United Nations Development Programme

REQUEST FOR PROPOSAL (RFP)

Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs

RFP Reference No.: **RfP26/03336**

Country: Republic of Moldova

Issued on: 26 August 2026

Contents

SECTION 1: LETTER OF INVITATION

United Nations Development Programme, hereinafter referred to as UNDP, through *"Enhancing Crisis Management and Cybersecurity Resilience of the Ministry of Foreign Affairs of the Republic of Moldova* ", hereby invites prospective proposers to submit a proposal for **Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**, in accordance with the General Conditions of Contract and the Terms of Reference as set out in this Request for Proposal (RFP).

To enable you to submit a proposal, please read the following attached documents carefully:

Section 1: This Letter of Invitation
Section 2: Instruction to Proposers
Section 3: Data Sheet
Section 4: Evaluation Criteria
Section 5: Terms of Reference
Section 6: Conditions of Contract and Contract Forms
Section 7: Proposal Forms
- *Form A*: Proposal confirmation
- *Form B*: Checklist
- *Form C*: Technical Proposal Submission
- *Form D*: Proposer Information
- *Form E*: Joint Venture/Consortium/Association Information
- *Form F*: Eligibility and Qualification
- *Form G*: Format for Technical Proposal
- *Form H*: Format for CV of Proposed Key Personnel
- *Form I*: Statement of Exclusivity and Availability
- *Form J*: Financial Proposal Submission
- *Form K*: Format for Financial Proposal

If you are interested in submitting a proposal in response to this RFP, please prepare your proposal in accordance with the requirements and procedure as set out in this RFP and submit it by the deadline for submission of proposals set out in Section 3: Data Sheet.

Should you be interested to submit a proposal, please log in to the Quantum NextGenERP supplier portal and subscribe to this tender following the instructions in the system user guide. Please search for the tender using search filters, namely **Negotiation ID: UNDP-MDA-01077**. Once subscribed to the tender, you will be able to receive notifications in case of amendments of the tender document and requirements.

Please indicate whether you intend to submit a bid by creating a draft response without submitting directly in the Quantum NextGenERP supplier portal.

Offers must be submitted directly in the Quantum NextGenERP supplier portal following this link: http://supplier.quantum.partneragencies.org/ using the profile you may have in the portal (please log in using your username and password). In case you have never registered before, follow the Supplier Portal Registration Link.

Please note that the access link to the Supplier registered profile is sent from Oracle within up to 3 days. In case you have not received the access link after 3 days since registration, you should address for support to UNDP at the email address: sc.md@undp.org. In case you encounter errors with registration (e.g. system states Supplier already is registered), you should address for support to UNDP at the email address: sc.md@undp.org.

Computer firewall could block *oracle* or *undp.org extension* and Suppliers might not receive the Oracle notifications. Please turn down any firewalls on your computers to ensure receipt of email notification.

Do not create a new profile if you already have one. Use the forgotten password feature in case you do not remember the password or the username from previous registration.

Should you require further clarifications on the application through the Quantum online portal, kindly contact the Procurement Unit at sc.md@undp.org. Please pay attention that the proposal shall be submitted online through the Quantum system and any proposal sent to the above email shall be disqualified.

Should you require further clarifications on the Request for Proposal, Terms of Reference or other requirements, kindly communicate using the messaging functionality in the portal.

Deadline for Submission of Offers (Date and Time), which is visible in the online procurement system will be final. System will not accept submission of any proposal after that date and time. It is the responsibility of the bidder to make sure that the proposal is submitted prior to this deadline for submission.

Bidders are advised to upload proposal documents and to submit their offer a day prior or well before the date and time indicated under the deadline for submission of Offers. Do not wait until last minute. If Bidder faces any issue during submitting offers at the last minutes prior to the deadline for submission, UNDP may not be able to assist on such a short notice and will not be held liable in such instance. UNDP will not accept any offer that is not submitted directly through the System.

We look forward to receiving your proposal.

UNDP Moldova

SECTION 2: INSTRUCTIONS TO PROPOSERS

GENERAL	
1. Scope	Proposers are invited to submit a proposal for the services specified in Section 5: Terms of Reference, in accordance with this Request for Proposal (RFP). A summary of the scope of the proposal is included in Section 3: Data Sheet. Proposers shall adhere to all the requirements of this RFP, including any amendment made in writing by UNDP. This RFP is conducted in accordance with Policies and Procedures of UNDP which can be accessed at UNDP Programme and OperationsPolicies and Procedures/Procurement. As part of the bid, it is desired that the Bidder registers at the United Nations Global Marketplace (UNGM) website (www.ungm.org). The Bidder may still submit a bid evenif not registered with the UNGM. However, if the Bidder is selected for contract award, the Bidder must register on the UNGM prior to contract signature.
2. Interpretation of the RFP	Any proposal submitted will be regarded as an offer by the proposer and does notconstitute or imply the acceptance of the proposal by UNDP. UNDP is under no obligation to award a contract to any proposer as a result of this RFP.
3. Supplier Code of Conduct, Fraud, Corruption, Gifts and Hospitality	All proposers must read the United Nations Supplier Code of Conduct and acknowledgethat it provides the minimum standards expected of suppliers to the UN. The Code of Conduct, which includes **principles on labor, human rights, environment and ethical conduct** may be found at: https://www.un.org/Depts/ptd/about-us/un-supplier-code- conduct Moreover, suppliers should note that certain provisions of the Code of Conduct will be binding on the supplier in the event that the supplier is awarded a contract, pursuant to the terms and conditions of any such contract. UNDP strictly enforces a policy of zero tolerance on proscribed practices, including fraud, corruption, collusion, unethical or unprofessional practices, and obstruction of UNDP vendors and requires all bidders/vendors observe the highest standard of ethics during the procurement process and contract implementation. UNDP's Anti-Fraud Policy can be found at: http://www.undp.org/content/undp/en/home/operations/accountability/audit/office_of_audit_andinvestigation.html#anti Bidders/vendors shall not offer gifts or hospitality of any kind to UNDP staff members including recreational trips to sporting or cultural events, theme parks or offers of holidays, transportation, or invitations to extravagant lunches or dinners. In pursuance of this policy, UNDP: a) Shall reject a proposal if it determines that the selected proposer has engaged in any corrupt or fraudulent practices in competing for the contract in question; b) Further to the UNDP's vendor sanctions policy, shall declare a vendor ineligible, either indefinitely or for a stated period, to be awarded a contract if at any time it determines that the vendor has engaged in any corrupt or fraudulent practices in competing for, or in executing a UNDP contract.
4. Eligible proposers	Proposers shall have the legal capacity to enter into a binding contract with UNDP. A proposer, and all parties constituting the proposer, may have the nationality of any country with the exception of the nationalities, if any, listed in Section 3: Data Sheet. A proposer shall be deemed to have the nationality of a country if the proposer is a citizenor is constituted, incorporated, or registered and operates in conformity with the provisions of the laws of that country. All proposers found to have a conflict of interest shall be disqualified. Proposers may beconsidered to have a conflict of interest if they are or have been associated in the past, with a firm or any of its affiliates that have been engaged by UNDP to provide consulting services for the preparation of the design, specifications, Terms of Reference, cost analysis/estimation and other documents to be used for the procurement of the services required in the present procurement process; were involved in the preparation and/or design of the programme/project related to the services requested under this RFP; or are found to be in conflict for any other reason, as may be established by, or at the discretion of UNDP and/or are found to be in conflict for any other reason, as may be established by, or at the discretion of UNDP. In the event of any uncertainty in the interpretation of a potential conflict of interest, Bidders must disclose to UNDP, and seek UNDP's confirmation on whether or not such a conflict exists. Similarly, the Bidders must disclose in their proposal their knowledge of the following: a) If the owners, part-owners, officers, directors, controlling shareholders, of thebidding entity or key personnel are family members of UNDP staff involved inthe procurement functions and/or

	the Government of the country or any Implementing Partner receiving services under this RFP; and b) All other circumstances that could potentially lead to actual or perceived conflict of interest, collusion or unfair competition practices. Failure to disclose such an information may result in the rejection of the proposal or proposals affected by the non-disclosure. The eligibility of Bidders that are wholly or partly owned by the Government shall be subject to UNDP's further evaluation and review of various factors such as being registered, operated and managed as an independent business entity, the extent of Government ownership/share, receipt of subsidies, mandate and access to informationin relation to this RFP, among others. Conditions that may lead to undue advantage against other Bidders may result in the eventual rejection of the Proposal. Proposers shall not be eligible to submit a proposal if at the time of proposalsubmission: • is included in the Ineligibility List, hosted by UNGM, that aggregates informationdisclosed by Agencies, Funds or Programs of the UN System; • is included in the Consolidated United Nations Security Council Sanctions List,including the UN Security Council Resolution 1267/1989 list; • is included in the World Bank Corporate Procurement Listing of Non-ResponsibleVendors and World Bank Listing of Ineligible Firms and Individuals.
5. Proprietary information	The RFP documents and any Terms of Reference or information issued or furnished by UNDP are issued solely for the purpose of enabling a proposal to be completed and may not be used for any other purpose. The RFP documents and any additional information provided to proposers shall remain the property of UNDP. All documents which may form part of the proposal will become the property of UNDP, who will not be required to return them to your firm.
6. Publicity	During the RFP process, a proposer is not permitted to create any publicity in connection with the RFP.
SOLICITATION DOCUMENTS	
7. Clarification of solicitation documents	Proposers may request clarifications on any of the RFP documents no later than the date indicated in Section 3: Data Sheet. Any request for clarification must be sent in writing in the manner indicated in Section 3: Data Sheet. Explanations or interpretations provided by personnel other than the named contact person will not be considered binding or official. UNDP will provide the responses to clarifications through the method specified in Section 3: Data Sheet. UNDP shall endeavor to provide responses to clarifications in an expeditious manner, but any delay in such response shall not cause an obligation on the part of UNDP to extend the submission date of the proposals, unless UNDP deems that such an extension is justified and necessary.
8. Amendment of solicitation documents	At any time prior to the deadline for proposal submission, UNDP may for any reason, such as in response to a clarification requested by a proposer, modify the RFP in the form of an amendment to the RFP. Amendments will be made available to all prospective proposers. If the amendment is substantial, UNDP may extend the deadline for submission of proposals to give the proposers reasonable time to incorporate the amendment into their proposal.
PREPARATION OF PROPOSALS	
9. Cost of preparation of proposal	The proposer shall bear all costs related to the preparation and/or submission of the proposal, regardless of whether its proposal is selected or not. UNDP shall not be responsible or liable for those costs, regardless of the conduct or outcome of the procurement process.
10. Language	The proposal, as well as any and all related correspondence exchanged by the proposer and UNDP, shall be written in the language(s) specified in Section 3: Data Sheet.
11. Documents establishing eligibility and qualifications ofthe proposer	The proposer shall furnish documentary evidence of its status as an eligible and qualified vendor, using the forms provided in Section 7 and providing the documents required in those forms. In order to award a contract to a proposer, its qualifications must be documented to UNDP's satisfaction.
11.a Documents comprising the proposal	The proposal bid shall comprise of the following documents and related forms whichdetails are provided in Section 3: Data Sheet: ▪ Documents Establishing the Eligibility and Qualifications of the Bidder; ▪ Technical Proposal; ▪ Financial Proposal;

	▪ Proposal Security, if required by DS; ▪ Any attachments and/or appendices to the Proposal.
12. Technical proposal format and content	The proposer is required to submit a technical proposal using the forms provided in Section 7 and taking into consideration the requirements in the RFP. The technical proposal shall not include any price or financial information. A technical proposal containing material financial information may be declared non-responsive.
13. Financial proposal	The financial proposal shall be prepared using the form provided in Section 7 and taking into consideration the requirements in the RFP. It shall list all major cost components associated with the services, and the detailed breakdown of such costs. Any output and activities described in the technical proposal but not priced in the financial proposal, shall be assumed to be included in the prices of other activities or items as well as in the final total price. Prices and other financial information must not be disclosed in any other place except in the financial proposal.
14. Currencies	All prices shall be quoted in the currency or currencies indicated in Section 3: Data Sheet. Where proposals are quoted in different currencies, for the purposes of comparison of all proposals: • UNDP will convert the currency quoted in the proposal into the UNDP preferredcurrency, in accordance with the UN Operational Rate of Exchange. • In the event that UNDP selects a proposal for award that is quoted in a currency different from the preferred currency in Section 3: Data Sheet, UNDP shall reservethe right to award the contract in the currency of UNDP's preference, using the conversion method specified above.
15. Duties and taxes	Article II, Section 7, of the Convention on the Privileges and Immunities provides, inter alia, that the United Nations, including UNDP as a subsidiary organ, is exempt from all direct taxes, except charges for public utility services, and is exempt from customs restrictions, duties, and charges of a similar nature in respect of articles imported or exported for its official use. All proposals shall be submitted net of any direct taxes andany other taxes and duties, unless otherwise specified in Section 3: Data Sheet.
16. Proposal validity period	Proposals shall remain valid for the period specified in Section 3: Data Sheet, commencing on the deadline for submission of proposals. A proposal valid for a shorterperiod may be rejected by UNDP and rendered non-responsive. During the proposal validity period, the proposer shall maintain its original proposal without any change, including the availability of the key personnel, the proposed ratesand the total price. In exceptional circumstances, prior to the expiration of the proposal validity period, UNDP may request proposers to extend the period of validity of their proposals. The request and the responses shall be made in writing and shall be considered integral tothe proposal. If the proposer agrees to extend the validity of its proposal, it shall be done without anychange to the original proposal but will be required to extend the validity of the proposal security, if required, for the period of the extension, and in compliance with Article 17 (Proposal security) in all respects. The proposer has the right to refuse to extend the validity of its proposal without forfeiting the proposal security, if required, in which case, the proposal shall not befurther evaluated.
17. Proposal security	A proposal security, if required by Section 3: Data Sheet, shall be provided in the amount and form indicated in the Section 3: Data Sheet. The proposal security shall be valid for a minimum of thirty (30) days after the final date of validity of the proposal. The proposal security shall be included along with the proposal. If a proposal security is required by the RFP but is not found in the proposal, the offer shall be rejected. If the proposal security amount, or its validity period, is found to be less than is required by UNDP, UNDP shall reject the proposal. In the event an electronic submission is allowed in Section 3: Data Sheet, proposers shall include a copy of the proposal security in their proposal and the original of the proposal security must be sent via courier or hand delivery as per the instructions in Section 3: Data Sheet. Unsuccessful proposers' proposal securities will be discharged/returned as promptly as possible but no later than thirty (30) days after the expiration of the period of proposal validity prescribed by UNDP pursuant to Article 16 (Proposal Validity Period). The Proposal security may be forfeited by UNDP, and the proposal rejected, in the event of any, or combination, of the following conditions: • If the proposer withdraws its offer during the period of the proposal validityspecified in Section 3: Data Sheet, or;

	• In the event the successful Proposer fails: o to sign the contract after UNDP has issued an award; or o to furnish the performance security, insurances, or other documentsthat UNDP may require as a condition precedent to the effectivity of the contract that may be awarded to the proposer.
18. Joint Venture, Consortium or Association	If the proposer is a group of legal entities that will form or have formed a Joint Venture(JV), Consortium or Association for the proposal, each such legal entity will confirm in their joint proposal that: • they have designated one party to act as a lead entity, duly vested with authority to legally bind the members of the JV, Consortium or Association jointly and severally, and this will be evidenced by a duly notarized agreement among the legal entities, which will be submitted along with the proposal; and • if they are awarded the contract, the contract shall be entered into by and between UNDP and the designated lead entity, who will be acting for and on behalf of all the member entities comprising the joint venture. After the deadline for submission of proposal, the lead entity identified to represent theJV, Consortium or Association shall not be altered without the prior written consent of UNDP. If a JV, Consortium or Association's proposal is the proposal selected for award, UNDPwill award the contract to the joint venture, in the name of its designated lead entity. The lead entity will sign the contract for and on behalf of all other member entities. The lead entity and the member entities of the JV, Consortium or Association shall abideby the provisions of Article 19 (Only one Proposal) herein in respect of submitting only one proposal. The description of the organization of the JV, Consortium or Association must clearly define the expected role of each of the entities in the joint venture in delivering the requirements of the RFP, both in the proposal and the JV, Consortium or Association Agreement. All entities that comprise the JV, Consortium or Association shall be subjectto the eligibility and qualification assessment by UNDP. A JV, Consortium or Association, in presenting its track record and experience, shouldclearly differentiate between: • Those that were undertaken together by the JV, Consortium or Association; and • Those that were undertaken by the individual entities of the JV, Consortium or Association. Previous contracts completed by individual experts working privately but who are permanently or were temporarily associated with any of the member firms cannot be claimed as the experience of the JV, Consortium or Association or those of its members,but should only be claimed by the individual experts themselves in their presentation oftheir individual credentials. JV, Consortium or Associations are encouraged for high value, multi-sectoral requirements when the spectrum of expertise and resources required may not be available within one firm.
19. Only one proposal	The proposer (including the individual members of any Joint Venture) shall submit only one proposal, either in its own name or as part of a Joint Venture. Proposals submitted by two (2) or more proposers shall all be rejected if they are found to have any of the following: • they have at least one controlling partner, director, or shareholder in common; or • any one of them receive or have received any direct or indirect subsidy from the other/s; or • they have the same legal representative for purposes of this RFP; or • they have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about, or influence on the proposal of another proposer regarding this RFP process; • they are subcontractors to each other's proposal, or a subcontractor to one proposal also submits another proposal under its name as lead proposer; or some key personnel proposed to be in the team of one proposer participates in more than one proposal received for this RFP process. This condition relating to • the personnel, does not apply to subcontractors being included in more than one proposal.
20. Alternative proposals	Unless otherwise specified in Section 3: Data Sheet, alternative proposals shall not be considered. If submission of alternative proposals is allowed in Section 3: Data Sheet, a proposer may submit an alternative proposal, but only if it also submits a proposal conforming to the RFP requirements. Where the conditions for its acceptance are met, or justifications are clearly established, UNDP reserves the right to award a contract based on an alternative proposal.

