



## Annex 1

### Terms of Reference

#### Implementation of the Information Security Management System in accordance with ISO/CEI 27001:2013 at the National Anticorruption Centre of Moldova

##### 1. BACKGROUND

Curbing Corruption through Building Sustainable Integrity in Moldova Project (further NAC II Project) will contribute to achieving a sustainable integrity and anticorruption system in the Republic of Moldova through the strengthened capacities of the public and private sector entities and the civil society for the efficient application and monitoring of national integrity instruments and standards. The project will enhance capacities of the public and private sector actors, as well as of the Civil Society Organisations (CSOs) for the implementation of effective corruption prevention instruments and tools and will strengthen the anticorruption demand side through an increased public awareness on anticorruption and on the means to curb corruption. It will contribute to the progressive implementation of the Sustainable Development Goal 16 that calls for a substantial reduction of corruption and bribery in all their forms and for developing effective, accountable and transparent institutions at all levels. The Project is framed around the National Integrity and Anticorruption Strategy (NIAS) 2017-2020 and responds to the needs of its various actors and stakeholders in addressing the challenges for the effective implementation of NIAS.

One of the Project's objectives is to strengthen the capacities of the anticorruption authority to enforce and improve integrity instruments. The National Anticorruption Centre (NAC) has a well-defined mandate for the fight and prevention of corruption and is the institution responsible for the coordination of the implementation of the National Integrity and Anticorruption Strategy 2017 - 2020. The Centre has the organizational, functional and operational independence granted by law and is independent in developing its work plan and in fulfilling its duties. (Details on the NAC organizational structure is attached to this ToR).

To enhance the capacities of the National Anticorruption Center for ensuring the uniform compliance with anticorruption and integrity standards across the country, the Project will support the implementation and certification of the Information Security Management System in accordance with ISO/CEI 27001:2013. In this context, the Project seeks a specialized company/consulting firm to carry out the implementation of the ISO/CEI 27001:2013 to further achieve the certification on this standard.

## 2. OBJECTIVES OF THE ASSIGNMENT

The objective of this service is to carry out the implementation of the Information Security Management System ISO/CEI 27001:2013 within the National Anticorruption Centre of Moldova with the main goal to achieve a modern and effective working environment certified under this standard.

This methodology is to be process-oriented, focused on the business objectives of the client and should incorporate all concepts of the security management system. It should also cover the need for continuous improvement with the objective of protecting the confidentiality, integrity and availability of critical information assets.

## 3. SCOPE OF WORK AND EXPECTED OUTPUTS:

In order to achieve the objectives set services **for the implementation of the Informational Security management system ISO 27001:2013** for the NAC of the Republic of Moldova, the selected company will provide targeted advisory services and will deliver the following:

1. Perform the Audit of the NAC informational Security Management System. The evaluation should be done in terms of effectiveness in relation to the specificity and individual needs of NAC as well as in terms of compliance to ISO / IEC 27001:2013. Formulate specific recommendations for improving the Information Security Management System.
2. Develop the Information Security Policy. Identify specific objectives of NAC regarding information security. Develop a mechanism of establishment of high-level directives and principles for information security management.
3. Develop Information Security Standards. Identify detailed safety standards and practices applicable to NAC, considering NAC activities and technologies within a Guide on information security addressed to NAC staff.
4. Train the NAC staff. Advise on establishment of target groups and develop specific training programs. Deliver training sessions to each target group. Three target groups are estimated in advance:
  - a. Advanced (6 users with a 24-hour training program);
  - b. Leaders (6 users with an 8-hour training program);
  - c. Users (22 users with a 4-hour training program).
5. Define and Organize the Basic Processes in the framework of the Information Security Management System. Develop a Regulation on information security management which will establish procedures for:
  - a. Management of the informational resources;
  - b. Control of the access to the informational system;
  - c. Management of changes in the informational system;
  - d. Management of incidents.
6. Analyse the Information Security Risks. Develop specific procedures for assessing and addressing possible informational security risks. After the implementation of these procedures on assessment of the security risks, draft a Report on assessment of an informational security risk that will be used by NAC as a model for future assessments.
7. Develop a Plan for the Continuity and Restoration of the NAC Informational System, to include:
  - An impact analysis for the informational subsystem of the NAC of the Republic of Moldova;
  - Establishment of continuity requirements for the information Subsystems based on individual NAC needs;

- Analysis of the risks of interruptions in information subsystems;
- A Policy of managing the backup copies (the inventory of information resources that fall within the policy coverage, the establishment of RPO (Recovery Point Objective) indicators, establishment of backup procedures applied to each resource, establishment of the general procedure for the management of backup copies, including off-site storage, testing, etc.).
- An analysis of risks that can lead to failures in information systems, the identification of necessary measures that need to be implemented in order to prevent and to prepare for incidents, the establishment of procedures that will be applied for each risk scenario separately.

