NATO Communications and Information Agency

Acquisition Directorate
giordano.mastrocinque@ncia.nato.int

NCIA/ACQ/2025/06687
4 April 2025

To: All Prospective Bidders

Subject: **Request for Proposals (RFP) - RFP-CO-424219-PBN_0, Support to Protected Business Network (PBN) Capability Programme Implementation – Project 0, Discover and Accelerate**

References:
A. Notification of Intent (NOI) RFP-CO-424219-PBN_0 dated 9 January 2025
B. AC/4-D/2261 (1996 Edition), NSIP Procedures for International Competitive Bidding
C. AC/4-D/2261-ADD2(1996 EDITION)
D. AC/4-D(2008)0002-REV2
E. AC/4-D(2023)0012
F. AC/4(PP)D/28701-ADD1
G. AC/4-DS(2024)0039
H. AC/4-D(2024)0001 (INV), Review of NATO's Procurement Policy and Acquisition Process – Extensions to Bid Closing Dates Under International Competitive Bidding (ICB)

Dear Madam/Sir,

1. Following release by the NATO Communications and Information Agency (NCIA) of the NOI at Reference A; your Company is hereby invited to participate in this RFP for the Support to Protected Business Network (PBN) Implementation – Project 0 (*Discover and Accelerate*).
2. The intent of this RFP is to meet the objective of PBN Project 0 by selecting the Industry Service Integrator to whom the NCIA will award an Indefinite Delivery Indefinite Quantity (IDIQ) requirement-type contract. This Contract will allow the Industry Service Integrator to support implementation of the two subsequent projects (Project 1 – *Implement and Scale*; Project 2 – *Community of Interest Migration*)[1] for establishing the PBN capability. Upon PBN Project 1 and/or 2 approvals by the relevant NATO Committees and subject to funds availability; the awardee resulting from this competition will be called upon providing services described at Annex A (Statement of Work) to this RFP.
3. This RFP will be progressively adapted and refined by the NCIA in parallel with the conduct and completion of a number of evaluation and down-selection Steps that are foreseen to constitute the full extent of the competitive source selection process as described in Paragraph 8.
4. Only companies which qualify to the various down-select Steps will receive, through subsequent RFP amendments, additional details and information which are necessary to continue in the source-selection process, up to award.

[1] Detailed description of Projects # 1 and 2 scope is provided in the Annex A to this RFP.

5. This RFP uses a Best Value Competitive Dialogue evaluation methodology based on a 4 (four) Steps RFP response submission authorized per Reference G, hence, and only in this respect, it deviates from standard competition processes per References B and C. A graphical representation of the 4 (four) RFP Steps is provided below. The graphical representation is then followed by an elaboration for each Step, provided at Paragraphs 8.1 through 8.4 :