	If multiple/alternative proposals are being submitted, proposer must create an alternate response directly in the system and upload all attachments relevant to the alternate proposal separately together with the alternate response.
21. Pre-proposal conference	When appropriate, a pre-proposal conference will be conducted at the date, time andlocation and according to any instructions specified in Section 3: Data Sheet. If it is stated in Section 3: Data Sheet that the pre-proposal conference is mandatory, a Proposer which does not attend the pre-proposal conference shall become ineligible tosubmit a proposal under this RFP. If it is stated in Section 3: Data Sheet that the pre-proposal conference is not mandatory, non-attendance shall not result in disqualification of an interestedproposer. UNDP will not issue any formal answers to questions from proposers regarding the RFP or proposal process during the pre-proposal conference. All questions shall be submitted in accordance with Article 38 (Clarification of Proposals). The pre-proposal conference shall be conducted for the purpose of providing background information only. Without limiting Article 24 (Proposers' responsibility) proposers shall not rely upon any information, statement or representation made at thepre-proposal conference unless that information, statement or representation is confirmed by UNDP in writing. Minutes of the pre-proposal conference will be disseminated as specified in Section 3:Data Sheet. No verbal statement made during the conference shall modify the terms and conditions of the RFP, unless specifically incorporated in the minutes of the proposer's conference or issued/posted as an amendment to RFP.
22. Site inspection	When appropriate, a site inspection will be conducted at the date, time and locationand according to any instructions specified in Section 3: Data Sheet. If it is stated in Section 3: Data Sheet that the site inspection is mandatory, a proposer who does not attend the site inspection shall become ineligible to submit a proposal under this RFP. If it is stated in Section 3: Data Sheet that the site inspection is not mandatory, non- attendance, shall not result in disqualification of an interested proposer. Proposers participating in a site inspection shall be responsible for making and obtaining any visa arrangements that may be required for the proposers to participate in a site inspection. Prior to attending a site inspection, proposers shall execute an indemnity and a waiverreleasing UNDP in respect of any liability that may arise from: (i) loss of or damage to any real or personal property; (ii) personal injury, disease, or illness to, or death of, any person; (iii) financial loss or expense, arising out of the carrying out of that siteinspection; and (iv) transportation by UNDP to the site (if provided) as a result of anyaccidents or malicious acts by third parties. UNDP will not issue any formal answers to questions from proposers regarding the RFP or solicitation process during a site inspection. All questions shall be submitted in accordance with Article 7 (Clarification of solicitation documents). A site inspection will be conducted for the purpose of providing background information only. Without limiting Article 24 (Proposers Responsibility), proposers shall not rely upon any information, statement or representation made at a site inspection unless that information, statement or representation is confirmed by UNDP in writing.
23. Errors or omissions	Proposers shall immediately notify UNDP in writing of any ambiguities, errors, omissions, discrepancies, inconsistencies, or other faults in any part of the RFP, with full details of those ambiguities, errors, omissions, discrepancies, inconsistencies, or other faults. Proposers shall not benefit from such ambiguities, errors, omissions, discrepancies, inconsistencies, or other faults.
24. Proposers' responsibility to inform themselves	Proposers shall be responsible for informing themselves in preparing their proposal. In this regard, proposers shall ensure that they: • examine and fully inform themselves in relation to all aspects of the RFP, includingthe Contract and all other documents included or referred to in this RFP; • review the RFP to ensure that they have a complete copy of all documents; • obtain and examine all other information relevant to the project and the scope of the requirements available on reasonable enquiry; • verify all relevant representations, statements and information, including those contained or

	referred to in the RFP or made orally during any clarification meetingor site Inspection or any discussion with UNDP, its employees or agents; • attend any pre-proposal conference if it is mandatory under this RFP; • fully inform and satisfy themselves as to requirements of any relevant authoritiesand laws that apply, or may in the future apply, to the supply of the services; and • form their own assessment of the nature and extent of the services required as included in Section 5: Terms of Reference and properly account for all requirementsin their proposal. Proposers acknowledge that UNDP, its directors, employees and agents make no representations or warranties (express or implied) as to the accuracy, currency orcompleteness of this RFP or any other information provided to the proposers.
25. No material change(s) in circumstances	The proposer shall inform UNDP of any change(s) of circumstances arising during the RFP process, including but not limited to: • a change affecting any declaration, accreditation, license or approval; • major re-organizational changes, company re-structuring, a take-over, buy-out or similar event(s) affecting the operation and/or financing of the proposer or its major sub-contractors; • a change to any information on which UNDP may rely in assessing proposals.
SUBMISSION AND OPENING OF PROPOSALS	
26. Instruction for proposal submission	The proposer shall submit a complete proposal in the format and comprising the documents and forms in accordance with requirements in Section 3: Data Sheet. The proposal shall be delivered according to the method specified in Section 3: Data Sheet. The proposal shall be submitted? by the proposer or person(s) duly authorized to commit the proposer. The authorization shall be communicated through a document evidencing such authorization issued by the legal representative of the proposing entity, or, if requested, a Power of Attorney, accompanying the proposal. Proposers must be aware that the mere act of submission of a proposal, in and of itself, implies that the proposer fully accepts the UNDP General Conditions of Contract.
26a. Online submission	Electronic submission through online portal shall be governed as follows: • Electronic files that form part of the proposal must be in accordance with the format and requirements indicated in DS; • The Technical Proposal and the Financial Proposal files MUST BE COMPLETELY SEPARATE and each of them must be uploaded individually and clearly labelled. • The Financial Proposal file must be uploaded separately only in the commercial section of the RFP in the system. • Documents which are required to be in original form (e.g., Bid Security, etc.) must be sent via courier or hand delivery as per the instructions in DS. Detailed instructions on how to submit, modify or cancel a bid in the online portal are provided in the system Bidder User Guide made available in the procurement notice site and in the portal.
27. Deadline for Submission of Proposals	Complete proposals must be received by UNDP in the manner, and no later than the date and time, specified in Section 3: Data Sheet. If any doubt exists as to the time zonein which the Proposal should be submitted, refer to http://www.timeanddate.com/worldclock/. It shall be the sole responsibility of the proposers to ensure that their proposal is received by the closing date and time. UNDP shall accept no responsibility for proposals that arrive late due to any technical issues and shall only recognize the actual date and time that the proposal was received by UNDP. UNDP may, at its discretion, extend this deadline for the submission of proposals by amending the solicitation documents in accordance with Article 8 (Amendment of solicitation documents). In this case, all rights and obligations of UNDP and proposers subject to the previous deadline will thereafter be subject to the new deadline as extended.
28. Withdrawal, substitution and modification of proposals	A proposer may withdraw or modify its proposal after it has been submitted at any timeprior to the deadline for submission directly in the system following the instructions provided in the user guide. However, after the deadline for proposal submission, the proposals shall remain validand open for acceptance by UNDP for the entire proposal validity period, as may be extended.
29. Storage of proposals	Proposals received are kept confidential and unopened in the system as part security protocols built in the system until the proposal opening date stated in Section 3: Data Sheet.
30. Proposal opening	There is no mandatory public bid opening for RFPs however UNDP may at its discretion send a public bid opening report from the system only to suppliers who successfully submitted a proposal. The report will include only the names of the companies but not the financial proposal.

31. Late proposals	Any proposal received by UNDP after the deadline for submission of proposals will be destroyed unless the proposer requests that it be returned and assumes the responsibility and expenses for the re-possession of the returned proposal documents. In exceptional circumstances, late proposals may be accepted if it is determined that the submission was sent in ample time prior to the proposal closing and the delay could not be reasonably foreseen by the proposer or were due to force majeure.
EVALUATION OF PROPOSALS	
32. Confidentiality	Information relating to the examination, evaluation, and comparison of proposals, and the recommendation of contract award, shall not be disclosed to proposers or any other persons not officially concerned with such process, even after publication of the contract award. Any effort by a proposer or anyone on behalf of the proposer to influence UNDP in the examination, evaluation and comparison of the proposals or contract award decisions may, at UNDP's decision, result in the rejection of its proposal and may subsequently be subject to the application of prevailing UNDP's vendor sanctions procedures.
33. Evaluation of proposals	UNDP shall evaluate a proposal using only the methodologies and criteria defined in thisRFP. No other criteria or methodology shall be permitted. UNDP shall conduct the evaluation solely based on the submitted technical andfinancial proposals. Evaluation of proposals shall be undertaken in the following steps: a) Preliminary examination; b) Evaluation of minimum eligibility and qualification (if pre-qualification is notdone); c) Evaluation of technical proposals; d) Evaluation of financial proposals.
34. Preliminary examination	UNDP shall examine the proposals to determine whether they are complete with respect to minimum documentary requirements, whether the documents have been properly signed, and whether the proposals are generally in order, among other indicators that may be used at this stage. UNDP reserves the right to reject any proposal at this stage.
35. Evaluation of eligibility and qualification	Eligibility and qualification of the proposer will be evaluated against the minimum eligibility and qualification requirements specified in Section 4: Evaluation Criteria and in Article 4 (Eligible proposers). In general terms, vendors that meet the following criteria may be considered qualified: a) They are not included in the UN Security Council 1267/1989 Committee's list of terrorists and terrorist financiers, and in UNDP's ineligible vendors' list; b) They have a good financial standing and have access to adequate financial resources to perform the contract and all existing commercial commitments; c) They have the necessary similar experience, technical expertise, production capacity, quality certifications, quality assurance procedures and other resources applicable to the supply of goods and/or services required; d) They are able to comply fully with the UNDP General Terms and Conditions of Contract; e) They do not have a consistent history of court/arbitral award decisions against the Bidder; and f) They have a record of timely and satisfactory performance with their clients.
36. Evaluation of technical and financial proposals	The evaluation team shall review and evaluate the technical proposals on the basis of their responsiveness to the Terms of Reference and other RFP documents, applying the evaluation criteria, sub-criteria, and point system specified in Section 4: Evaluation Criteria. A proposal shall be rendered non-responsive at the technical evaluation stage if it fails to achieve the minimum technical score indicated in Section 3: Data Sheet. When necessary, and if stated in the Data Sheet, UNDP may invite technically responsive proposers for a presentation related to their technical proposals. The conditions for the presentation shall be provided in the proposal document where required. When necessary, and if stated in the Section 3: Data Sheet, UNDP may invite technically responsive bidders for a presentation related to their technical Proposals. The conditions for the presentation shall be provided in the bid document where required. In the second stage, only the financial proposals of those proposers who achieve the minimum technical score will be opened for evaluation. The evaluation method that applies for this RFP shall be as indicated in Section 3: Data Sheet, which may be either of two (2) possible methods, as follows: (a) the lowest priced method which selects the lowest evaluated financial proposal of the technically responsive Proposers; or (b) the

	combined scoring method which will be based on a combination of the technical and financial score. When the Data Sheet specifies a **combined scoring method**, the formula for the rating of the proposals will be as follows: Rating the Technical Proposal (TP): **TP Rating** = (Total Score Obtained by the Offer / Max. Obtainable Score for TP) x 100 Rating the Financial Proposal (FP): **FP Rating** = (Lowest Priced Offer / Price of the Offer Being Reviewed) x 100 Total Combined Score: **Combined Score =** (TP Rating) x (Weight of TP, e.g., 70%) + (FP Rating) x (Weight of FP, e.g., 30%)
37. Post-qualification/ DueDiligence	UNDP reserves the right to undertake a post-qualification assessment, aimed at determining, to its satisfaction, the validity of the information provided by the proposer. Such exercise shall be fully documented and may include, but need not be limited to, all or any combination of the following: a) Verification of accuracy, correctness and authenticity of information provided by the proposer; b) Validation of extent of compliance to the RFP requirements and evaluationcriteria based on what has so far been found by the evaluation team; c) Inquiry and reference checking with Government entities with jurisdiction onthe proposer, or with previous clients, or any other entity that may have done business with the proposer; d) Inquiry and reference checking with previous clients on the performance on on-going or completed contracts, including physical inspections of previous works, as deemed necessary; e) Physical inspection of the proposer's offices, branches or other places where business transpires, with or without notice to the proposer; f) Other means that UNDP may deem appropriate, at any stage within the selection process, prior to awarding the contract.
38. Clarification of proposals	UNDP may request clarification or further information in writing from the proposers atany time during the evaluation process. The proposers' responses shall not contain anychanges regarding the substance or price of the proposal, except to confirm the correction of arithmetic errors discovered by UNDP in the evaluation of the proposals, in accordance with Instructions to Proposers Article 23 (Errors or omissions). NDP may use such information in interpreting and evaluating the relevant proposal but is under no obligation to take it into account. Any unsolicited clarification submitted by a proposer in respect to its proposal which is not a response to a request by UNDP, shall not be considered during the review and evaluation of the proposals.
39. Responsiveness of proposal	UNDP's determination of a proposal's responsiveness is to be based on the contents of the proposal itself. A substantially responsive proposal is one that conforms to all the terms, conditions, TOR and other requirements of the RFP without material deviation, reservation, or omission. A material deviation, reservation, or omission is one that: a) affects in any substantial way the scope, quality, or performance of the servicesspecified in the contract; or b) limits in any substantial way, inconsistent with the solicitation documents, UNDP's rights or the proposer's obligations under the contract; or c) if rectified would unfairly affect the competitive position of other proposerspresenting substantially responsive proposals. If a proposal is not substantially responsive, it shall be rejected by UNDP and may notsubsequently be made responsive by the proposer, by correction of the material deviation, reservation, or omission.
40. Nonconformities, reparable errors and omission	Provided that a proposal is substantially responsive, UNDP may waive any non- conformities or omissions in the proposal that, in the opinion of UNDP, do not constitute a material deviation. These are a matter of form and not of substance and can be corrected or waived without being prejudicial to other proposers. Provided that a proposal is substantially responsive UNDP may request the proposer to submit the necessary information or documentation, within a reasonable period, to rectify nonmaterial nonconformities or omissions in the proposal related to documentation requirements. Such omission shall not be related to any aspect of the price of the proposal. Failure of the proposer to comply with the request may result in the rejection of its proposal. For financial proposals that have been opened, UNDP shall check, and correctarithmetical errors as