General information about NAC can be found in the hereby attached Questionnaire (see attachment to Annex 1).

The implementing companies are expected to prepare commercial proposals with detailed work plans and timelines.

### Travel

All envisaged travel costs must be included in the Annex 2: Form for Submitting Supplier's Quotation under the point *Cost of Transportation*. The Costs of Transportation shall be disbursed depending on the effective travel and the duty travel restrictions due to Covid19 pandemics.

## 4. DELIVERABLES AND TIMEFRAME

No.	Deliverables	Specifications	Indicative Timeframe
1.	For the implementation of the Informational Security management system ISO 27001:2013	a. Audit Report on the Information Security Management System produced;	weeks 1-6 by October 9, 2020
		b. Informational Security Policy developed;	weeks 7-9 by October 30, 2020
		c. Information Security Standards developed;	weeks 10-12 by November 21, 2020
		d. Training programs for NAC staff delivered;	weeks 7-12 by November 20, 2020
		e. Regulation on information security management developed;	weeks 13-16 by December 15, 2020
		f. Set of documents for analysis of security risks developed;	weeks 18-22 by January 15, 2021
		g. Plan for the Continuity and Restoration of the NAC Informational System developed;	weeks 22-24 by February 15, 2021
		i. Final Report on the services delivered and future recommendations;	week 25 by February 28, 2021

A more concrete implementation schedule (divided into phases) should be produced and submitted for approval by the implementing contractor at the beginning of the assignment. Final report and other documents related to the assignment should be submitted to the Project Manager. Reports shall be written in Romanian.

## Timeframe

The entire assignment is to be finalized not later than **28 February 2021**.

## Deliverables Format

All deliverables will be submitted in both hardcopy one (1) unbound original and one (1) electronic copy using the standard software products (Microsoft Office Word, Excel, Access and PowerPoint). The Final Report will be presented in Romanian language and an Executive Summary in English language.

## 5. MANAGEMENT ARRANGEMENTS:

Organizational Setting: The contractor will work under the direct supervision of the NAC and UNDP Project. The contractor shall take overall responsibility on the quality and timeliness of the assessment process within its competency.

The NAC will provide the contractor with the necessary information and materials in order to ensure the successful completion of the assignment.

Duration of the Work: **September 2020 – February 2021**. The payment will be done after submission of deliverables, as to be agreed at contract signature stage.

## Confidentiality statement

All data and information received from UNDP and NAC staff for the purpose of this assignment is to be treated confidentially and are only to be used in connection with the execution of these Terms of Reference. All intellectual property rights arising from the execution of these Terms of Reference are assigned to UNDP. The contents of written materials obtained and used in this assignment may not be disclosed to any third parties without the expressed advance written authorization of the UNDP Programme.

## 6. QUALIFICATIONS OF THE SUCCESSFUL SERVICE PROVIDER AT VARIOUS LEVELS

Bidders should enclose a résumé for each person anticipated to be assigned to the project and should include specific information on staff experience and roles. Bidders agree that named staff will participate in the project at the level and duration specified unless agreement is provided in writing by the Programme to allow substitutions.

Résumés of key project personnel must be included in the offer, résumés for other personnel may be included as deemed applicable by the Bidder. Descriptions of subcontractor staff members, if applicable, should follow the format utilized for the Bidder organization. The résumés submitted for project personnel should be detailed and comprehensive. Specifically, résumés should include:

- Anticipated role and level of participation in the project;
- Previous experience relevant to the assigned role in the project;
- Education, training and certification details;

- Linguistic skills.

Bidders should describe, in detail, their previous corporate experience in similar related to the project's assignment, if any. This section should include the corporate experience as well as the role of any subcontract organization(s) indicated in the Bidder's proposal. Descriptions of subcontractor staff members, if applicable, should follow the format utilized for the Bidder organization. The Project retains the right to accept or reject all proposed project personnel and to ask for replacement of the Project staff, as necessary.

**The Service Provider should meet the following minimum qualifications criteria** which make the applicant eligible for this assignment:

- Be legally registered entity or a consortium of firms/organizations;
- Possess documents or diplomas issued by established certified organizations that would confirm certification for Security Management Systems ISO/IEC 27001;
- At least four (4) years of experience in designing and providing consultancy services related/similar to the implementation of the ISO standards in the Republic of Moldova or in the region of Central and Eastern Europe;
- At least one (1) team member with experience/assignments in designing and providing services for the implementation of the ISO standards for public institutions in the Republic of Moldova;
- At least three (3) assignments in designing and providing services for the implementation of the ISO standards. Letters of reference should be provided by the applicant for minimum three (3) projects related to the implementation of the ISO standards developed and implemented;
- If the applicant is a foreign entity, it should have local legal subsidiary or have at least one (1) core auditor that is a Moldovan resident;
- Key members of the consulting firms/consortium of firms must have qualified and experienced personnel including certified Lead Auditors for the above-mentioned management standards.