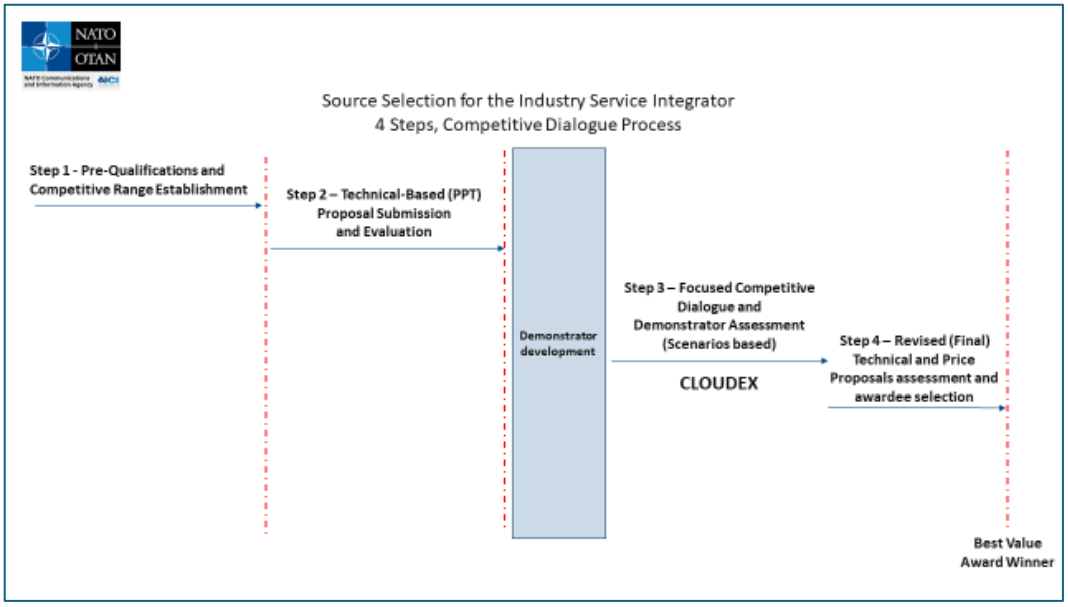

Figure 1: RFP 4 (four) Steps outsourcing strategy

6. Each RFP Step is aimed at progressively down-selecting to a lower number of companies' (hereinafter referred to as "Bidders") proposals based on the scoring of technical and - when applicable - pricing criteria that are established up front by the NCIA in the RFP per each single Step.

7. For the purpose of this RFP and in respect of the NCIA's Prime Contractor Principle (following which the Prime Contractor is solely liable for the overall execution and management of the Contract, including delivering the agreed upon outcomes, managing the project's scope, budget and schedule, and ensuring compliance with all contractual obligations):

   7.1. The Prime Contractor may subcontract certain tasks to other companies (see also Paragraph 12.2 below) but retains full liability for the project's success and for managing any issues that arise.

   7.2. Bidders are at liberty to constitute themselves into any form of contractual arrangements or legal entity they desire, bearing in mind that in consortium-type arrangements, a single judicial personality must be established to represent that legal entity and take on the role of Prime Contractor (see above). A legal entity, such as an individual, partnership or corporation (herein referred to as the "Contractor"), shall represent all members of the consortium with the NCIA. The Contractor shall be vested with full power and authority to act on behalf of all members of the consortium within the prescribed powers stated in an irrevocable Power of Attorney issued to the Contractor by all members associated with the consortium.

   7.3. Evidence of authority to act on behalf of the consortium by the Contractor shall be enclosed and sent with any Bidder's response to this RFP. Failure to furnish proof of authority may be a reason for the RFP response being declared non-compliant.

8. Here below follows a description of the 4 (four) Steps foreseen in this RFP:

8.1. **STEP 1 – Pre-Qualifications and Competitive Range Establishment (purpose: down-selection of up to 5 Bidders based on the pre-qualification methodology and criteria outlined hereinafter in this RFP).** Bidders shall note that Step 1 down-selection is informed by the content of this initial version of the RFP. Full detailed information on how and what to submit an RFP response for Step 1 down-selection is available as from Paragraph 12 herein.

8.2. **STEP 2 – Technical-Based Proposal Submission and Evaluation (applicable to the down-selected Bidders identified after Step 1 completion; purpose: further down-selection of up to 3 Bidders).**

8.2.1. Following the completion of Step 1 procedures; an RFP amendment will be distributed to the down-selected Bidders resulting from Step 1. The RFP amendment will provide detailed instructions and information, including evaluation criteria and methodology, to allow the up to the Step 1 down-selected Bidders to provide their response for the Step 2. A Bidders Conference[2] is intended for Step 2.

8.2.2. Besides the Bidders Conference foreseen at Step 2, the NCIA also plans to invite the Step 1 down-selected Bidders to one-on-one meeting sessions[2]. Purpose of these sessions will be to allow Bidders' demonstration of their understanding of NATO's migration to cloud strategy; to elaborate on their proposed methodology, approach and model (supported as required by demos of previously deployed services based on the NCIA use cases that will be provided in the RFP at Step 2). The details of this Step 2 included but not limited to timing and submission artefacts will be disclosed at a later date only to down-selected Bidders from Step 1.

8.2.3. Models proposed by the Bidders as from Step 2 shall enable the NCIA to exercise impartial and independent monitoring of Contractor's performance in respect of cybersecurity and IT Service Management (SM) services as well as to benefit of Contractor delivering performance agility in respect of Cloud Platform Engineering Services. The NCIA reserves the right, throughout the RFP process, to require measures from the Bidders in order to ensure the above mentioned independence and impartiality.

8.2.4. The RFP Step 2 will result in the down-selection of up to 3 Bidders. Each one of these 3 down-selected Bidders will be awarded a firm fixed price contract for not-to-exceed (NTE) MEUR 2.5. This intended award represents the NCIA financial contribution to each of the 3 down-selected Bidders for the development of a complete functioning demonstrator which will have to support the solutions submitted in response to RFP Step 2. Details about the demonstrator are provided in the following paragraphs.