	follows: a) if there is a discrepancy between the unit price and the line-item total that isobtained by multiplying the unit price by the quantity, the unit price shall prevail and the line-item total shall be corrected, unless in the opinion of UNDP there is an obvious misplacement of the decimal point in the unit price; in which case, the line item total as quoted shall govern and the unit price shall be corrected; b) if there is an error in a total corresponding to the addition or subtraction ofsubtotals, the subtotals shall prevail, and the total shall be corrected; and c) if there is a discrepancy between words and figures, the amount in wordsshall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail. If the proposer does not accept the correction of errors, its proposal shall be rejected,and its proposal security may be forfeited.
41. Right to accept any proposal and to reject any or all proposals	UNDP reserves the right to accept or reject any proposals, and to annul the proposal process and reject all proposals at any time prior to contract award, without thereby incurring any liability to the affected proposer or proposers or any obligation to inform the affected proposer or proposers of the grounds for UNDP's action. UNDP shall not beobliged to award the contract to the lowest priced offer.
AWARD OF CONTRACT	
42. Award criteria	Prior to expiration of the proposal validity, UNDP shall award the Contract to the qualified proposer based on the award criteria indicated in Section 3: Data Sheet.
43. Right to vary requirement at time of award	At the time the Contract is awarded, UNDP reserves the right to increase or decrease the quantity of services originally specified by up to a maximum twenty-five per cent (25%) of the total offer, without any change in the unit price or other terms and conditions and the solicitation document.
44. Notification of award	Prior to the expiration of the period of proposal validity, UNDP will notify the successful proposer in writing by email, fax or post, that its proposal has been accepted. Please note that the proposer, if not already registered at the appropriate level in UNGM, will be required to complete the vendor registration process on the UNGM prior to the signature and finalization of the contract.
45. Debriefing	In the event that a proposer is unsuccessful, the proposer may request a debriefing from UNDP. The purpose of the debriefing is to discuss the strengths and weaknesses of the proposer's submission, in order to assist the proposer in improving its future proposals for UNDP procurement opportunities. The content of other proposals and how they compare to the proposer's submission shall not be discussed.
46. Publication of contract award	UNDP will publish the contract award on UNDP Procurement Notices website https://procurement-notices.undp.org/view_awards.cfm which is linked to the UnitedNations Global Marketplace, with the RFP Reference number, the information of the awarded proposer's company name, contract amount or LTA and the date of the contract.
47. Contract Signature	Within fifteen (15) days from the date of receipt of the Contract, the successful Bidder shall sign and date the Contract and return it to UNDP. Failure to do so may constitute sufficient grounds for the annulment of the award, and forfeiture of the Bid Security, if any, and on which event, UNDP may award the Contract to the Second highest rated or call for new Bids.
48. Contract Type and General Terms and Conditions	The types of Contract to be signed and the applicable UNDP Contract General Termsand Conditions, as specified in Data Sheet, can be accessed at: http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html
49. Performance security	The successful Proposer, if so specified in Section 3: Data Sheet shall furnish a Performance Security in the amount and form specified herein: https://popp.undp.org/_layouts/15/WopiFrame.aspx?sourcedoc=/UNDP_POPP_DOCUMENT_LIBRARY/Public/PSU_Solicitation_Performance%20Guarantee%20Form.docx&action=default , within the specified number of days after receipt of the Contract from UNDP. Banks issuing performance securities must be acceptable to the UNDP comptroller, i.e. banks certified by the central bank of the country to operate as a commercial bank. The Performance Security form is available here. UNDP shall promptly discharge the proposal securities of the unsuccessful proposers pursuant to Article 17 (Proposal security). Failure of the successful proposer to submit the above-mentioned Performance Securityor sign the Contract shall constitute sufficient grounds for the annulment of the award and forfeiture of the proposal security. In that event UNDP may award the contract to the next lowest ranked proposer.

50. Bank guarantee for advance payment	Except when the interests of UNDP so require, it is UNDP's standard practice not to make advance payment(s) (i.e., payments without having received any outputs). If anadvance payment is allowed as per Section 3: Data Sheet, and if specified there, the proposer shall submit a Bank Guarantee in the full amount of the advance payment using this bank guarantee form available at: https://popp.undp.org/_layouts/15/WopiFrame.aspx?sourcedoc=/UNDP_POPP_DOCUMENT_LIBRARY/Public/PSU_Contract%20Management%20Payment%20and%20Taxes_Advanced%20Payment%20Guarantee%20Form.docx&action=default . Banks issuingbankguarantees must be acceptable to the UNDP comptroller, i.e. banks certified by the central bank of the country to operate as a commercial bank.
51. Liquidated Damages	If specified in Section 3: Data Sheet, UNDP shall apply Liquidated Damages for the damages and/or risks caused to UNDP resulting from the Contractor's delays or breachof its obligations as per the Contract. The payment or deduction of such liquidated damages shall not relieve the Contractor from any of its other obligations or liabilities pursuant to any current contract or purchase order.
52. Proposal protest	Any proposer that believes to have been unjustly treated in connection with this proposal process or any contract that may be awarded as a result of such proposal process may submit a complaint to UNDP. The following link provides further details regarding UNDP vendor protest procedures: http://www.undp.org/content/undp/en/home/procurement/business/protest-and-sanctions.html
53. Other Provisions	In the event that the Bidder offers a lower price to the host Government (e.g., General Services Administration (GSA) of the federal government of the United States of America) for similar goods and/or services, UNDP shall be entitled to the same lower price. The UNDP General Terms and Conditions shall have precedence. UNDP is entitled to receive the same pricing offered by the same Contractor in contracts with the United Nations and/or its Agencies. The UNDP General Terms and Conditions shall have precedence. The United Nations has established restrictions on employment of (former) UN staff who have been involved in the procurement process as per bulletin ST/SGB/2006/15 http://www.un.org/en/ga/search/view_doc.asp?symbol=ST/SGB/2006/15&referer

SECTION 3: DATA SHEET (DS)

The following specific data shall complement, supplement or amend the provisions in Section 2: Instructions to Proposers. In case there is a conflict, the provisions herein shall prevail over those in Section 2: Instructions to Proposers.

No.	Data	Specific Instructions / Requirements
1.	Scope	The reference number of this Request for Proposal (RFP) is **RfP26/03336: Company to conduct a Cybersecurity Operational Evaluation, Specialized Tools Requirements, and ISMS Certification Readiness for the Ministry of Foreign Affairs.** This will cover governance, processes, technology (hardware, software, applications, networks, and security infrastructure), as well as institutional capacities and resources, in order to identify cybersecurity gaps, tools requirements, and operational risks, and to define mitigation measures, strategic priorities, and modernization actions required to strengthen the Ministry's cyber resilience and cybersecurity posture, as further described in Section 5 of this RFP.
2.	Eligible proposers	Proposers from all countries are eligible to participate in this proposal process.
3.	Clarification of solicitation documents	Any request for clarification of solicitation documents must be sent directly in the system through **Quantum message functionality**. **ATTENTION: PROPOSALS (OR ANY PART OF IT) SHALL NOT BE SUBMITTED IN THE ABOVE MANNER.**
		Deadline for submitting requests for clarifications / questions: **5 days before the submission deadline**
		Supplemental information to the RFP and responses / clarifications to queries will be posted directly in the system.
4.	Language	All proposals, information, documents and correspondence exchanged between UNDP and the proposers in relation to this solicitation process shall be in **Romanian and English**
5.	Partial proposals	Submitting proposals for parts or sub-parts of the TOR is: **Not allowed**
6.	Currencies	Legal entities registered in the Republic of Moldova should quote in **Moldovan leu (MDL).** Legal entities registered in any other country should quote in **US Dollars (USD)** UNDP shall not be kept liable for any fluctuations of the exchange market during contract implementation, the Contractor being legally responsible to register any loss/gain of currency exchange resulting from payments against the Contract in accordance with the national legislation.
7.	Duties and taxes	All prices shall: **Be exclusive of VAT and other applicable indirect taxes.**
8.	Proposal validity period	90 days
9.	Proposal security	Not Required
10.	Alternative proposals	Shall not be considered.
11.	Pre-proposal conference	Will not be conducted
12.	Site inspection	A site inspection will not be held.
13.	Instructions for proposal submission	**Bidders must submit their proposal directly in Quantum.** ▪ File Format: PDF files only ▪ File names must be maximum 60 characters long and must not contain any letter or special character other than from Latin alphabet/keyboard. ▪ All files must be free of viruses and not corrupted.

No.	Data	Specific Instructions / Requirements
		▪ It is recommended that bidders organize and name the files according to the requirements and structure of the bid to facilitate their review. ▪ The bidder should receive an email acknowledging email receipt from the system. ▪ **The Financial Proposal (Forms J and K) shall be submitted directly in the system only in the "Commercial section" of the requirements. Non-compliance with this instruction may result in rejection of the proposal received.**
14.	Deadline for proposal submission	Deadline for proposal submission is **indicated in the portal**. In case of discrepancies between the deadline in the system and deadline indicated elsewhere, the one in the system prevails. **Note that system time zone is in EST/EDT (New York) time zone.**
15.	Proposal Opening	Public proposal opening will **NOT** be held
16.	Evaluation of technical and financial proposals	Evaluation will be based on: ☒ Combined scoring method using a distribution of 70%-30% Technical proposal - financial proposal The maximum number of technical points is detailed in Section 4: Evaluation Criteria To be substantially compliant, Proposers must obtain a minimum threshold of 70% of maximum points from technical evaluation.
17.	Right to vary requirement at time of award	The maximum percentage by which quantities may be increased is 25% The maximum percentage by which quantities may be decreased is 25%
18.	Contract award to one or more proposer	UNDP will award a contract to: **One Bidder Only**
19.	Type of contract to be awarded	**Contract Face Sheet** More information can be accessed at http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html See Section 6 for link to sample contract.
20.	Expected date for commencement of contract	1 October 2026
21.	Conditions of contract to apply	**UNDP General Terms and Conditions for contracts (goods and/or services)** See Section 6 for link to the contract terms.
22.	Performance Security	Not Required
23.	Advance payment	Not Allowed
24.	Liquidated damages	Will be imposed as follows: Percentage of contract price per week of delay: 2.5%, up to a maximum of 10% of the Contract value, after which UNDP may terminate the contract.
25.	Documents to be submitted with your Proposal	▪ Company Profile, which should not exceed fifteen (15) pages, including printed brochures and product catalogues relevant to the services being procured. The document shall include company portfolio, demonstrating experience in implementation of projects with similar content and similar complexity ▪ Certificate of Incorporation/ Business Registration ▪ List of Shareholders and Other Entities Financially Interested in the Firm owning 5% or more of the stocks and other interests, or its equivalent if Bidder is not a corporation including the Certificate from State Register ▪ Certification related to information security management (ISO/IEC 27001 or equivalent), received by the Bidder

No.	Data	Specific Instructions / Requirements
		▪ Other Quality Certificate (e.g., ISO 9001, ISO 20000, etc.) and/or other similar certificates, accreditations, awards and citations received by the Bidder, if any ▪ Tax Registration Payment Certificate issued by the Internal Revenue Authority evidencing that the Bidder is updated with its tax payment obligations, or Certificate of Tax exemption, if any such privilege is enjoyed by the Bidder ▪ Financial Statement (Income Statement and Balance Sheet) including Auditor's Reports (for international companies) or registered Financial Report at the Statistical Bureau (for local companies) for the past 3 years (2025, 2024, 2023). ▪ Statement of Satisfactory Performance from the Top three (3) Clients in terms of Contract Value in the past three (3) years (in case of JV/Consortium/Association, of the leader of the consortium) ▪ A copy of preliminary Agreement in case of Joint Venture/Consortium/Association ▪ Detailed description of the Methodology, Approach and Implementation Plan (sequence of actions) for the services required in the ToR. The distribution of roles and responsibilities of the proposed key personnel should be reflected. The proposal shall include but shall not be limited to project management organizational structure/chart with clear roles and responsibilities; approach to project planning and implementation, including detailed activity planning; resource allocation and management arrangements; communication and coordination plan; change management and risk management approach; quality control measures for deliverable; progress monitoring and reporting. ▪ Copies of contracts (minimum 3 in the last 5 years) to prove that Offeror meets the similar experience requirement (stated under Section 4: Evaluation Criteria) ▪ CVs and Statements of Exclusivity and Availability (signed by the envisaged person) of the Key personnel (mentioned in ToR), together with relevant professional certifications (if applicable/e.g., diplomas, certificates) and training certificates (if applicable) (valid at the date of presentation) clearly stipulating the relevant experience which meets the listed requirements. ▪ A written statement certifying that the proposed key personnel have no personal, professional, or financial conflict of interest under the envisaged contract ▪ **Dully filled in Proposal Forms A-K (as per Section 7: Proposal Forms).** **Forms A-I, representing the Technical Proposal, shall be submitted directly in the system in the "Technical section" of the requirements.** ▪ **Forms J and K, representing the Financial Proposal shall be submitted directly in the system only in the "Commercial section" of the requirements. Please, ensure that no other documents are disclosing your financial proposal apart from Forms J and K. Non-compliance with this instruction may result in rejection of the proposal received.**

SECTION 4: EVALUATION CRITERIA

Preliminary Examination Criteria

All criteria will be evaluated on a **Pass/Fail basis** and checked during Preliminary Examination.

Criteria	Documents to establish compliance
Completeness of the Proposal	All documents requested in Section 2: Instructions to Bidders Articles 11 and 12 have been provided and are complete.
Proposer accepts UNDP General Conditions of Contract as specified in Section 6.	Duly signed and stamped Form C: Technical Proposal Submission has been provided.
Proposal Validity	Duly signed and stamped Form C: Technical Proposal Submission has been provided.
Appropriate signatures	Proposal Forms have been duly signed and stamped.
Power of Attorney [if applicable]	Certified Letter of Appointment and/or power of attorney authorizing the representative of the Bidder to sign bids has been provided.

Minimum Eligibility and Qualification Criteria

Minimum eligibility and qualification criteria will be evaluated on a **Pass/Fail basis**.

If the Proposal is submitted as a Joint Venture, Consortium or Association, each member should meet the minimum criteria, unless otherwise specified.

