding source?	• Invoices are stamped as 'paid' when they have been paid to avoid duplicate payments. • The stamped documents are dated, reviewed, and approved. • Procedures are in place to make sure that payments cannot be claimed against more than one funding source.	• Stamped invoices, • Stamped other source documents. • Stamp showing charges against different funding sources with clear %. • Exchange of information/documents with other donors e.g., UN agencies (if possible) • Special audit reports.	Inspection of the paid payment vouchers showed that upon payment, these and their supporting documents were stamped 'PAID,' dated, reviewed, and approved. In such scenario the suggested rating is **Low**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level

Q22: **_Document management/record keeping_** Does the organization maintain all its records in an orderly and consistent way, that enables the ready identification of relevant documentation?	• Records management allows organizations to:
	  o establish strategies, policies, and procedures for making and keeping records,
	  o allocate resources to manage records effectively,
	  o ensure records are accurate and reliable regardless of form or medium,
	  o create and manage records consistently,
	  o distinguish between valuable and obsolete records and evidence,
	  o store records safely and dispose of records appropriately.
		• Policy on record management both manual and online.
		• Retention and disposal procedures
		• Destroy and deleting procedures.
			The accounting and personnel records were maintained in hard-copy files. These were kept in a segregated office with restricted access.
			
			There is no written policy on records management, however through discussion with management they narrated the procedures being followed in records management which seemingly adequate but needs few improvements.
			
			In such scenario the suggested rating is **Medium/Moderate**

DIST – ICT related questions:

B. People and behaviours
Recruitment and retention

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q6: Are procedures in place to ensure that, when staff leave employment with the organization, they are removed from the payroll after receipt of the final salary due, are required to return any equipment belonging to the organization, and have any access rights to in-house systems terminated?	There are procedures that covers various actions to be taken in connection with the separation from employment including but not limited to removal from payroll, return of any equipment belonging to the organization and removal of access rights to each individual system of importance.	• Separation Brochure (s) • Separation Checklist (s) • List of contact person /units regarding the separation process • Separation policies and procedures including evidence of request to remove partner-owned data from any personal devices. • Extract of people who have rights on their systems still. • List of equipment owned/held in trust and who has them.	The organization has adequate procedures in place to ensure that proper hand-over is done during the separation from employment. Review of the sample of staff that were separated during the year revealed that policies and procedures were properly followed and documented accordingly. Reports from their main systems do not show "strangers" (ex-employees) with rights still. No equipment "lost" when staff left. In such scenario the suggested rating is **Low**

H. Systems

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q1: Does the organization have and make use of a computerized accounting	Unless sanctions make this impossible, the partner should use licensed versions (or open-source	Confirm that the partner has as commercial/standard accounting system.	Partner has a standard accounting package, and it is being updated.