8.3. **STEP 3 - Focused Competitive Dialogue and Demonstrator Assessment (applicable to the down-selected Bidders identified after Step 2 completion; purpose: competitive dialogue in preparation of Best and Final Offer (BAFO) submission at Step 4).**

8.3.1. Following the completion of Step 2 procedures; an RFP amendment will be distributed to the Step 2 down-selected Bidders. The RFP amendment will provide detailed instructions and information, including

[2] Written notifications and instructions will be distributed to eligible Bidders with location details and timeframes.

evaluation criteria and methodology, to allow the down-selected Bidders to provide their response for the Step 3.

8.3.2. Bidder's required response to Step 3 will include the submission of a demonstrator that the NCIA will be using to support the evaluation. The demonstrator will serve as proof of concept in respect of the solidity of each Bidder's proposals and its viability.

8.3.3. Each demonstrator will be put by the NCIA to the test in the context of an NCIA led exercise[3] (so-called "CLOUDEX"). This exercise will include simulation activities based on a pre-determined set of scenarios. The CLOUDEX will be an opportunity for clarifying areas that can be improved by each Bidder in preparation of Bidders' BAFO submissions at the following Step 4.

8.3.4. Furthermore at Step 3, Bidders will submit their proposed cost model and the prices applicable - in case of award - to deliver the services listed at Annex A to this RFP. A set of NCIA pre-defined Use Cases will be used by the NCIA to calculate the overall price applicable to each evaluated Bidder, based on each Bidder's proposed cost model and related proposed prices. Step 3 will also offer an opportunity to clarify pricing model and information in preparation of Bidders' BAFO submissions at the following Step 4.

8.3.5. Each Bidder will be evaluated by the NCIA based on the methodology and scoring applicable to Step 3 and then provisionally ranked.

8.4. **STEP 4 - Revised Proposals assessment and Final Selection (applicable to the down-selected Bidders identified after Step 2 completion; purpose: final proposals (BAFO) evaluation and award determinations).**

8.4.1. At Step 4 each Bidder will be allowed to formally submit a BAFO addressing technical and pricing clarifications discussed at the previous Step 3.

8.4.2. Using each Bidder's submitted BAFO; the NCIA will perform a final round of evaluation and scoring from both technical and pricing standpoints. In accordance with Reference G; the authorized top-level criteria applicable at the final Step 4 of the RFP evaluation process are: Technical (70%) and Price (30%).

8.4.3. At conclusion of the RFP Step 4, the NCIA will identify the Best Value awardee who, upon award, will cover the role of Industry Service Integrator supporting the implementation of the PBN capability.

9. Bidders shall note that the successful Bidder resulting from this RFP will be required to possess a NATO S3CRET security clearance to perform the prospective contract. This is due to the fact that the prospective contract resulting from this RFP will require Contractor's ability to handle and store classified material to the level of up to NATO S3CRET.

10. Accordingly, the awardee resulting from this RFP shall therefore have the appropriate facility and personnel clearances at the date of contract signature.

[3] Tentative duration: 1 week per each Bidder; tentative location: NCIA, The Hague (NLD). Written notifications and instructions will be distributed to eligible Bidders with confirmed location details and timeframes.

Bidders are advised that contract signature will not be delayed in order to allow the processing of NATO S3CRET security clearances for personnel and/or facilities and, should the otherwise successful Bidder not be in a position to accept the offered contract within 30 (thirty) calendar days due to the fact that its personnel and/or facilities do not possess the appropriate security clearance(s), the NCIA may determine the Bidder's proposal to be non-compliant as a whole and offer the contracts to the Bidder next-in-rank.

11. Contract Award is currently estimated for the 1st Quarter 2026. The NCIA intends to award to the selected Industry Service Integrator an Indefinite Delivery Indefinite Quantity (IDIQ), requirement-type framework contract. Bidders shall note that the intended contract will not generate neither any immediate financial obligation for the NCIA (the contract does not provide any minimum guaranteed) nor any immediate financial revenue for the Industry Service Integrator. However, it is envisaged that the intended framework contract will start producing financial benefits for the Industry Service Integrator once the NCIA would start tasking the Industry Service Integrator to deliver its services following formal approval by the relevant NATO Authorities of the subsequent PBN Projects 1 and 2 (as indicated at Paragraph 2 above) that are foreseen in the capability implementation plan. Based on the currently available initial assumptions and with no commitments from the NCIA's end; it is estimated that the value of the intended contract awarded to the Industry Service Integrator may result in a business opportunity of estimated EUR 200,000,000 over an estimated period of 7 years. However, this will depend on the future developments in respect of how the PBN Capability will be implemented through Projects 1 and 2, with the associated delineation of responsibilities between the NCIA and the external contracting partners.