Eligibility Criteria	Documents to establish compliance
Legal Status: Vendor is a legally registered entity and can ensure rapid local response (including presence of staff) to any of the contract related requests (whether though a local branch or office, through a local consortium partner or other – all relationships to be documented through official documents and valid contracts submitted with the Proposal).	Form D: Proposer Information
Diversity, Inclusion and Belonging: Proposer belongs to a diverse supplier group, including micro, small or medium sized enterprise, women or youth owned business or other civil society organization	Form D: Proposer Information
Eligibility: Vendor is not suspended, nor otherwise identified as ineligible by any UN Organization, the World Bank Group or any other International Organisation in accordance with Section 2 Article 4.	Form C: Technical Proposal Submission
Conflict of Interest: No conflicts of interest in accordance with Section 2 Article 4.	Form C: Technical Proposal Submission
Bankruptcy: The Proposer has not declared bankruptcy, is not involved in bankruptcy or receivership proceedings, and there is no judgment or pending legal action against the vendor that could impair its operations in the foreseeable future	Form C: Technical Proposal Submission

Qualification Criteria	Documents to establish compliance
History of non-performing contracts[1]: Non-performance of a contract did not occur as a result of contractor default within the last 3 years[1].	Form F: Eligibility and Qualification
Litigation History: No consistent history of court/arbitral award decisions against the Proposer for the last 3 years.	Form F: Eligibility and Qualification
Previous Experience:	
At least five (5) years of experience in providing consultancy services related to the assessment of compliance and implementation of ICT and cyber security projects in Moldova (based on national legislation and international recognized standards for cybersecurity and ICT management); *(For JV/Consortium/Association, **Lead company** should meet requirement. Each other **consortium Partner** should have at least three (3) years of the above indicated experience.)*	Form F: Eligibility and Qualification
At least three (3) contracts of similar nature and complexity, in providing consultancy services in Moldova related to the implementation of national and/or internationally recognized cybersecurity and/or information management standards and/or frameworks, over the last 5 years. *(For JV/Consortium/Association, **Lead company** should meet requirement).*	Form F: Eligibility and Qualification
Valid Information Security Management Certification (ISO/IEC 27001 or equivalent) *(For JV/Consortium/Association, **Lead company** should meet requirement).*	Attach required documents to Form F: Eligibility and Qualification
Minimum Key Personnel:	
The Key personnel mandatory for the implementation of the contract:	Attach required documents to Form H: Format for CV of proposed Key Personnel
• Project Manager (Team Leader/ Information Security Governance Expert) • ICT Infrastructure & Security Integration Architect • Application Security Expert (Software Auditor) • Business Continuity & Crisis Management Expert ***Please note**: The above listed roles can be cumulated by certain team members, but not more than two roles per team member, clarifying in the Methodology the reasoning for such approach and distribution of tasks.* ***Please note: None of additional staff will be admitted to the project.*** *The Bidder shall formally disclose if any proposed key experts have any ongoing or active contract*	

engagements with UNDP. *(For JV/Consortium/Association, **all Parties** cumulatively should meet requirement. Project Manager should be an employee of the **Lead company**)*	
Financial Standing:	
Turnover: Minimum average annual turnover of USD 150,000 for the last 3 (three) years. *(For JV/Consortium/Association, **all Parties** should meet the requirement).*	Copy of audited financial statements for the last 3 (three) years. Form F: Eligibility and Qualification
Liquidity: The Ratio Average current assets / Current liabilities over the last 3 (three) years must be equal or greater than 1. If QR is less than 1: UNDP shall verify financial capacity of the bidder and has the authority to seek references from concerned parties & banks on the bidder financial standing. UNDP has the right to reject any bid if submitted by a contractor whom investigation leads to a result that he is not financially capable and/or had serious financial problems. *(For JV/Consortium/Association, **all Parties** should meet requirement cumulatively).*	Copy of audited financial statements for the last 3 (three) years. Form F: Eligibility and Qualification

Technical Evaluation Criteria

Summary of Technical Proposal Evaluation Forms		Points Obtainable
1.	Proposer's qualification, capacity, and experience	300
2.	Proposed Methodology, Approach, and Implementation Plan	400
3.	Management Structure and Key Personnel	300
	Total	**1000**

	Section 1. Proposer's qualification, capacity and experience	Points obtainable
1.1	Reputation of Organization and Staff Credibility / Reliability / Industry Standing Organization / Company profile – 25 points: • Excellent (25 pts): The company is a well-known, top-tier market leader with an impeccable reputation for reliability and quality. Staff are recognized experts. Supported by strong, verifiable references and positive industry analysis. • Good (22.5 pts): The company is well-known and has a good standing in the field. There is positive evidence of reliability and staff credibility, but it may not be a top-tier leader. Supported by good references. • Satisfactory (17.5 pts): The company is known in the industry but may have a mixed or limited reputation. Staff credibility is adequate but not exceptional. References are satisfactory but may have minor issues. • Poor (10 pts): The company is not well-known, has a poor reputation, or lacks verifiable evidence of industry standing and staff credibility. References are weak or unavailable. Clarification may be required. • Very Poor (2.5 pts): The submission provides minimal or no credible information regarding the company's reputation or staff credibility and is not supported by evidence to demonstrate ability to comply with requirements. • No Submission (0 pts): Information has not been submitted or is unacceptable.	**25**
1.2	General Organizational Capability which is likely to affect implementation: management structure, financial stability and project financing capacity, project management controls, extent to which any work would be subcontracted: • Age of the legal entity (public/business association, public/business support organization, public/business development service provider, etc.) (5 years – 10 pts, 2 pts for each additional year, up to 20 pts) • Project management support mechanism (no – 0 pts, yes – 10 pts.) • Project management controls (no – 0 pts, yes – 10 pts.) • Financial standing – (at least USD 150,000 of average annual turnover during the last three (3) years – 15 pts, each additional USD 50,000 – 2,5 pts, up to a maximum of 20 pts)	**60**
1.3	Relevance of specialized knowledge and experience on similar engagements done in the region / country: • Have at least five (5) years of experience providing consultancy services related to the assessment of compliance and implementation of ICT and cyber security projects (based on national legislation and international recognized standards for cybersecurity and ICT management); (5 years – 30 pts, 5 pts for each additional year, up to 55 pts); • At least three (3) contracts of similar nature and complexity, in providing consultancy services related to the implementation of national and/or internationally recognized cybersecurity and/or information management standards and/or frameworks over the last 5 years (3 contracts – 40 points, 5 points for each additional contract, up to 50 points);	**200**

	• Information Security Management Certifications (ISO/IEC 27001 or equivalent), and other relevant to the assignment (ISO/IEC 27001 certification – 15 pts, each additional certification 5 pts, up to 20 pts). • Proven experience in projects for Central public administration authorities, ministries, agencies, or other public sector entities will be considered a strong advantage (no experience – 0 pts, 1-2 relevant contracts – 15 pts, 3 and more relevant contracts – 25 pts); • Proven previous experience in providing consultancy services related to the assessment of compliance with ICT and cybersecurity standards and frameworks in the Republic of Moldova or in the region of Eastern Europe is an advantage (no experience – 0 pts, 1-2 relevant contracts – 10 pts, 3 relevant contracts – 15 pts, each additional contract – 5 pts, up to 30 pts); • Previous proven experience of working with UNDP and/or other international development partners is an asset (no experience – 0 pts, 1-2 contracts – 10 pts, 3 and more contracts – 20 pts).	
1.4	Organizational Commitment to Sustainability: • Organisation is compliant with ISO 14001 or ISO 14064 or equivalent – 5 pts; • Organisation is a member of the UN Global Compact – 5 pts; Organization demonstrates significant commitment to sustainability through some other means (for example internal company policy documents on women empowerment, renewable energies or membership of trade institutions promoting such issues) – 5 pts.	**15**
	Total Section 1	**300**
	Section 2. Proposed Methodology, Approach and Implementation Plan	**Points obtainable**
2.1	To what degree does the Proposer understand the task? (up to max 60 pts.): • Excellent (60 pts): The Proposer demonstrates a comprehensive understanding of the assignment. The proposed approach and methodology fully address the TOR requirements and clearly demonstrate how the objectives and expected results will be achieved. • Good (54 pts): The Proposer demonstrates a good, but not comprehensive, understanding of the assignment. The proposed approach and methodology address all key TOR requirements, although some elements could be further elaborated or clarified. • Satisfactory (42 pts): The Proposer demonstrates a basic or partial understanding of the assignment. The proposed approach and methodology address the main TOR requirements but lack sufficient detail or require some adjustments. • Poor (24 pts): The Proposer demonstrates limited understanding of the assignment. The proposed approach and methodology require major adjustments to adequately address the TOR requirements. • Very Poor (6 pts): The Proposer demonstrates minimal understanding of the assignment. The proposed approach and methodology do not adequately address the TOR requirements and provide insufficient evidence of the Proposer's ability to perform the assignment. • No Submission (0 pts): Information has not been submitted or is unacceptable.	**60**
2.2	Have the important aspects of the task been addressed in sufficient detail? (up to max 80 pts): • Excellent (80 pts): All important aspects of the assignment are comprehensively addressed in sufficient detail. The proposed methodology is clear, complete, and project-specific, requiring no clarification. • Good (72 pts): Most important aspects of the assignment are addressed in sufficient detail. The proposed methodology is appropriate and requires only minor clarification or elaboration. • Satisfactory (56 pts): The important aspects of the assignment are generally addressed; however, some elements lack sufficient detail or require clarification.	**80**

	• Poor (32 pts): Several important aspects of the assignment are insufficiently addressed. The proposed methodology requires significant clarification or further development. • Very Poor (8 pts): The important aspects of the assignment are minimally addressed. The proposed methodology lacks sufficient detail and raises significant concerns regarding its adequacy. • No Submission (0 pts): Information has not been submitted or is unacceptable.	
2.3	Is the adopted conceptual framework appropriate for the task? (up to max 80 pts): • Excellent (80 pts): The Proposer demonstrates a comprehensive understanding of the assignment. The presented conceptual framework is fully appropriate for the assignment, all important aspects are comprehensively described, and all TOR requirements are clearly addressed. • Good (72 pts): The Proposer demonstrates a good, but not comprehensive, understanding of the assignment. The conceptual framework is appropriate and addresses all key aspects of the assignment, although some elements could be further elaborated or clarified. • Satisfactory (56 pts): The Proposer demonstrates a basic or partial understanding of the assignment. The conceptual framework addresses the main requirements but lacks sufficient detail, depth, or consistency and requires some adjustments. • Poor (32 pts): The Proposer demonstrates limited understanding of the assignment. The presented conceptual framework requires major adjustments to adequately address the TOR requirements. • Very Poor (8 pts): The Proposer demonstrates minimal understanding of the assignment. The conceptual framework is inappropriate or incomplete and does not demonstrate the Proposer's ability to address the assignment requirements. • No Submission (0 pts): Information has not been submitted or is unacceptable.	**80**
2.4	Is the presentation clear and is the sequence of activities and the planning logical, realistic and promise efficient implementation of the project? (up to max 40 pts.) • Excellent (40 pts): The proposal is clearly presented, well structured, and logically organized. The sequence of activities and implementation plan are realistic, coherent, and demonstrate a high likelihood of efficient implementation of the assignment. • Good (36 pts): The proposal is clear and well structured. The sequence of activities is logical and realistic, although some aspects could be further elaborated or refined. • Satisfactory (28 pts): The proposal is generally clear and structured. The sequence of activities is mostly logical but contains some weaknesses or inconsistencies that require minor adjustments. • Poor (16 pts): The proposal lacks clarity or structure in several areas. The sequence of activities or implementation plan requires major adjustments to ensure effective implementation. • Very Poor (4 pts): The proposal is poorly structured, difficult to follow, and does not present a logical or realistic implementation plan. The proposed sequence of activities raises significant concerns regarding the feasibility of implementation. • No Submission (0 pts): Information has not been submitted or is unacceptable.	**40**
2.5	Understanding of the Republic of Moldova's institutional, cybersecurity, and regulatory environment and proposed local implementation approach. (Maximum 140 points) • Excellent (140 pts): The Proposer demonstrates a comprehensive understanding of the Republic of Moldova's institutional, cybersecurity, and regulatory environment. The proposed team includes experts with extensive and directly relevant experience in Moldova and/or comparable governmental environments, particularly in cybersecurity, information security governance, crisis management, critical infrastructure protection, or public sector digital transformation. The proposed methodology comprehensively addresses stakeholder engagement, secure handling of sensitive information, field activities, coordination with national institutions, and local implementation arrangements, clearly demonstrating the Proposer's capacity to successfully implement the assignment.	**140**

	• Good (126 pts): The Proposer demonstrates a good, but not comprehensive, understanding of the Republic of Moldova's institutional, cybersecurity, and regulatory environment. The proposed team includes experts with relevant local or comparable governmental experience. The proposed methodology adequately addresses stakeholder engagement, secure handling of sensitive information, coordination with national institutions, and local implementation arrangements, although some aspects could be further elaborated or strengthened. • Satisfactory (98 pts): The Proposer demonstrates a basic or partial understanding of the Republic of Moldova's institutional, cybersecurity, and regulatory environment. The proposed team includes limited local or comparable governmental experience. The proposed methodology addresses the main requirements related to stakeholder engagement, secure handling of sensitive information, coordination with national institutions, and local implementation but lacks sufficient detail or requires some adjustments. • Poor (56 pts): The Proposer demonstrates limited understanding of the Republic of Moldova's institutional, cybersecurity, and regulatory environment. The proposed team provides limited evidence of relevant local or comparable governmental experience. The proposed methodology requires major adjustments to adequately address stakeholder engagement, secure handling of sensitive information, coordination with national institutions, and local implementation arrangements. • Very Poor (14 pts): The Proposer demonstrates minimal understanding of the Republic of Moldova's institutional, cybersecurity, and regulatory environment. The proposed team lacks relevant experience, and the proposed methodology does not adequately address stakeholder engagement, secure handling of sensitive information, coordination with national institutions, or local implementation requirements. • No Submission (0 pts): Information has not been submitted or is unacceptable.		
	Total Section 2		**400**
	Section 3. Management Structure and Key Personnel		**Points obtainable**
3.1	**Project Manager (Team Leader/ Information Security Governance Expert)**		**95**
	University degree in the field of Computer Science and/or Information Technologies, or another relevant technical sciences field. (10 pts)	10	
	At least ten (10) years of professional experience in information security governance, risk management, and compliance evaluation of ISMS within public sector institutions or enterprise-level organizations. (less than 10 years – 0 pts, 10 years – 15 pts, each additional year – 2,5 pts, up to 20 pts)	20	
	Proven professional experience dealing with cyber security governance, evaluation and implementation of ISMS, ICT infrastructure and cybersecurity systems within Moldovan state/governmental institutions in at least 4 (four) similar projects. (less than 4 projects – 0 pts, 4 projects – 10 pts, each additional project – 2 pts, up to 12 pts)	12	
	Demonstrated experience in applying cybersecurity regulatory requirements, including the Republic of Moldova cybersecurity regulatory framework (GD No. 562/2025) and/or EU cybersecurity frameworks such as NIS2 and CER Directive. (less than 1 projects – 0 pts, 2 projects – 4 pts, each additional project – 2 pts, up to 8 pts)	8	
	Experience as Project Manager/Team Leader in at least 3 (three) projects implemented within the last five (5) years, involving similar scope, and complexity to the assignment. (less than 3 projects – 0 pts, 3 projects – 10 pts, each additional project – 2,5 pts, up to 15 pts)	15	
	Proven experience in working with international development organizations, in at least two (2) similar projects.	10	