system that records sufficient details of each transaction to allow it to be linked to the corresponding documentation and allocated to the relevant funding source?	software) for its main applications and have auto-update enabled for them.	For their main applications (accounting, payroll, inventory, email, file storage, collaboration) ask for records of their purchases of software assets or licenses. Ask for screenshots of "last updated" dates.	No sanctions applicable, but they are using "freeware" and unlicensed software for other tools and "cracked" software which may contain viruses and does not get any patches or updates. In such scenario the suggested rating is **Significant**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q2: Is access to the accounting system protected through the use of usernames and passwords?	• UNHCR expects that access to key systems (including accounting systems) are protected by named user ids with complex and regularly changed passwords. • For systems processing personal data, the entity should use multi-factor authentication (MFA) whenever technically possible, including any common case management tools and document drives.	• List of key systems (normally accounting, payroll, inventory, email, file storage collaboration). • List of users in each key system • Check no "user 1" or "admin" accounts performing transactions. • Request copy of password policy • Obtain last changed report from key system for each account password. • Technical document on how MFA implemented. • Report on which account has MFA and which it does not have.	Key systems identified and agreed. Most accounts there are for users but there are a couple of "user 123" account which are not clearly owned by anyone. Passwords are complex and most, but not all changed with the last 90 days. However, the organisation does not use MFA at all. In such scenario the suggesting is **Significant** with MFA it would be **Medium/Moderate**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q3: Do different users have different access rights so that they are only able to review or make changes to information that is relevant to their function?	The partner does not allow the sharing of user accounts. All operational activity can be traced to a specific person. No personal data sharing takes place using generic accounts.	• For each key system, a list of users and their access rights is available in some way. • On a sample basis, check that access rights match current roles. • Check for any shared or anonymous accounts being used for transactions. • Check email sent records for any shared accounts and check no excel attachments with personal data.	In key systems, staff all use the same account for their work. No one knows who did what. All personal data is sent and received from the same shared account and all transactions are posted by "user 123" or 'admin'. In such a scenario the suggested rating is **High**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q4: Is the accounting system backed up to a secure offsite location on a sufficiently regular basis?	This may include checking for other technical aspects of information security and preventing IT attacks and unwanted access not limited to accounting system only. In addition, the entity should have an IT focal point competent and qualified to address IT, information security and data protection risks.	• Is there a named person responsible for IT – can you meet and speak to them? • Ask for a register of backups for the last 90 days (about 3 months). • Ask where the backups are kept and how that transfer takes place. • Ask if they allow home and remote access? • Ask when they last had an infosec or data protection problem. • Ask how they would know if they had a problem?	The IT manager is available and well informed. He has a register of backups and confirmed they are sent manually to a nearby sub-office (or even the home of the IT manager). They confirm they lost a laptop recently, but they know it did not contain personal data of refugees. They periodically review transactions and accesses on all main systems. Most of their systems (except email and file sharing) are not on the internet so physical access is required to be able to perform any duties. They have a VPN and use it. In such scenario the suggested outcome is **Low**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q6: Do appropriate procedures and controls exist to ensure that the same or similar level of oversight is maintained even if staff are not physically present in the office?	This includes ensuring that there are policies and procedures in place defining minimum standards of internal control system. Responsibilities related to internal control system have been assigned within the partner's personnel. Furthermore, ensuring that staff not in the office are using authorized platforms to transfer documents, rather than public/freeways, which may be subject to hacking	• How do staff working remotely get access to partner systems? • Is there strong authentication to cloud services (e.g., MFA) or do they use a VPN? • Does the partner have a preferred tool for file exchange, and do they have any form of license for it?	(IT side only) Partner uses mostly licensed cloud services (but without MFA). Partner uses the cloud provided file exchange tool. In such scenario the suggested risk is **Medium/Moderate**

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q7: Are all staff issued with computers that are maintained by and accessible to the organization's IT department, and that have adequate anti-malware installed	This may include checking: • If the entity has an official website and is regularly updated. • If the relevant entity staff have official email addresses issued for official correspondence (not using Gmail or other personal accounts). • If the entity has an up-to-date antivirus solution on its personal computers and schedules regular scans. • If there are mechanisms in place to ensure that all funded equipment is subject to review by the organization in relation to an	• Ask for a list of staff and Computers – are staff using personal devices for their main work or do they have IT-department devices.? • Check their website before you go to see if they have one and see if it has been updated in the last 6 months. • Ask what domain the org uses for its email (like "unhcr.org"). Do they have a proper domain or are they asking their staff to register to Gmail or similar. • For each PC, ask what antivirus tool it uses and when it was last	Organization has no proper IT team or domain. Staff are asked to use Gmail and their personal devices for work. No effort is made to have any antivirus tool for them. When you ask about the IT equipment which was loaded or gifted to them, they do not have it and cannot explain where it went. In such scenario the suggested risk is **High**

	audit/investigation, and/or by an authorized investigative body.	updated (should be a recent report) • Bring a list of any equipment UNHCR funded or loaned and ask where it is.	

Question	Good Practices (low risk)	Source of evidence for good practices	Hypothetical scenario with the recommended risk level
Q24: Does the organization have a data protection policy?	• When storing personal data, the entity should always use encryption including hard disk encryption (such as Bit locker) for its laptops (in case they are stolen). • When sharing information on forcibly displaced and stateless persons over the Internet, the partner should always use encrypted methods such as password-protected files or other commercial, custom or UNHCR-provided tools example WeTransfer, Dropbox, OneDrive, UNHCR's Secure File Sharing (SFS), Oracle Aconex."	• Ask if all PCs are encrypted with bit locker and Macs with Filevault or equivalent. Ask for a printout of evidence. • Ask what solution they use for their file storage - if in the cloud, ok, if in a local File server, how is refugee data stopped from being exported or stolen? • What standard or recommended tool do they use for file sharing? If not UNHCRs, how is it protected? Do they have a license or are they using a freeware version? • Ask whether they have a policy on not sharing refugee person data over the internet unencrypted? • On a sample basis, ask for a list of emails over 1Mb in the last week and verify that none contain personal data not encrypted (might be hard to do).	Company encrypts laptops and uses Microsoft cloud storage which default encrypts most things. They use Teams and SharePoint and OneDrive for file storage and collaboration, and they have bought a license. They promise they never email refugee data without WinZip and a password or equivalent. In such scenario the suggest rating is **Low**