12. **STEP 1: PRE-QUALIFICATION AND COMPETITIVE RANGE ESTABLISHMENT**

12.1. As a pre-qualifying step, Step 1 will be a down-select process (based on the assessment of past performance information) after which up to 5 (top ranking) down-selected Bidders will receive a notice of competitive viability allowing to progress to the next Step 2. Any Bidder not selected to proceed to Step 2 will not be considered for award nor receive further communication concerning this RFP besides the notification process foreseen at completion of Step 1 evaluation procedures in compliance with References B to E.

12.2. For the purpose of RFP Step 1 pre-qualification and competitive range establishment, Bidders are permitted to submit information related to contracts performed by the Bidder and/or up to 2 (two) sub-Contractor the Bidder proposes to use when performing the scope under competition through this RFP. In this case, Bidders shall submit in their RFP response a **formal joint statement or agreement**, signed by the Bidder and its 2 (two) proposed sub-Contractors confirming the Bidder, and its proposed sub-Contractors, irrevocably commit to maintaining the proposed cooperation arrangement, including related services/deliverables by the Prime Contractor or its sub-Contractors, throughout the entire RFP competition and in case of award throughout contract performance. This commitment is a prerequisite for the Bidder advancing to subsequent stages in the selection process. Bidders shall be allowed to propose additional sub-Contractors at a later stage of the competition, up to and until completion of the RFP process and, in case of award, throughout contract performance. Any cooperation construct proposed during the first stage (RFP Step 1) and throughout the entire competition shall be subject to NCIA's Prime Contractor Principle stated at Paragraph 7 of this RFP.

12.3. Bidders' assessment, ranking and down-selection for Step 1 will be based on the NCIA's assessment of the Power of Attorney (to be submitted by the Bidder

- if applicable - as per Paragraph 7 above) and of the information received in the Annexes B and C, as detailed below:

Annex B (Past Performance Questions):

12.4. Bidders shall address all Technical and Management questions provided in the Annex B to this RFP, and carefully follow instructions and guidelines provided in such Annex.

12.5. In the Annex B, Bidders shall refer to 3 (three) past performed contracts executed **within the last 6 (six) years from the date of issuance of this RFP and with a minimum of 12 (twelve) months performance period.** These referenced contracts must be similar or exceeding the scope and complexity of the requirements stated at Annex A to this RFP.

12.6. In addition, **at least 1 (one) of the 3 (three) past performance contracts referenced in the Annex B shall be where the Bidder itself (and not any of its proposed sub-Contractors) was a Prime Contractor**. For the remaining 2 (two) past performance contracts referenced in the Annex B, it will be allowed to make reference to contracts performed by the Bidder (and/or any Bidder's proposed sub-Contractor) as a significant teaming partner or a significant sub-Contractor. The NCIA considers a significant teaming partner or a significant sub-Contractor to be a company which is able to demonstrate having:

a) Provided 30% or more (based on the referenced contract monetary value) of the entire scope;

b) Provided a critical portion of the effort required such as: CloudOps activities, including cloud-enabled workplace and landing zone management, Enterprise service integration and transformation.

12.7. **Once completed by the Bidder**, the Annex B shall be signed by an authorized Bidder's representative and returned with all required supporting documentation to the NCIA at the email address provided at Paragraph 12.15. Prior to submission to the NCIA, Bidders shall ensure Annex B information includes the following:

12.7.1. **Mandatory:** an **executive summary** (maximum word count limit for the executive summary: 5,000 words) and **the answers to all technical and management questions** addressed in the Annex B (maximum overall word count limit for the totality of questions: 10,000 words). Bidders shall note that submission of graphical drawings, illustrations, diagrams will not account for the total number of words of the Annex B response. IMPORTANT NOTE: while submission of the executive summary is a mandatory requirement to achieve administrative compliance; information submitted by the Bidder in the executive summary will not be evaluated for the purpose of determining the Bidder's Overall Technical Score the NCIA will use for RFP Step 1 down-selection.