	(less than 2 projects – 0 pts, 2 projects – 6 pts, each additional project – 2 pts, up to 10 pts)		
	Certifications in IT Audit (CISA), ICT Governance, Informational Security Management, ISO 27001 Lead implementer, or other relevant fields will be a strong advantage (no certification – 0 pts, 1 certificate – 3 pts, 2 certificates – 6, each additional certificate 2 pts, up to 10 pts)	10	
	Proficiency in Romanian and English (verbal and writing) (Romanian – 5 pts, English – 5 pts). Romanian is mandatory.	10	
3.2	**ICT Infrastructure & Security Integration Architect**		**85**
	University degree in areas such as computer sciences, engineering, telecommunications or related fields. (10 pts)	10	
	Minimum seven (7) years of experience in enterprise IT infrastructure design, cloud architecture and security engineering. (less than 7 years – 0 pts, 7 years – 10 pts, each additional year – 2 pts, up to 16 pts)	16	
	Proven experience in implementation and/or provision consultancy/advisory services related to assessment of ICT and cyber security processes and tools and cloud-based infrastructures (at least 3 projects within the last five (5) years). (less than 3 projects – 0 pts, 3 projects – 10 pts, each additional project – 2 pts, up to 16 pts)	16	
	Demonstrated experience in architecting telemetry data pipelines, centralized Log Management Systems (LMS), and SIEM solutions (including log correlation rules and retention strategy design (less than 3 records – 0 pts, 3 records – 6 pts, each additional record – 2 pts, up to 10 pts)	10	
	Proven experience in defining technical requirements for specialized security tools, including AI/ML-powered (EDR/XDR) network anomaly detection platforms (e.g., Darktrace or equivalents). (less than 3 records – 0 pts, 3 records – 6 pts, each additional record – 2 pts, up to 10 pts)	10	
	Proven experience within the public sector in at least 3 (three) similar projects within the last five (5) years (less than 3 projects – 0 pts, 3 projects – 4 pts, each additional project – 2 pts, up to 8 pts)	8	
	Certifications: Azure Solutions Architect Expert, Azure Security Engineer Associate (AZ-500), or vendor-neutral certifications such as CISSP (Certified Information Systems Security Professional) or Certified Cloud Security Professional (CCSP by ISC^2), or similar (no certification – 0 pts, 1 certificate – 3 pts, 2 certificates – 6, each additional certificate 2 pts, up to 10 pts).	10	
	Proficiency in Romanian and English languages (Each language 2,5 pts, up to max of 5 pts.)	5	
3.3	**Application Security Expert (Software Auditor)**		**60**
	University degree in IT management, Computer Sciences, computer engineering or other relevant discipline. (10 pts)	10	
	Minimum seven (7) years of professional experience in, application security testing and implementing security mechanisms in complex systems or secure software architecture. (less than 7 years – 0 pts, 7 years – 5 pts, each additional year – 2.5 pts, up to 10 pts)	10	
	Demonstrated experience (at least three (3) track records within the last five (5) years) supervising or assessing complex software implementation processes (including documentation, QA/UAT, pen-test and software audit, specifically SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), and SCA (Software Composition Analysis). (less than 3 track records – 0 pts, 3 track records – 5 pts, each additional track record – 2,5 pts, up to 15 pts)	15	
	Proven experience within the last five (5) years in drafting technical specifications and tender documents for informational systems security audits and penetration testing. (less than 2 projects – 0 pts, 2 projects – 5 pts)	5	

	Working experience within Moldovan state/governmental institutions within the last five (5) years is a strong advantage (yes – 5 pts, no - 0 pts)	5	
	At least one of the following certifications: CSSLP (Certified Secure Software Lifecycle Professional), OSCP (Offensive Security Certified Professional), or equivalent application security certifications (no certification – 0 pts, 1 certificate – 5 pts, 2 certificates – 8, each additional certificate 2 pts, up to 10 pts)	10	
	Proficiency in Romanian and English languages (Each language 2,5 pts, up to max of 5 pts.)	5	
3.4	**Business Continuity & Crisis Management Expert**		**60**
	University degree in areas such as computer sciences, engineering, telecommunications or related (10 pts)	10	
	Minimum seven (7) years of experience in business continuity planning and disaster recovery (less than 7 years – 0 pts, 7 years – 7 pts, each additional year – 1 pts, up to 10 pts).	10	
	Proven experience in developing business continuity and operational resilience strategies and related SOP, aligned with ISO 22301 and crisis management protocols aligned with ISO 22361. Experience in conducting Business Impact Analyses (BIA), mapping critical operational disruption scenarios, and guiding organizations in defining RTO (Recovery Time Objectives) and RPO (Recovery Point Objectives). (less than 3 track records – 0 pts, 3 track records – 5 pts, each additional track record – 2,5 pts, up to 15 pts).	15	
	Previous proven experience (at least 3 track records within the last five (5) years) in similar projects within public sector institutions or enterprise-level organizations (less than 3 projects – 0 pts, 3 projects – 10 pts, each additional project – 2,5 pts, up to 10 pts)	10	
	Certifications: ISO 22301 Lead Implementer/Auditor, CBCP (Certified Business Continuity Professional), or equivalent professional crisis management credentials. (no certification – 0 pts, 1 certificate – 6 pts, each additional certificate 2 pts, up to 10 pts)	10	
	Proficiency in Romanian and English (verbal and writing) (Each language 2,5 pts, up to max of 5 pts)	5	
	Total Section 3		**300**

SECTION 5: TERMS OF REFERENCE

A. Background information

The Republic of Moldova is at a tipping point where the protracted regional security crisis, country's energy vulnerability and divide of the society could derail the development trajectory. The war in Ukraine continues to affect the Republic of Moldova in multiple ways and has significantly increased the country's political, economic, social, security and environmental fragility. This complex situation poses multiple threats, further aggravated by internal vulnerabilities, limited institutional capacities, and societal divisions. The cyberattacks on public institutions, services, and infrastructure become more frequent and severe.

The risks of foreign interference and hybrid threats underscore the pressures Moldova faces as it strives to assert its sovereignty and protect its democratic processes. Considering the highly polarized context of the 2024 presidential elections and EU integration constitutional referendum, the risks of crisis situations aimed at destabilizing the critical infrastructure and disrupting provision of governmental services are likely to increase.

Being at the forefront of advancing the country's EU integration, the Ministry of Foreign Affairs (MFA) of the Republic of Moldova faces a rapidly evolving threat landscape shaped by geopolitical tensions and regional security situation, marked by increasing number of hybrid threats, and the increasing digitalization of diplomacy. As Moldova advances on its path toward EU integration, the security of its diplomatic communications, institutional resilience, and crisis response capabilities have become matters of national security.

The MFA faces deeply embedded vulnerabilities in its digital security and crisis management capabilities. The Ministry's role in advancing national interests, coupled with its responsibility to manage sensitive diplomatic communications, requires a more robust and adaptive system that goes beyond basic cybersecurity improvements. Last years cyberattacks, particularly those before the European Political Community Summit in 2023, have revealed critical weaknesses in the national authorities' infrastructure.

Thus, UNDP is implementing the Enhancing Crisis Management and Cybersecurity Resilience of the Ministry of Foreign Affairs of the Republic of Moldova (MFA Support) Project, which aims at strengthening the long-term institutional resilience of the MFA by modernizing its crisis management system and bolstering its cybersecurity capabilities. As a result, the MFA becomes more effective, accountable, and resilient institution, equipped to manage crises and safeguard its critical operations.

To effectively address these issues, the project will adopt a three-pronged approach: policy review/process optimization, infrastructure enhancement and capacity-building. This approach will prioritize enhancing the MFA's dedicated crisis management spaces, including utility networks such as water, sewage, electricity, ventilation, and fire protection for the MFA offices for encrypted communication, archives, and crisis management team premises. It should also focus on modernizing cybersecurity protocols and the technology stack, while fostering a culture of gender-responsive crisis preparedness and collaboration, both internally and with external partners. Furthermore, the enhanced capabilities will be essential for the adoption at the institutional level of the requirements introduced by the new Crisis Management Law.

To achieve this, the project will focus on three strategic pillars:

1. **Strengthening Crisis Management and Cybersecurity Policy Frameworks**: This involves revising existing policies to ensure they are adaptive to evolving threats and give due consideration to gender dimension. Clear roles and responsibilities will be defined for crisis response, and EU-aligned cybersecurity and gender-responsive crisis management standards will be integrated into the MFA's operations, including in its missions abroad, ensuring consistency and coherence in both policy and implementation throughout the entire structure. Support will be provided in conducting risk assessment and drafting institutional/sectorial crisis management plan, as needed.
2. **Modernizing Crisis Management Infrastructure**: The MFA's infrastructure, including crisis management spaces, utility networks, and secure communication systems, will be upgraded to meet modern security standards. This includes enhancing physical spaces to ensure continuity of operations during emergencies and improving IT systems to protect against cyber threats.
3. **Expanding Operational and Human Capacities**: Modern technologies will be introduced to optimize processes and enhance crisis response capabilities. Comprehensive professional development programs will train MFA staff in best practices for cybersecurity and crisis management, ensuring long-term institutional capacity. Special attention will be given to gender-responsive prevention and risk assessment strategies, equipping staff with the skills necessary to proactively identify threats and mitigate risks before they escalate into crises. Moreover, exchanges with peer institutions from EU member states will be sought to strengthen cooperation and knowledge transfer.

The objective is not only to enhance processes but also to shift the institutional culture towards prioritizing security and preparedness, including from a gender perspective. As staff experience the practical benefits of these new systems, this mindset is likely to spread organically throughout the institution, ultimately strengthening the MFA's long-term resilience against cyber threats and crises.

The specific needs of women will be a key priority in a context where women face heightened risks in cyberspace, are often underrepresented and perceived as playing a marginal role in cybersecurity. Thus, the project will actively address possible gender imbalances or influences by identifying barriers that hinder women's participation in the field and challenging stereotypes that limit women's roles in the sector. Additionally, efforts will be made to ensure that Project activities engage both men and women and reflect balance and inclusion.

The development challenge, lies in transforming the MFA into a resilient, digitally secure institution capable of safeguarding national interests, protecting sensitive diplomatic data, and responding swiftly and effectively to crises, including from a gender-responsive perspective. This transformation must be aligned with EU standards and best practices, ensuring that Moldova's foreign policy apparatus is equipped to navigate the complexities of modern diplomacy and hybrid threats, including international crisis situations affecting Moldovan citizens abroad.

Considering the various difficulties the MFA faces in strengthening its cyber resilience, including limited understanding of cyber vulnerabilities the institution is dealing with, insufficient and outdated hardware and software to underpin a solid response to a cyber threat, and limited cybersecurity skills, targeted assistance will be provided to support the MFA in strengthening the institution's cybersecurity resilience and putting in place cybersecurity solutions and tools to safeguard critical data flows and operations.

B. Objectives of the assignment

The objective of the assessment is to provide the MFA with a comprehensive understanding of the current state, maturity, resilience, and operational effectiveness of its ICT, cybersecurity, crisis management, and information security environment, including related infrastructure, technologies, governance arrangements, regulatory and procedural frameworks, institutional capabilities, and operational practices, while directly supporting the fortification of the Ministry's cybersecurity capabilities and institutional crisis response posture through clear recommendations and strategic directions, where required.

The scope of work of the Service Provider under the current assignment is to contribute to strengthen the institutional and technological cybersecurity resilience of the Ministry of Foreign Affairs (MFA). This will be achieved by evaluating existing ICT and security processes, defining comprehensive technical requirements for advanced security and automation tools, and designing a robust Information Security Management System (ISMS) to ensure full compliance with GD No. 562/2025 and readiness for ISO/IEC 27001 certification.

To achieve the general objective, the Consultant shall fulfil the following specific objectives:

Objective 1: Evaluate ICT and Cybersecurity Process Maturity

To conduct a comprehensive maturity and gap analysis of the MFA's operational ICT and cybersecurity workflows against international frameworks (COBIT, ITIL), ISO/IEC 27001 control objectives, GD No. 562/2025, and other relevant requirements, establishing a clear remediation roadmap for process optimization.

Objective 2: Analyse e-Consulat Artifacts and Formulate Advanced Security Audit Requirements

To review the architecture, documentation, and development artifacts of the critical e-Consulat system, and to formulate production-ready technical specifications for a subsequent independent security assessment, explicitly defining criteria for application security testing (SAST/DAST/SCA) and penetration testing.

Objective 3: Architect Technical Requirements for Advanced Security and Automation Infrastructure

To define detailed functional, technical, and structural requirements for a tiered Log Management System (LMS) and SIEM architecture, an AI/ML-powered network threat detection platform, and specialized ICT process automation tools based on detailed needs assessment.

Objective 4: Establish and Operationalize the ISMS Governance Framework

To design and deploy a formal Information Security Management System (ISMS) aligned with ISO/IEC 27001 and GD No. 562/2025, encompassing the definition of scope, drafting of core security policies, establishment of an ISO/IEC 27005 risk management methodology, and the formal alignment of internal regulations and job descriptions.

Objective 5: Ensure Certification Readiness and Provide External Audit Support

To validate the operational effectiveness of newly implemented controls through a formal pre-certification internal audit (gap analysis), and to provide continuous expert technical and operational support to the MFA during the formal external certification audit, including the development and implementation of post-audit corrective action plans.

Objective 6: Enhance Institutional Competencies through Active Capacity Building and Knowledge Transfer

To provide direct support in elevating the competencies of the responsible MFA personnel through tailored training sessions, practical operational guidance, and structured knowledge transfer, ensuring the internal team is fully equipped to independently run, manage, and sustain the newly established ICT processes, governance frameworks, and security technologies.

To achieve the above-mentioned scope, the following specific tasks shall be carried out by the Service Provider. Throughout the process the Service Provider shall ensure technical advice to the MFA designated representatives as well actively engage with stakeholders (MFA representatives, UNDP representatives, and other related parties, including E-Governance Agency, STISC, Cybersecurity Agency, and others, when required and applicable).

Phase 1: Cybersecurity Operational Process Evaluation & Critical Systems assessment

Activity 1.1: Kick-off and Context Baseline Assessment

- Conduct initial stakeholder workshops to understand existing security assessment findings (limited to project scope).
- Define the exact boundary and scope for the process evaluation, covering both MFA and external infrastructure (diplomatic missions).

Activity 1.2: ICT and Security Process Maturity Analysis

- Evaluate existing ICT operational and security workflows against ISO/IEC 27001 controls, ISO/IEC 27005, ISO 22301, ISO 22361, GD 562/2025[1], (EU) 2022/2555 (NIS2 Directive), (EU) 2022/2557 (CER Directive), and relevant ICT management frameworks (ex. ITIL, COBIT) requirements.
- Identify operational and technological bottlenecks preventing the transition from a reactive to a proactive security posture.

Activity 1.3: Gap Analysis and Remediation Roadmap

- Identify operational gaps between current MFA processes and COBIT/ITIL/ISO 27001, ISO 22301, ISO 22361, GD 562/2025, Directive (EU) 2022/2555 (NIS2), Directive (EU) 2022/2557 (CER) requirements/benchmarks.
- Formulate a comprehensive remediation strategy detailing the required process automation tools and the skills/training matrix needed to bridge the identified gaps.
- Review roles, responsibilities, and data protection mechanisms for handling critical personal data against ISO/IEC 27001 controls.

Activity 1.4: Delivery of Specialized Information Security Training and Capacity Building

- Design and deliver a dedicated training module for the designated Internal ISMS Auditor, focusing explicitly on the roles, statutory responsibilities, audit techniques, execution of mock internal audits, and compliance tracking methodologies.
- Conduct targeted risk management workshops for Critical Process and Asset Owners, focusing on the practical application of the information security risk management methodology, risk identification, asset valuation, and the implementation of risk treatment plans.
- Provide advanced practical guidance and specialized coaching for the Head of the ICT Department (DTI) and the Information Security Officer, covering the operational aspects of daily ISMS maintenance, metrics tracking, incident reporting lines, and long-term framework sustainability.

Activity 1.5: Define requirements for comprehensive Security Audit of the e-Consulat System

- Review and analyse all available e-Consulat system documentation, including functional and non-functional requirements, architecture designs, High-Level Design (HLD) documents, and system administration guides.

[1] https://www.legis.md/cautare/getResults?doc_id=150574&lang=ro#

- Evaluate the platform's implementation process and developer-delivered artifacts, including Quality Assurance (QA) documentation, test execution reports, and User Acceptance Testing (UAT) results, to identify procedural security baselines.
- Define technical and operational requirements for Static Application Security Testing (SAST) on the source code and Software Composition Analysis (SCA) to identify structural flaws and open-source dependency vulnerabilities.
- Define scope and technical criteria for Dynamic Application Security Testing (DAST) on the dedicated environment and targeted Penetration Testing exercises designed to validate external perimeter resilience and simulate real-world exploit scenarios.
- Consolidate all defined requirements into a production-ready Technical Specifications package to facilitate the subsequent public procurement of the independent security audit services.