#### **Qualification of the Team members:**

The Bidder shall describe the proposed key personnel taking into consideration following positions:

- Team Leader;
- Key Experts.

#### **Minimum requirements for the Project Team:**

- Team Leader or one of the Key Experts to be fully competent in the field of the Security Management Systems ISO/IEC 27001, proven via recognized certifications.

#### **Minimum requirements for the Team Leader position:**

- University Degree in Accounting, Finance, Economics, Banking, Law or other relevant fields;
- minimum five (5) years of experience in the provision of consultancy services related/similar to the implementation of the ISO standards;
- working knowledge of English and Romanian languages.

#### **Minimum requirements for the Key Experts:**

- University Degree in Accounting, Finance, Economics, Banking, Law or other relevant fields;
- minimum three (3) years of experience in the provision of consultancy services related/similar to the implementation of the ISO standards;
- working knowledge of Romanian language.

**Each bidder should develop and submit a technical offer containing:**

- **Their internal quality assurance standards, recommendations, previous works:**
  - constituent and legal documents available;
  - list of services provided over the past four (4) years in the field of providing consultancy services related/similar to the implementation of the ISO standards;
  - recommendations from enterprises, organizations and other clients available (at least three (3));
  - list of Key Personnel, including CVs and accreditation certificates.

**Note:** Proposed timeline should include all indicative dates for deliverables as outlined above and a plan for meeting these and any additional deadlines.

Proven commitment to the core values of the United Nations, in particular, respecting differences of culture, gender, religion, ethnicity, nationality, language, age, HIV status, disability, and sexual orientation, or other status.

UNDP Moldova is committed to workforce diversity. Women, persons with disabilities, Roma and other ethnic or religious minorities, persons living with HIV, as well as refugees and other non-citizens legally entitled to work in the Republic of Moldova, are particularly encouraged to apply.

**Attachment to Annex 1:** Questionnaire about the National Anticorruption Center of the Republic of Moldova

## Questionnaire about the National Anticorruption Center of the Republic of Moldova

Numele instituției:	Centrul Național Anticorupție din Republica Moldova
Adresa sediului social:	MD-2004, mun. Chișinău, bd. Ștefan cel Mare și Sfint 198
IDNO:	1006601000222
Statutul juridic al organizației:	autoritate publică LP1104/2002 <a href="https://www.legis.md/cautare/getResults?doc_id=66260&amp;lang=ro">https://www.legis.md/cautare/getResults?doc_id=66260&amp;lang=ro</a>
Structura aparatului central al CNA	HP34/2016 <a href="https://www.legis.md/cautare/getResults?doc_id=119758&amp;lang=ro#">https://www.legis.md/cautare/getResults?doc_id=119758&amp;lang=ro#</a>
Tel:	/+373 22/ 257-257
Fax:	/+373 22/ 257-294, 244-766
E-mail:	<a href="mailto:secretariat@cna.md">secretariat@cna.md</a>
Subdiviziuni teritoriale:	Direcția teritorială „Centru”, cu sediul în municipiul Chișinău; Direcția generală teritorială "Nord" cu sediul în municipiul Bălți și Direcția generală teritorială "Sud" cu sediul în orașul Cahul
Numele, numărul de telefon și emailul persoanei de contact:	Valeriu Cupcea, șef al Direcției cooperare internațională Tel: +373 79743505, e-mail: <a href="mailto:valeriu.cupcea@cna.md">valeriu.cupcea@cna.md</a>
Numărul total de angajați:	efectiv-limită în număr de 359 unități (Hotărârea Parlamentului nr.34/2016)
Numărul de angajați implicați în procesele sensibile	Activitatea oricărei subdiviziuni a CNA este susceptibilă anumitor riscuri. Respectiv numărul coincide cu efectivul limită: 359
Numărul de angajați în funcții manageriale	60
Program de lucru:	Luni-Vineri, 08:00 – 17:00, Prînz 12:00-13:00
Exista un alt Sistem de Management implementat:	Nu
Limba de comunicare:	Româna
Tipul de informații furnizate	Date cu caracter personal, informații de interes public (rapoarte de expertiză anticorupție a proiectelor actelor normative, rapoarte aferente activității de evaluare a integrității instituționale, studii analitice, informația transmisă în cadrul campaniilor de sensibilizare și educație anticorupție); informații cu acces restricționat/atribuite la secretul de stat
Documentație confidențială:	<b>DA</b> ISMS include (proceduri, înregistrări etc.) clasificată ca fiind "confidențială" și/sau care nu poate fi pusă la dispoziție pentru verificare?: <b>informație cu acces restricționat</b> – informația aferentă activității de urmărire penală, activității speciale de investigații, activității de testare a integrității profesionale, a activității Agenției de Recuperare a Bunurilor Infractionale, altă informație a cărei divulgare poate prejudicia realizarea atribuțiilor CNA