12.7.2. **If applicable:** a **formal joint statement or agreement** (reference Paragraph 12.2), signed by the Bidder and all of the Bidder's proposed sub-Contractors named in Annex B;

12.7.3. **Mandatory:** an **official attestation** to demonstrate the declared global annual revenue and the global annual revenue for public cloud IT transformation services, in response to Annex B, Question 1A;

12.7.4. **Mandatory:** copies of **certifications or links** to partner listings or evidence of advanced specializations or awards from Commercial Cloud Service Providers, in response to Annex B, Question 3B.

12.7.5. **Mandatory:** copies of **certifications** for continuous compliance to industry-recognized security certification and standards, in response to Annex B, Question 6A.

12.8. Bidders shall note that references to past performed contracts that do not fully meet the criteria stated at Paragraphs 12.5 and 12.6 will not be considered.

Annex C (Past Performance Package):

12.9. For each of the 3 referenced contracts indicated in the Annex B; Bidders shall request each relevant Bidder's (or Bidder's proposed sub-Contractor's) Customer to fill in and return to the NCIA the Past Performance Questionnaire (Annex C) following the instructions and guidelines provided in such document.

12.10. Technical and Management questions addressed in the Past Performance Questionnaire are intended to give evidence of Bidder's (and/or Bidder's proposed sub-Contractor's) successful past performance of previous contracts delivered for other Customers. The Annex C includes the following:

a) The Sample Consent Letter;

b) The Past Performance Questionnaire Rating Sheet; and

c) The Past Performance Questionnaire (Technical and Management questions).

12.11. **The Bidder's (and, whether applicable, the Bidder's proposed sub-Contractor's) Authorized Representative** shall fill in, sign and submit the Consent Letter to each Customer that was referenced in the Annex B. The purpose of the Consent Letter is to authorize release and submission, by the referenced Customer, of the past performance information directly to the NCIA.

12.12. Together with the Consent Letter; the Bidder shall send to each referenced Customer the Past Performance Questionnaire Rating Sheet as well as the Past Performance Questionnaire. These will allow each Customer referenced in the Annex B to conduct past performance assessment and to return the Past Performance Package (the signed Consent Letter, the Rating Sheet and the completed Past Performance Questionnaire) directly to the NCIA.

12.13. The Bidder shall not complete any section of the Past Performance Questionnaire **except SECTION I** as it is highlighted (in yellow) in the questionnaire. Once the questionnaire is completed by the Bidder's (or the Bidder's proposed sub-Contractor's) Customer, the information contained therein shall be considered Source Selection Information and it shall be sent **by the Bidder's (or the Bidder's proposed sub-Contractor's) Customer directly to the NCIA** using the email address provided at Paragraph 12.15.

RFP Step 1 response submission to the NCIA:

12.14. To summarize:

- The Bidder shall submit the **Power of Attorney**, if required, as per Paragraph 7 above;

- The Bidder shall submit **Annex B** (Technical and Management Questions) with all supporting documentation (listed at Paragraph 12.7) to the NCIA;

- The Bidder's (or the Bidder's proposed sub-Contractor's) Customer shall

directly submit to the NCIA the **Annex C** (Past Performance Package**)** once completed.

12.15. The email address to use for both Annex B and Annex C submissions is the following: **RFPCO424219PBN@ncia.nato.int**

IMPORTANT NOTE TO BIDDERS: It is the sole responsibility of the Bidder to ensure Bidder's (and/or Bidder's proposed sub-Contractor's) Customer submits the Past Performance Questionnaire assessment to the NCIA.

12.16. Files shall be submitted in PDF format only. The NCIA will not accept hard copies, CDs, thumb drives and/or zip files.

12.17. Emails submitted in response to this RFP shall be less than 10 MB in size per email with no encryption and/or password protection to the file. The individual electronic files sent by email shall have the naming convention listed in the table below. In the event the documents must be split into more than one file due to surpassing the 10 MB limit, the Bidder shall add "Part 1 of 2", "Part 2 of 2", etc. as necessary.

12.18. Failure to meet compliance verification by the NCIA with the RFP Step 1 bidding requirements stated in this RFP will be cause to determine the Bidder as not-compliant for Step 1 down-selection and **will preclude the Bidder from participating to the subsequent Steps foreseen for this RFP**.