Phase 2: Technical Requirements Definition for Specialized Security Tools

Activity 2.1: Log Management & SIEM Architecture Requirements Definition

- Assess all critical log sources across MFA and external system's infrastructure to define log ingestion (integration) scope.
- Develop technical specifications for a centralized SIEM and Log Management System solutions, explicitly covering at least:
  - Centralized event collection, storage architectures, and compliance-driven retention periods.
  - Real-time log correlation rules and security incident detection use-cases.
  - Automated alerting/notification mechanisms and digital forensics/audit trail support.
  - Log transmission integrity and data protection/anti-tampering mechanisms.

Activity 2.2: Technical Requirements Definition for Specialized Security and Automation Tools

- Define structural and functional requirements for an AI/ML-powered network threat detection platform (Darktrace equivalent).
- Draft technical criteria for network and user anomaly detection, including the capability to flag zero-day attacks.
- Specify parameters for automated response mechanisms designed to contain incidents in real-time without disrupting diplomatic operations.
- Define usage scenarios, specific technical criteria, and operational parameters for ICT and security automation tools integrated with MFA infrastructure and components (covering at least: incident management, service request management, change management, access management, and risk management workflows).
- Develop automation (implementation) scenarios for identified (required) tools and system, including process and technological dependencies, explicitly focusing on the automated integration between security alerts (SIEM/AI) and ICT operational workflows (Incident and Access Management).

Activity 2.3: Formulation of Procurement requirements and development of Technical Specifications

- Consolidate all requirements from Activities 2.1 & 2.2 into a comprehensive technical specification's documents suitable for public tendering.
- Conduct market research to identify viable technical solutions and available vendors within the Republic of Moldova (RM) market, and define potential budgetary requirements, and licensing models.

Activity 2.4: Business Continuity and Crisis Management Strategic Framework Definition

- Define the overarching strategy and implementation methodology for aligning the MFA's operational resilience with ISO 22301 (Business Continuity Management) and ISO 22361 (Crisis Management) best practices.
- Develop a high-level implementation roadmap that outlines the necessary phases, organizational structures, and resource allocations required for the future deployment of business continuity and crisis management capabilities.
- Establish strategic alignment between the core information security workflows (ISO/IEC 27001) and the business continuity/crisis management governance, ensuring a seamless escalation path from cybersecurity incidents to institutional crisis response.
- Identify and map critical operational disruption scenarios (including critical downtime for key systems like e-Consulat and diplomatic communication networks) to serve as the baseline for future Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) definitions.

Phase 3: ISMS Framework Design & Certification Readiness

Activity 3.1: ISMS Scope Definition and Policy Governance

- Define the formal boundaries of the Information Security Management System (ISMS) for the MFA, aligned with ISO/IEC 27001 and GD 562/2025.
- Develop and/or update (in pre-approved versions) all necessary information security policies and procedures aligned with ISO/IEC 27001 GD No. 562/2025, necessary for ISMS functioning and certification process.
- Consultative support in GD 562/2025 requirements implementation, including practical aspects controls of implementation.
- Establish a formal risk management methodology compliant with ISO 31000 / ISO/IEC 27005.
- Develop and document ISMS security baselines.
- Advise for alignment and adjustment of internal regulations (including departmental/subdivision mandates, internal operational rules, and individual job descriptions) to formally embed information security roles, authorities, and accountability.

Activity 3.2: Pre-Certification Gap Analysis (Internal Audit)

- Conduct a comprehensive follow-up evaluation against all applicable ISO/IEC 27001 and GD No. 562/2025 requirements to verify control adoption.
- Perform a mock internal audit to verify the operational effectiveness of the newly implemented ISMS controls and document remaining gaps.

Activity 3.3: Certification Audit Support and Post-Audit Remediation

- Provide comprehensive technical and operational support to the MFA throughout the formal external certification audit phase by:
  - Facilitating communication with external auditors and providing technical clarifications regarding the designed ISMS architecture and controls.
  - Assisting MFA personnel in explaining and demonstrating compliance with the established information security policies and baselines.
  - Developing and implementing immediate corrective actions to remedy any potential audit findings, deficiencies, or non-conformities identified by the certification body.

Other requirements:

1. Flag issues as they arise to UNDP MFA Support Team in the context of and proactively suggest remedial actions;
2. Notify the UNDP MFA Support Project Team on unresolved issues and provide recommendations for resolution;
3. Conduct weekly update meetings or ad-hoc discussions with UNDP MFA Support Project Team and MFA representatives.
4. Prepare one Final Report covering the overall assignment, implementation support provided, coordination activities, strategic advice delivered, and final recommendations.

** The responsibility for facilitating the consultation process for the purpose of completing the tasks outlined hereto will be borne primarily by the Service Provider. The Service Provider shall be responsible for preparing working materials and agendas and will be supported by the UNDP Project Team to ensure participation, communication, and coordination with invited stakeholders.*

*** The duration of the tasks to be provided under point 12 of section Objectives of the assignment of the ToR shall be of 3 months and is expected to require an engagement of 5 working days per month of a Service Provider team member.*

C. Key deliverables and tentative timetable

#	Key deliverables	Tentative deadline
1.	**Deliverable 1. Inception Report**, including the assessment methodology, workplan, and proposed structure of the Assessment Report (Phase 1). (submitted in Romanian and English languages).	By October 15, 2026
2.	**Activity 1.1 Kick-off and Context Baseline Assessment. Deliverable 1.1 Scope Definition Report.** Detailed work plan, stakeholder interview matrix, and the formalized boundaries/scope definition for the process evaluation across MFA and its diplomatic missions.	By October 19, 2026
3.	**Activity 1.2 ICT and Security Process Maturity Analysis. Deliverable 1.2. ICT and Cybersecurity Process Maturity Assessment Report.** Formal evaluation report of existing ICT and cybersecurity workflows against ISO/IEC 27001, ISO/IEC 27005, ISO 22301, ISO 22361, GD No. 562/2025. Includes a dedicated section on critical personal data protection mechanisms and organizational bottlenecks.	By October 28, 2026
4.	**Activity 1.3 Gap Analysis and Remediation Roadmap. Deliverable 1.3 Comprehensive Gap Analysis and Remediation Roadmap.** A structured gap analysis log mapping current practices against target benchmarks, a strategic roadmap for process optimization, an automation tools recommendations matrix, and a specialized skills/training matrix.	By November 5, 2026
5.	**Activity 1.4 Delivery of Specialized Information Security Training and Capacity Building. Deliverable 1.4. Specialized Training Material Kits and Issued Certificates:** Training agendas and materials (including sessions records and exercises). Official signed attendance sheets and formal individual training completion certificates issued to all participating MFA representatives.	By November 19, 2026
6.	**Activity 1.5. Define requirements for comprehensive Security Audit of the e-Consulat System. Deliverable 1.5. Technical Specifications Package for the e-Consulat Security Audit.** A production-ready to integrate UNDP tendering document defining the exact technical, operational, and compliance requirements for independent application security testing (SAST, DAST, SCA) and penetration testing of the e-Consulat platform.	By November 5, 2026
7.	**Activity 2.1. Log Management & SIEM Architecture Requirements Definition. Deliverable 2.1 Log Management & SIEM Architectural Requirements Document.** Detailed engineering requirements for the tiered Log Management System (LMS) and SIEM solutions, covering data ingestion scope, retention periods, real-time correlation use-cases, alerting mechanisms, and log integrity protection.	By November 16, 2026
8.	**Activity 2.2. Technical Requirements Definition for Specialized Security and Automation Tools. Deliverable 2.2. Specialized Security & Process Automation Tools Specifications:** Integrated Technical Specifications document for public UNDP tendering of all Phase 2 security tools, paired with a comprehensive RM market vendor analysis and cost/budgetary estimation report.	By November 19, 2026
9.	**Activity 2.3 Formulation of Procurement requirements and development of Technical Specifications. Deliverable 2.3. Consolidated Procurement Package and Market Research Report:** Integrated Technical Specifications document for public UNDP tendering of all Phase 2 security tools, paired with a comprehensive RM market vendor analysis and cost/budgetary estimation report.	By January 5, 2027
10.	**Activity 2.4. Business Continuity and Crisis Management Strategic Framework Definition. Deliverable 2.4. Business Continuity and Crisis Management Strategic Framework Assessment Report.** A high-level strategic alignment methodology and implementation roadmap for ISO 22301 and ISO 22361 frameworks, including critical disruption scenario	By January 5, 2027

	mapping, recovery objectives (RTO/RPO) guidelines, and incident escalation paths.	
11.	**Deliverable 2.5. Training needs assessment and draft Capacity Building Programme** for MFA personnel, based on Phase 1 assessments.	By November 15, 2026
12.	**Activity 3.1. ISMS Scope Definition and Policy Governance. Deliverable 3.1. ISMS Governance and Policy Manual.** Manual shall contain: - Formal ISMS Scope Statement; - comprehensive set of all necessary information security policies and procedures (aligned with ISO/IEC 27001, GD No. 562/2025), enough for certification and ISMS functioning; - Information Security Risk Management Methodology (ISO/IEC 27005 and ISO 31000); and - draft amendments for internal regulations, departmental mandates, and individual job descriptions.	By January 15, 2027
13.	**Activity 3.2. Pre-Certification Gap Analysis (Internal Audit). Deliverable 3.2. Pre-Certification Internal Audit Report.** Official mock internal audit report verifying the operational effectiveness of implemented controls, alongside a detailed Compliance Gaps Log listing outstanding actions required prior to the external certification audit.	By January 15, 2027
14.	**Activity 3.3 Certification Audit Support and Post-Audit Remediation. Deliverable 3.3. Certification Audit Support Log and Post-Audit Corrective Action Plan.** Documented log of technical clarifications provided during the external ISO/IEC 27001 audit and corrective actions realised to address findings or non-conformities raised by the external certification body to secure the final certificate. **Note: t**his deliverable can be considered accepted only after successful MFA certification according with ISO/IEC 27001 standard.	By May 20, 2027
15.	**Deliverable 4 Final Report** covering the overall assignment, implementation support provided, coordination activities, strategic advice delivered, and final recommendations.	By May 28, 2027

Note: *The timeline and sequencing of activities may be further refined during the inception phase and development of the assignment methodology, in coordination with UNDP and MFA. Such adjustments are not expected to affect the overall duration or end date of the assignment.*

Confidentiality statement

All data and information received from the UNDP, MFA for the purposes of this assignment are to be treated confidentially and only to be used for the execution of these Terms of Reference.

The Service Provider shall ensure that all experts engaged under the assignment comply with confidentiality and non-disclosure obligations. Where required, separate confidentiality or non-disclosure agreements may be signed between the Service Provider and the relevant institutions involved in the assignment.

The Service Provider may conduct interviews, consultations, workshops, and coordination meetings through online collaboration and video-conferencing tools (e.g. MS Teams, Zoom or similar), where appropriate and agreed with the parties involved.

Where online consultation or working sessions are recorded for documentation or reporting purposes, such recordings shall be treated as confidential, used strictly for assignment implementation purposes, and managed securely by the Service Provider. Upon completion and acceptance of the assignment deliverables, the Service Provider shall ensure the secure transfer or destruction of such recordings and related materials, unless otherwise agreed in writing with UNDP and MFA.

Remote activities shall not replace physical assessments or technical verification activities where physical presence is required due to cybersecurity, operational, or infrastructure-related considerations.

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 UNDP.

D. Institutional arrangements

The timeframe for the work of the Service Provider is tentatively planned through October 2026 – May 2027.
The Service Provider will work under the guidance of and in close cooperation with the UNDP Project Team and with the delegated representatives from the MFA for both substantive and administrative aspects of the assignment.
The Service Provider is expected to cooperate closely with the MFA management and delegated staffers from the MFA, E-Government Agency, Information Technology and Cyber Security Service, Cybersecurity Agency.
Deliverables shall be approved by the UNDP Project Manager.
The Service Provider shall follow the agreed time schedule and be accountable for the delivery of quality outputs to the Project Manager, who will approve contractor's deliverables.
All documentation related to deliverables shall be provided by the Service Provider in one (1) electronic copy using the standard software products (Microsoft Office Word, Excel, SPSS/STRATA, Access, and PowerPoint).
Before submission of final deliverables, the Service Provider will discuss the draft documents with the parties involved, so that the final products reflect their comments.

Language requirements
All documentation related to the assignment shall be in Romanian, whereas the final redaction of the Cybersecurity Readiness Assessment Report shall be provided in English.
The Service Provider shall ensure, if necessary, interpretation into Romanian and English during interviews, meetings, presentations, and briefings organised through telephone or online, as well as translation of assignment related documentation and deliverables into Romanian and/or English as specified at Section D. Key deliverables and tentative timetable.
Any translation, interpretation and proof-reading costs shall be listed separately in the financial proposal.

E. Company qualifications and resourcing requirements
The bidder shall provide sound argumentation of the proposal by demonstrating compliance with the ToR and the environment in which it will provide the services. The bidder shall include information on the volume of allocated resources to carry out the assignment.

A breakdown per working days allocated for each deliverable shall be submitted, clearly explaining the role of the team members involved in producing the deliverable. In this context, the Service Provider shall ensure a clear presentation of distribution of tasks and allocation of working days deemed necessary for engagement of Key staff.

The proposed team should consist of Key personnel mentioned below (none of additional staff will be admitted to the project)

Key personnel:

- Project Manager (Team Leader/ Information Security Governance Expert)
- ICT Infrastructure & Security Integration Architect
- Application Security Expert (Software Auditor)
- Business Continuity & Crisis Management Expert

Bidders should enclose a resume for Key personnel and separately for each person anticipated to be assigned to the project and should include specific information on the experience and roles.

Only Key staff, as per section 3. Management Structure and Key Personnel under the Technical Evaluation Criteria, will be subject to technical evaluation.
Bidders agree that the Key staff included into the bid will participate and will provide high quality outputs and expertise in the project at the level and duration specified unless agreement is provided in writing by the UNDP Project Team to allow substitutions. Descriptions of subcontractor Key staff members, if applicable, should follow the format utilized for the Bidder organization.

The resumes submitted for the Key project personnel should be detailed and comprehensive. Specifically, resumes 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;
- Contact information (name, title, organization, mailing address, phone, and email) of a minimum of three business references;
- Linguistic skills.

Bidders should describe, in detail, their previous corporate experience in similar assignments, if any. This section should include the corporate experience as well as the role of any subcontracted organization(s) indicated in the Bidder's proposal.

During the assignment, the Service Provider's team of experts should prove 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.
Should any changes be necessary in this regard, a formal request for the agreement of the UNDP MFA Support Project team to allow substitutions, shall be submitted.

UNDP may at any time request the withdrawal or replacement of any of the Service Provider personnel should non-performance happen. Replacement will be at the Service Provider expense.

Qualification Requirements for the Service Provider (Company)

The company should fulfill the following criteria:

- Legally registered entity or consortium of firms.
- At least five (5) years of experience in providing consultancy services related to the assessment of compliance and implementation of ICT and cyber security projects in Moldova (based on national legislation and international recognized standards for cybersecurity and ICT management); For JV/Consortium/Association, Lead company should meet requirement. Each consortium Partner should have at least three (3) years of the above indicated experience.
- At least three (3) contracts of similar nature and complexity, in providing consultancy services in Moldova related to the implementation of national and/or internationally recognized cybersecurity and/or information management standards and/or frameworks, over the last 5 years. (For JV/Consortium/Association, Lead company should meet requirement).; Valid certification related to information security management (ISO/IEC 27001 or equivalent), and other relevant to the assignment. For JV/Consortium/Association, Lead company should meet requirement.

Failure to comply with the above-mentioned minimum requirements may constitute a reason for disqualification.