12.19. The following table summarizes the required information to be submitted via email at: **RFPCO424219PBN@ncia.nato.int** and it also states who is the individual responsible for the submission to the NCIA:

Bidder's required content for RFP-CO-424219-PBN_0 - Step 1 response:		
Item	**Responsible for submission to NCIA**	**Description**
Power of Attorney (if applicable)	**Bidder**	As per Paragraph 7 above. **File Naming Convention:** RFP-CO-424219PBN-Bidder's Company Name-Step1-Power of Attorney
Annex B - Bidder's answers to Technical and Management questions	**Bidder**	One merged PDF document to include all supporting documents listed at Paragraph 12.7 of this RFP. Bidders shall also follow instructions provided in the Annex B to this RFP. **File Naming Convention:** RFP-CO-424219PBN-Bidder's Company Name-Step1-Annex B
Annex C - Past Performance Package • Consent Letter • Past Performance Questionnaire Rating Sheet • Past Performance Questionnaire	**Customer**	One merged PDF document including all documents listed at Paragraph 12.10. of this RFP. **File Naming Convention:** RFP-CO-424219PBN-Bidder's Company Name-Step1-Annex C

12.20. The closing date/time for the electronic submission of the RFP Step 1 response is: **Monday, 26 May 2025, 15:00 hours Central European Summer Time (CEST).**

12.21. Any Bidder's response to the RFP Step 1 received by the NCIA after the exact date and time indicated in Paragraph 12.20. above is "late" and may not be considered.

12.22. The Bidder is informed that requests for Closing Date extensions for RFP Step 1 shall be submitted to the Point of Contact indicated in Paragraph 17 below no later than fourteen 14 (fourteen) calendar days prior to the closing date and time established in this RFP. Requests for additional time, following the initial Bid Closing Date, may be granted subject to the provisions at Reference H.

12.23. The Bidder is informed that any request for clarification must be submitted to the NCIA as soon as possible. Such requests for clarification must be received by the NCIA no later than 28 (twenty-eight) calendar days prior to the closing date and time established in this RFP. The NCIA reserves the right to reject questions clearly devised or submitted for the purpose of artificially obtaining an extension of the solicitation time (i.e. questions re-submitted using different wording where such wording does not change the essence of the question being requested).

12.24. All Step 1 documentation shall be submitted in English.

12.25. Participating NATO nations (32) contributing to the project namely: Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, The Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Republic of Türkiye, The United Kingdom, and The United States.

12.26. All Contractors, subcontractors and manufacturers, at any tier, shall be from and operate from within Participating NATO Countries.

12.27. In the event of Step 1 response submissions received by the NCIA via email is unreadable to the degree that conformance to the essential requirements of this RFP cannot be ascertained, the NCIA Contracting Officer responsible for this RFP will immediately notify the Bidder that the Step 1 documents will be rejected unless the Bidder provides clear and convincing evidence:

a) of the content of the Step 1 documents as originally submitted; and,

b) that the unreadable condition of the Step 1 documents was caused by NCIA software or hardware error, malfunction, or other NCIA mishandling.

12.28. Step 1 documentation submitted that fails to conform to the above requirements may be declared non-compliant and may not be evaluated further by the NCIA.

12.29. **RFP Step 1 evaluation criteria and methodology:** please refer to Annex D to this RFP.

13. All correspondence pertaining to this RFP shall reference: RFP-CO-424219-PBN_0.

14. The overall security classification for this RFP is: NATO UNCLASSIFIED.

15. Recipients are requested to complete and return within seven (7) calendar days the Acknowledgement of Receipt at Attachment A.

16. Bidders are advised that NCIA reserves the right to cancel, withdraw or suspend this RFP process at any time in its entirety and bears no liability for costs incurred by Bidders or any other collateral costs if RFP cancellation occurs.