Criteria for the evaluation of the management structure and key personal:
Project Manager (Team Leader/ Information Security Governance Expert)
- University degree in the field of Computer Science and/or Information Technologies, or another relevant technical sciences field.
- At least ten (10) years of professional experience in information security governance, risk management, and compliance evaluation of ISMS within public sector institutions or enterprise-level organizations.
- Proven professional experience dealing with cyber security governance, evaluation and implementation of ISMS, ICT infrastructure and cybersecurity systems within Moldovan state/governmental institutions in at least 4 (four) similar projects.
- Demonstrated experience in applying cybersecurity regulatory requirements, including the Republic of Moldova cybersecurity regulatory framework (GD No. 562/2025) and/or EU cybersecurity frameworks such as NIS2 and CER Directive.
- Experience as Project Manager/Team Leader in at least 3 (three) projects implemented within the last five (5) years, involving similar scope, and complexity to the assignment.
- Proven experience in working with international development organizations, in at least 2 (two) similar projects.
- Certifications in IT Audit (CISA), ICT Governance, Informational Security Management, ISO 27001 Lead implementer, or other relevant fields.
- Proficiency in Romanian and English (verbal and writing). Romanian is mandatory.

ICT Infrastructure & Security Integration Architect

- University degree in areas such as computer sciences, engineering, telecommunications or related fields.
- Minimum seven (7) years of experience in enterprise IT infrastructure design, cloud architecture and security engineering.
- Proven experience in implementation and/or provision consultancy/advisory services related to assessment of ICT and cyber security processes and tools and cloud-based infrastructures (at least 3 projects within the last five (5) years).
- Demonstrated experience in architecting telemetry data pipelines, centralized Log Management Systems (LMS), and SIEM solutions (including log correlation rules and retention strategy design).
- Proven experience in defining technical requirements for specialized security tools, including AI/ML-powered (EDR/XDR) network anomaly detection platforms (e.g., Darktrace or equivalents).
- Proven experience within the public sector in at least 3 (three) similar projects within the last five years.
- Certifications: Azure Solutions Architect Expert, Azure Security Engineer Associate (AZ-500), or vendor-neutral certifications such as CISSP (Certified Information Systems Security Professional) or Certified Cloud Security Professional (CCSP by ISC²), or similar.
- Proficiency in Romanian and English languages.

Application Security Expert (Software Auditor)

- University degree in IT management, Computer Sciences, computer engineering or other relevant discipline.
- Minimum 7 years of professional experience in, application security testing and implementing security mechanisms in complex systems or secure software architecture.
- Demonstrated experience (at least 3 track records within the last five years) supervising or assessment of complex software implementation processes (including documentation, QA/UAT, pen-test and software audit, specifically SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), and SCA (Software Composition Analysis).
- Proven experience within the last 5 (fuve) years in drafting technical specifications and tender documents for informational systems security audits and penetration testing.
- At least one of the following certifications: CSSLP (Certified Secure Software Lifecycle Professional), OSCP (Offensive Security Certified Professional), or equivalent application security certifications.
- Proficiency in Romanian and English languages.

Business Continuity & Crisis Management Expert

- University degree in areas such as computer sciences, engineering, telecommunications or related.
- Minimum 7 years of experience in business continuity planning and disaster recovery.
- Proven experience in developing business continuity and operational resilience strategies and related SOP, aligned with ISO 22301 and crisis management protocols aligned with ISO 22361. Experience in conducting Business Impact Analyses (BIA), mapping critical operational disruption scenarios, and guiding organizations in defining RTO (Recovery Time Objectives) and RPO (Recovery Point Objectives).
- Previous proven experience (at least 3 track records within the last five years) in similar projects within public sector institutions or enterprise-level organizations.
- Certifications: ISO 22301 Lead Implementer/Auditor, CBCP (Certified Business Continuity Professional), or equivalent professional crisis management credentials.
- Proficiency in Romanian and English (verbal and writing).

The bidder will provide support facilities to their team of experts (back-stopping) during the implementation of the contract.

Note that civil servants and other staff of the public administration, of the partner country or of international/regional organisations based in the country, shall only be approved to work as experts if well justified. The justification should be submitted with the tender and shall include information on the added value the expert will bring as well as Nonobjection letter from the employer.

Other requirements:

- Access to the MFA's information, systems, and infrastructure shall be granted exclusively to personnel identified in the Contractor's Technical Proposal and approved in advance by the UNDP and MFA.
- The Contractor shall submit to the UNDP and MFA a complete list identifying all personnel involved in the execution of the Contract, including any additional personnel and subcontractors who may have access to the MFA's information, systems, or infrastructure.

- Any changes to the composition of the project team during Contract implementation shall be subject to the prior written approval of the UNDP and MFA.
- All personnel who will have access to sensitive or non-public information shall, where required by the MFA, provide a valid criminal record certificate (or equivalent certificate of no criminal convictions) and shall sign confidentiality and information protection undertakings before being granted such access.
- Access rights shall be granted strictly on a need-to-know basis and in accordance with the principle of least privilege, ensuring that each member of the Contractor's personnel has access only to the information and systems necessary to perform their assigned duties.

F. Schedule of Payments

The payments to the Company shall be made upon approval and acceptance of the deliverables by the UNDP project team.

SECTION 6: CONDITIONS OF CONTRACT AND CONTRACT FORMS

6.1 The types of Contract to be signed and the **applicable UNDP Contract General Terms and Conditions**, as specified in Data Sheet, can be accessed at http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html

SECTION 7: PROPOSAL FORMS

Form A: Proposal Confirmation

Form B: Checklist

Form C: Technical Proposal Submission

Form D: Proposer Information

Form E: Joint Venture/Consortium/Association Information

Form F: Eligibility and Qualification

Form G: Format for Technical Proposal

Form H: Format for CV of Proposed Key Personnel

Form I: Statement of Exclusivity and Availability

Form J: Financial Proposal Submission *[Form J is part of the Financial Proposal and shall be submitted directly in the system only in the "Commercial section" of the requirements. Please, ensure that no other documents are disclosing your financial proposal apart from Forms J and K. Non-compliance with this instruction may result in rejection of the proposal received.]*

Form K: Format for Financial Proposal *[Forms K is part of the Financial Proposal and shall be submitted directly in the system only in the "Commercial section" of the requirements. Please, ensure that no other documents are disclosing your financial proposal apart from Forms J and K. Non-compliance with this instruction may result in rejection of the proposal received.]*

FORM A: PROPOSAL CONFIRMATION

Please acknowledge receipt of this RFP by completing this form and returning it by email to the address, and by the date specified, in the Letter of Invitation.

To:	Insert name of contact person	Email: Insert contact person's email - do not enter secure proposal email address
From:	Insert name of proposer	
Subject	**RfP26/03336: Company to conduct a Cybersecurity Readiness Assessment of the Ministry of Foreign Affairs and prepare a Roadmap for modernization**	

Check the appropriate box	Description
☐	**YES**, we intend to submit a proposal.
☐	**NO**, we are unable to submit a competitive proposal for the requested services at the moment

If you selected NO above, please state the reason(s) below:

Check applicable	Description
☐	The requested services are not within our range of supply
☐	We are unable to submit a competitive proposal for the requested services at the moment
☐	The requested services are not available at the moment
☐	We cannot meet the requested terms of reference
☐	The information provided for proposal purposes is insufficient
☐	Your RFP is too complicated
☐	Insufficient time is allowed to prepare a proposal
☐	We cannot meet the delivery requirements
☐	We cannot adhere to your terms and conditions e.g. payment terms, request for performance security, etc. Please provide details below.
☐	Sustainability criteria/requirements are too stringent (if applicable)
☐	We do not export
☐	We do not sell to the UN
☐	Your requirement is too small
☐	Our capacity is currently full
☐	We are closed during the holiday season
☐	We had to give priority to other clients' requests
☐	The person handling proposals is away from the office
☐	Other (please provide reasons below):
Further information: Click or tap here to enter text.	
☐	We would like to receive future RFPs for this type of services
☐	We don't want to receive RFPs for this type of services

Questions to the Supplier concerning the reasons for no proposal should be addressed to Click or tap here to enter text. phone Click or tap here to enter number., email Click or tap here to enter text..

FORM B: CHECKLIST

This form serves as a checklist for preparation of your Proposal. Please complete the returnable Proposal Forms in accordance with the instructions and return them as part of your Proposal submission: No alteration to the format of forms shall be permitted and no substitution shall be accepted.

Before submitting your Proposal, please ensure compliance with the instructions in Section 2: Instructions to Proposers and Section 3: Data Sheet.

Technical Proposal:

Have you duly completed all the Returnable Proposal Forms?	
▪ Form C: Technical Proposal Submission	☐
▪ Form D: Proposer information	☐
▪ Form E: Joint Venture/Consortium/Association Information	☐
▪ Form F: Eligibility and Qualification	☐
▪ Form G: Technical Proposal	☐
▪ Form H: CVs of proposed key personnel	☐
▪ Form I: Statements of exclusivity and availability for key personnel	☐
Have you provided the required documents to establish compliance with the evaluation criteria in Section 4?	☐
Have you provided the required documents in support of Form D: Proposer Information?	☐

Financial Proposal:

▪ Form J: Financial Proposal Submission	☐
▪ Form K: Financial Proposal	☐

Forms J and K, representing the Financial Proposal shall be submitted directly in the system only in the "Commercial section" of the requirements. Please, ensure that no other documents are disclosing your financial proposal apart from Forms J and K. Non-compliance with this instruction may result in rejection of the proposal received.

FORM C: TECHNICAL PROPOSAL SUBMISSION

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	**RfP26/03336: Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**		

We, the undersigned, offer to supply the services required for Click or tap here to enter text.in accordance with your Request for Proposals No. Click or tap here to enter text.. We hereby submit our Proposal, which includes this Technical Proposal and our Financial Proposal uploaded separately under the commercial section in the system as instructed.

Proposer Declaration: on behalf of our firm, its affiliates, subsidiaries, and employees, including any JV / Consortium / Association members or subcontractors or suppliers for any part of the contract.

Yes	No	
☐	☐	**Requirements and Terms and Conditions:** I/We have read and fully understand the RFP, including the RFP Information and Data Sheet, Terms of Reference, the General Conditions of Contract and any Special Conditions of Contract. I/we confirm that the proposer agrees to be bound by them.
☐	☐	I/We confirm that the proposer has the necessary capacity, capability and necessary licenses to fully meet or exceed the requirements and will be available to deliver throughout the relevant contract period.
☐	☐	**Ethics**: In submitting this proposal I/we warrant that the proposer: has not entered into any improper, illegal, collusive or anti-competitive arrangements with any competitor; has not directly or indirectly approached any representative of the buyer (other than the point of contact) to lobby or solicit information in relation to the RFP; has not attempted to influence, or provide any form of personal inducement, reward or benefit to any representative of the buyer.
☐	☐	I/We confirm to undertake not to engage in proscribed practices, or any other unethical practice, with the UN or any other party, and to conduct business in a manner that averts any financial, operational, reputational or other undue risk to the UN and we have read the United Nations Supplier Code of Conduct :https://www.un.org/Depts/ptd/about-us/un-supplier-code-conduct and acknowledge that it provides the minimum standards expected of suppliers to the UN.
☐	☐	**Conflict of interest:** I/We warrant that the proposer has no actual, potential or perceived conflict of Interest in submitting this proposal, or entering into a contract to deliver the requirements. Where a conflict of interest arises during the RFP process the proposer will report it immediately to the Procuring Organisation's Point of Contact.
☐	☐	**Prohibitions and Sanctions:** I/We hereby declare that our firm, ultimate beneficial owners, affiliates or subsidiaries or employees, including any JV/Consortium members or subcontractors or suppliers for any part of the contract is not under procurement prohibition by the United Nations, including but not limited to prohibitions derived from the Compendium of United Nations Security Council Sanctions Lists and have not been suspended, debarred, sanctioned or otherwise identified as ineligible by any UN Organization or the World Bank Group or any other international Organization.
☐	☐	I/We do not employ, or anticipate employing, any person(s) who is, or has been a UN staff member within the last year, if said UN staff member has or had prior professional dealings with our firm in his/her capacity as UN staff member within the last three years of service with the UN (in accordance with UN post-employment restrictions published in ST/SGB/2006/15);
☐	☐	**Bankruptcy**: I/We have not declared bankruptcy, are not involved in bankruptcy or receivership proceedings, and there is no judgment or pending legal action against us that could impair our operations in the foreseeable future.
☐	☐	**Proposal Validity Period:** I/We confirm that this Proposal, including the price, remains open for acceptance for the proposal validity period.
☐	☐	I/We understand and recognize that you are not bound to accept any proposal you receive.
☐	☐	By signing this declaration, the signatory below represents, warrants and agrees that he/she has been authorised by the Organisation/s to make this declaration on its/their behalf.

Name: _____

Title: _____

Date: _____

Signature: _____

[*Stamp with official stamp of the Proposer*]

FORM D: PROPOSER INFORMATION

RFP Reference	**RfP26/03336: Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**
Legal name of Proposer	Click or tap here to enter text.
Legal Address, City, Country	Click or tap here to enter text.
Website	Click or tap here to enter text.
Year of registration	Click or tap here to enter text.
Proposer's Authorized Representative information	Name and Title: Click or tap here to enter text. Telephone numbers: Click or tap here to enter text. Email: Click or tap here to enter text.
Legal structure	Choose an item.
No. of full-time employees	Click or tap here to enter number.
No. of staff involved in similar contracts	Click or tap here to enter number.
Are you a UNGM registered vendor?	☐ Yes ☐ No If yes, insert UNGM Vendor Number
Years of supplying to UN organisations	Click or tap here to enter text.
Are you a Click or tap here to enter text.**vendor?**	☐ Yes ☐ No If yes, insert Vendor Number
Countries of operation	Click or tap here to enter text.
Subsidiaries in the region (please indicate names of subsidiaries and addresses, if relevant to the proposal)	Click or tap here to enter text.
Commercial Representatives in the country: Name/Address/Phone (for international companies only)	Click or tap here to enter text.
Quality Assurance Certification (e.g. ISO 9000 or Equivalent) *(If yes, provide a Copy of the valid Certificate):*	Click or tap here to enter text.
Does your Company have a corporate environmental policy or environmental management system/accreditation such as ISO 14001 or ISO 14064 or equivalent? *(If yes, provide a Copy of the valid Certificate):*	Tick all that apply and **provide supporting documentation**: ☐ Corporate Environmental Policy ☐ ISO 14001 ☐ ISO 14064 ☐ Other, specify Click or tap here to enter text.
Does your organization demonstrate significant commitment to sustainability, including the following aspects that have	Attach a formal statement that outlines your organisation's commitment to sustainability, where possible providing evidence of tangible results that demonstrate progress such as:

been identified in the UN Sustainable Procurement Framework? • Environmental: prevention of pollution, sustainable resources; climate change and mitigation and the protection of the environment, biodiversity. • Social: human rights and labour issues, gender equality, sustainable consumption, and social health and wellbeing. • Economic: whole life cycle costing, local communities and small or medium enterprises, and supply chain sustainability.	Tick all that are attached: ☐ Formal statement ☐ Sustainability report ☐ UN Global Compact Communication on Progress ☐ Other, specify Click or tap here to enter text.
Does your company belong to a diverse supplier group including micro, small or medium sized enterprise, women or youth owned business or other? *(If yes, please provide details and documentation]*	Click or tap here to enter text.
Is your company a member of the UN Global Compact?	Choose an item. If yes, please provide link to Global Compact profile: Click or tap here to enter text.
Bank Information	Bank Name: Click or tap here to enter text. Bank Address: Click or tap here to enter text. IBAN: Click or tap here to enter text. SWIFT/BIC: Click or tap here to enter text. Account Currency: Click or tap here to enter text. Bank Account Number: Click or tap here to enter text.
Contact person that Click or tap here to enter text. **may contact for requests for clarifications during Proposal evaluation**	Name and Title: Click or tap here to enter text. Telephone numbers: Click or tap here to enter text. Email: Click or tap here to enter text.

FORM E: JOINT VENTURE/CONSORTIUM/ASSOCIATION INFORMATION

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	**RfP26/03336: Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**		

To be completed and returned with your Proposal if the Proposal is submitted as a Joint Venture/Consortium/Association.

No	**Name of Partner and contact information** *(address, telephone numbers, fax numbers, e-mail address)*	**Proposed proportion of responsibilities (in %) and type of services to be performed**
1	Click or tap here to enter text.	Click or tap here to enter text.
2	Click or tap here to enter text.	Click or tap here to enter text.
3	Click or tap here to enter text.	Click or tap here to enter text.

Name of leading partner (with authority to bind the JV, Consortium, Association during the RFP process and, in the event a Contract is awarded, during contract execution)	Click or tap here to enter text.

We have attached a copy of the below referenced document signed by every partner, which details the likely legal structure of and the confirmation of joint and severable liability of the members of the said joint venture:

☐ Letter of intent to form a joint venture ***OR*** ☐ JV/Consortium/Association agreement

We hereby confirm that if the contract is awarded, all parties of the Joint Venture/Consortium/Association shall be jointly and severally liable to Click or tap here to enter text for the fulfilment of the provisions of the Contract.

Name of partner: _____

Signature: _____

Date: _____

Name of partner: _____

Signature: _____

Date: _____

Name of partner: _____

Signature: _____

Date: _____

Name of partner: _____

Signature: _____

Date: _____

FORM F: ELIGIBILITY AND QUALIFICATION

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	**RfP26/03336: Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**		

If JV/Consortium/Association, to be completed by each partner.

History of Non- Performing Contracts

☐No non-performing contracts during the last 3 years			
☐ Contract(s) not performed in the last 3 years			
Year	**Non- performed portion of contract**	**Contract Identification**	**Total Contract Amount** (current value in US$)
		Name of Client: Address of Client: Reason(s) for non-performance:	

Litigation History (including pending litigation)

☐ No litigation history for the last 5 years			
☐ Litigation History as indicated below			
Year of dispute	**Amount in dispute** (state currency)	**Contract Identification**	**Total Contract Amount** (state currency)
		Name of Client: Address of Client: Matter in dispute: Party who initiated the dispute: Status of dispute: Party awarded if resolved:	

Previous Relevant Experience

Please list only previous similar assignments successfully completed in the **last 5 years**.

List only those assignments for which the Proposer was legally contracted or sub-contracted by the Client as a company or was one of the Consortium/JV partners. Assignments completed by the Proposer's individual experts working privately or through other firms cannot be claimed as the relevant experience of the Proposer, or that of the Proposer's partners or sub-consultants, but can be claimed by the Experts themselves in their CVs. The Proposer should be prepared to substantiate the claimed experience by presenting copies of relevant documents and references if so requested.

Project name & Country of Assignment	**Client & Reference Contact Details**	**Contract Value** ***(please indicate the currency)***	**Period of activity and status**	**Types of activities undertaken and role (Contractor, sub-contractor or consortium member)**

Proposers may also attach their own Project Data Sheets with more details for assignments above.

☐ Attached are the Statements of Satisfactory Performance from the Top 3 (three) Clients or more.

Financial Standing

Annual Turnover for the last 3 years	**Year 2025**	Currency: USD	Amount
	Year 2024	Currency: USD	Amount
	Year 2023	Currency: USD	Amount
Latest Credit Rating (if any), indicate the source and date.			

Financial information (state currency)	**Historic information for the last 3 years**		
	2023	**2024**	**2025**
	Information from Balance Sheet		
Total Assets (TA)			
Total Liabilities (TL)			
Current Assets (CA)			
Current Liabilities (CL)			
	Information from Income Statement		
Total / Gross Revenue (TR)			
Profits Before Taxes (PBT)			
Net Profit			
Current Ratio (current assets/current liabilities)			

☐ Attached are copies of the audited financial statements (balance sheets, including all related notes, and income statements) for the years required above complying with the following condition:

a) Must reflect the financial situation of the Proposer or party to a JV, and not sister or parent companies;
b) Historic financial statements must be audited by a certified public accountant;
c) Historic financial statements must correspond to accounting periods already completed and audited. No statements for partial periods shall be accepted.

FORM G: FORMAT FOR TECHNICAL PROPOSAL

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	**RfP26/03336: Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**		

The proposer's proposal must be organised to follow the format of this Technical Proposal Form. Where the proposer is presented with a requirement or asked to use a specific approach, the proposer must not only state its acceptance, but also describe, where appropriate, how it intends to comply. Where a descriptive response is requested, failure to provide the same will be viewed as non-responsive.

Section 1: Proposer's qualification, capacity and expertise

1.1 Brief description of the organisation, including the year and country of incorporation, and types of activities undertaken.

1.2 General organizational capability which is likely to affect implementation: management structure, financial stability and project financing capacity, project management controls, extent to which any work would be subcontracted (if so, provide details).

1.3 Relevance of specialised knowledge and experience on similar engagements done in the region/country.

1.4 Quality assurance procedures and risk mitigation measures.

1.5 Organization's commitment to sustainability.

Section 2: Proposed Methodology, Approach and Implementation Plan

This section should demonstrate the proposer's responsiveness to the TOR by identifying the specific components proposed, addressing the requirements, providing a detailed description of the essential performance characteristics proposed and demonstrating how the proposed approach and methodology meets or exceeds the requirements. All important aspects should be addressed in sufficient detail and different components of the project should be adequately weighted relative to one another.

2.1 A detailed description of the approach, conceptual framework and methodology for how the Proposer will achieve or exceed the requirements of the Terms of Reference, keeping in mind the appropriateness to local conditions and project environment. Detail how the different service elements shall be organised, controlled and delivered.

2.2 A detailed description of the Bidder's internal technical and quality assurance mechanisms and risks identified, if any.

2.3 A detailed description of the System's technical functional and non-functional requirements.

2.4 Implementation plan including a Gantt chart or Project Schedule indicating the detailed sequence of activities that will be undertaken and their corresponding timing.

2.5 Any other comments or information regarding the project approach and methodology that will be adopted.

Section 3: Management Structure and Key Personnel

3.1 Describe the overall management approach toward planning and implementing the project. Include details of key personnel including their name and nationality, the Position they will assume and their role as per the ToR. Include an organisation chart for the management of the project describing the relationship of key positions and designations. Provide a spreadsheet to show the activities of each personnel and the time allocated for his/her involvement.

3.2 For each of the key personnel provide: the CV using the format in **Form H** and the statement of exclusivity and availability using the format in Form I. *Please provide copies of Certifications/Awards for the Key Personnel to be involved in the project.*

FORM H: FORMAT FOR CV OF PROPOSED KEY PERSONNEL

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	**RfP26/03336: Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**		

Position (as per ToR)		
Personnel Information	Name:	
	Nationality:	Date of birth:
	Language Proficiency:	
Present Employment	Name of employer:	Contact: (manager or HR)
	Address of employer:	
	Telephone:	Email:
	Job title:	Years with present employer:
Education / Qualifications	*Summarise college/university and other specialised education of personnel member, giving names of schools, dates attended, and degrees/qualifications obtained.*	
Professional Certifications	*Provide details of professional certifications relevant to the scope of services including name of institution and date of certification.*	
References:	*Provide names, addresses, phone and email contact information for two (2) references*.	

Summarise professional experience over the last 20 years in reverse chronological order. Indicate particular technical and managerial experience relevant to the project.

From	To	Company / Project / Position / Relevant technical and management experience

I, the undersigned, certify that, to the best of my knowledge and belief, this CV is accurate.

_____ _____

Signature of Personnel

Date (Day/Month/Year)

FORM I: STATEMENT OF EXCLUSIVITY AND AVAILABLITY

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	**RfP26/03336: Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**		

I, the undersigned, hereby declare that I agree to participate exclusively with the Proposer Click or tap here to enter text.in the above referenced RFP. I further declare that I am able and willing to work for the period(s) foreseen for the position for which my CV has been included in the event that this proposal is successful, namely:

From	**To**
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.

I confirm that I am not engaged in other projects in a position for which my services are required during the periods where my services are required under this RFP.

By making this declaration, I understand that I am not allowed to present myself as a candidate to any other proposer submitting a proposal for this RFP. I am fully aware that if I do so, I will be excluded from this RFP, the proposals may be rejected, and I may also be subject to exclusion from other UNDP's solicitation procedures and contracts.

Furthermore, should this proposal be successful, I am fully aware that if I am not available at the expected start date of my services for reasons other than ill-health or *force majeure*, I may be subject to exclusion from other Click or tap here to enter text. solicitation procedures and contracts and that the notification of award of contract to the Proposer may be rendered null and void.

Name: _____

Title: _____

Date: _____

Signature: _____

FORM J: FINANCIAL PROPOSAL SUBMISSION

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	**RfP26/03336: Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**		

We, the undersigned, offer to provide the services indicated in our proposal and in accordance with your Request for Proposal. We are hereby submitting our Financial Proposal in the amount indicated herewith.

Our Proposal shall be valid and remain binding upon us for the period of time specified in the Data Sheet.

We understand that you are not bound to accept any Proposal that you receive.

Our attached Financial Proposal is for the sum of *[Insert amount in words and figures]*. Please make sure the total matches with the total indicated in the deliverables section of the system (lines) and with the total deriving from the cost breakdown (form K).

FORM K: FORMAT FOR FINANCIAL PROPOSAL

Name of Proposer:	Click or tap here to enter text.	Date:	Click or tap to enter a date.
RFP reference:	**RfP26/03336: Cybersecurity Readiness Assessment and Roadmap for Modernization for the Ministry of Foreign Affairs**		

The proposer is required to prepare the Financial Proposal following the below format and submit it in an envelope separate from the Technical Proposal as indicated in the Instruction to Proposers. **The inclusion of any financial information in the Technical Proposal shall lead to disqualification of the Proposer.** The Financial Proposal should align with the requirements of the Terms of Reference and the proposer's Technical Proposal.

Currency of the proposal: MDL (Moldovan Leu) for local suppliers and USD (US Dollars) for international suppliers

Table 1 Financial Proposal:

Deliverable / Activity description	**Professional Fees**				**Other Costs**				**Total Amount per deliverable** (subtotal 1 + sub-total 2)
	Position	**Daily fee Rate**	**No. of Working Days**	**Total Amount**	**Description**	**Q-ty**	**Price**	**Total**	
Deliverable 1. Inception Report, including the assessment methodology, workplan, and proposed structure of the Assessment Report (Phase 1). (submitted in Romanian and English languages).	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
			Sub-total 1				**Sub-total 2**		

								Total:	
Activity 1.1 Kick-off and Context Baseline Assessment: Deliverable 1.1 Scope Definition Report. Detailed work plan, stakeholder interview matrix, and the formalized boundaries/scope definition for the process evaluation across MFA and its diplomatic missions.	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
			Sub-total 1				**Sub-total 2**		
								Total:	
Activity 1.2 ICT and Security Process Maturity Analysis: Deliverable 1.2. ICT and Cybersecurity Process Maturity Assessment Report. Formal Assessment Report of existing ICT and cybersecurity workflows against ISO/IEC 27001, ISO/IEC 27005, ISO 22301, ISO 22361, GD No. 562/2025. Includes a dedicated section on critical personal data protection mechanisms and organizational bottlenecks.	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
			Sub-total 1				**Sub-total 2**		
								Total:	
Activity 1.3 Gap Analysis and Remediation Roadmap: Deliverable 1.3	Project Manager (Team Leader/ Information				Travel (if any)				

Comprehensive Gap Analysis and Remediation Roadmap: A structured gap analysis log mapping current practices against target benchmarks, a strategic roadmap for process optimization, an automation tools recommendations matrix, and a specialized skills/training matrix.	Security Governance Expert)								
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
	Total:								
Activity 1.4 Delivery of Specialized Information Security Training and Capacity Building. Deliverable 1.4. Specialized Training Material Kits and Issued Certificates Training agendas and materials (including sessions records and exercises). Official signed attendance sheets and formal individual training completion certificates issued to all participating MFA representatives	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
	Total:								
Activity 1.5. Define requirements for comprehensive Security Audit of the e-Consulat System Deliverable 1.5. Technical Specifications Package for the e-Consulat Security Audit A production-ready to integrate UNDP tendering document defining the	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				

exact technical, operational, and compliance requirements for independent application security testing (SAST, DAST, SCA) and penetration testing of the e-Consulat platform.	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
	Total:								
Activity 2.1. Log Management & SIEM Architecture Requirements Definition Deliverable 2.1 Log Management & SIEM Architectural Requirements Document. Detailed engineering requirements for the tiered Log Management System (LMS) and SIEM solutions, covering data ingestion scope, retention periods, real-time correlation use-cases, alerting mechanisms, and log integrity protection.	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
	Total:								
Activity 2.2. Technical Requirements Definition for Specialized Security and Automation Tools Deliverable 2.2. Specialized Security & Process Automation Tools Specifications. Integrated Technical Specifications document for public UNDP tendering of all Phase 2 security tools, paired with a comprehensive RM market vendor analysis and cost/budgetary estimation report.	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				

		Sub-total 1				**Sub-total 2**			
								Total:	
Activity 2.3 Formulation of Procurement requirements and development of Technical Specifications **Deliverable 2.3. Consolidated Procurement Package and Market Research Report.** Integrated Technical Specifications document for public UNDP tendering of all Phase 2 security tools, paired with a comprehensive RM market vendor analysis and cost/budgetary estimation report.	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
								Total:	
Activity 2.4. Business Continuity and Crisis Management Strategic Framework Definition **Deliverable 2.4. Business Continuity and Crisis Management Strategic Framework Assessment Report.** A high-level strategic alignment methodology and implementation roadmap for ISO 22301 and ISO 22361 frameworks, including critical disruption scenario mapping, recovery objectives (RTO/RPO) guidelines, and incident escalation paths.	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
								Total:	

Deliverable 2.5 Training needs assessment and draft Capacity Building Programme for MFA personnel, based on Phase 1 assessments.	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
								Total:	
Activity 3.1. ISMS Scope Definition and Policy Governance **Deliverable 3.1. ISMS Governance and Policy Manual.** Manual shall contain: - Formal ISMS Scope Statement; - comprehensive set of all necessary information security policies and procedures (aligned with ISO/IEC 27001, GD No. 562/2025), enough for certification and ISMS functioning; - Information Security Risk Management Methodology (ISO/IEC 27005 and ISO 31000); and - draft amendments for internal regulations, departmental mandates, and individual job descriptions.	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
								Total:	
Activity 3.2. Pre-Certification Gap Analysis (Internal Audit).:	Project Manager (Team Leader/ Information				Travel (if any)				

Deliverable 3.2. Pre-Certification Internal Audit Report. Official mock internal audit report verifying the operational effectiveness of implemented controls, alongside a detailed Compliance Gaps Log listing outstanding actions required prior to the external certification audit.	Security Governance Expert)								
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
	Total:								
Activity 3.3 Certification Audit Support and Post-Audit Remediation. **Deliverable 3.3. Certification Audit Support Log and Post-Audit Corrective Action Plan.** Documented log of technical clarifications provided during the external ISO/IEC 27001 audit and corrective actions realised to address findings or non-conformities raised by the external certification body to secure the final certificate. **Note: t**his deliverable can be considered accepted only after successful MFA certification according with ISO/IEC 27001 standard.	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				
	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
	Total:								
Deliverable 4 Final Report covering the overall assignment, implementation support provided, coordination	Project Manager (Team Leader/ Information Security Governance Expert)				Travel (if any)				

activities, strategic advice delivered, and final recommendations.	ICT Infrastructure & Security Integration Architect				Local transportation costs (if any)				
	Application Security Expert (Software Auditor)				Communication Expenses				
	Business Continuity & Crisis Management Expert				Other costs (please specify)				
		Sub-total 1				**Sub-total 2**			
								Total:	
Total Amount of Financial Proposal (insert currency)									