17. The Contracting Officer responsible for this RFP is Mr. Giordano Mastrocinque. All correspondence regarding this RFP shall solely be addressed to:

RFQCO424219PBN@ncia.nato.int

FOR THE CHIEF OF ACQUISITION:

[ORIGINAL SIGNED]

Giordano Mastrocinque
Senior Contracting Officer

Attachments:

A: Acknowledgement of Receipt of RFQ-CO-424219-PBN_0
B: List of Prospective Bidders

Annexes:

A: Statement of Work
B: Technical and Management questions
C: Past Performance Questionnaire Package
D: RFP Step 1 Evaluation criteria and methodology

NCIA/ACQ/2025/06687
4 April 2025

ATTACHMENT A

ACKNOWLEDGEMENT OF RECEIPT
RFQ-CO-424219-PBN_0

Please complete, sign and return by email (scanned to pdf) within 7 (seven) calendar days to:

RFQCO424219PBN@ncia.nato.int

We hereby advise that we have received the Request for Proposal (RFP) reference number RFP-CO-424219PBN_0 on ....., together with all the attachments.

PLEASE CHECK ONE

☐ As of this date and without commitment on our part we **do intend** to submit the required documentation as described in this RFP.

☐ We **do not intend** to participate in this RFP.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Address: _____

POC: _____

Tel.: _____

E-mail: _____

NCIA/ACQ/2025/06687
4 April 2025

ATTACHMENT B

LIST OF PROSPECTIVE BIDDERS

COMPANY NAME	COUNTRY
ACCENTURE	BEL
AIRBUS DEFENCE AND SPACE AS	NOR
AIRBUS DEFENCE AND SPACE SAS	FRA
ALITER TECHNOLOGIES, A.S.	SVK
AMAZON WEB SERVICES BELGIUM	BEL
ARICOMA SYSTEMS A.S.	CZE
ASELSAN ELEKTRONIK SANAYI VE TICARET A.S.	TUR
ATOS BELGIUM	BEL
ATOS FRANCE	FRA
BAE SYSTEMS AI LTD	GBR
BECHTLE GMBH & CO. KG	DEU
BOOZ ALLEN HAMILTON, INC.	USA
BREVCO SERVICES	BEL
BT GLOBAL SERVICES BELGIUM	BEL
CAPGEMINI TECHNOLOGY SERVICES	FRA
CGI DEUTSCHLAND B.V. & CO. KG	DEU
CISCO SYSTEMS BELGIUM	BEL
COMPUTACENTER	BEL
CS GROUP - FRANCE	FRA
CYBER STRATEGY CONSULTING INC.	CAN
CYPROS C	BEL
DARKTRACE HOLDINGS LIMITED	GBR
DELL	BEL
DELOITTE & TOUCHE LLP	USA
DELOITTE CANADA	CAN
DELOITTE CONSULTATIVE SERVICES B.V.	NLD
DELOITTE CONSULTING AND ADVISORY BV	BEL
DELOITTE LLP	GBR
DEUTSCHE TELEKOM GLOBAL BUSINESS SOLUTIONS BELGIUM	BEL
DIGIA FINLAND OY	FIN
DXC TECHNOLOGY B.V.	NLD
E-COMPASS	BEL
ENGINEERING - INGEGNERIA INFORMATICA S.P.A	ITA

ENTSERV UK LIMITED, T/A DXC TECHNOLOGY	GBR
ETME	GRC
EVIDEN BELGIUM	BEL
FORTE BILGI ILETISIM TEK. VE SA V. SAN. AS	TUR
FORTINET	BEL
FUJITSU SERVICES LIMITED	GBR
GMV AEROSPACE AND DEFENCE S.A.U. (A79197356)	ESP
HEWLETT-PACKARD ENTERPRISE BELGIUM	BEL
IBM BELGIUM	BEL
IBM UK LIMITED	GBR
INDRA SISTEMAS, S.A. (A28599033)	ESP
INDUSTRIA PROJECT SP. Z O. O.	POL
INDUSTRIEANLAGEN-BETRIEBSGESELLSCHAFT MBH (IABG MBH)	DEU
INSTA ADVANCE OY	FIN
ISCG SP. Z O. O.	POL
JANES (JANE'S GROUP UK LIMITED)	GBR
KING ICT D.O.O.	HRV
KLARRIO	BEL
L.A. INTERNATIONAL COMPUTER CONSULTANTS LIMITED	GBR
LEIDOS, INC.	USA
LEONARDO S.P.A	ITA
LIREX BG	BGR
M&I PARTNERS	NLD
MDOS CONSULTING INC.	CAN
MICROSOFT	BEL
MSG SYSTEMS AG	DEU
NCP ENGINEERING GMBH	DEU
NETAPP U.S. PUBLIC SECTOR, INC.	USA
NOKIA BELL	BEL
NORTAL AS	EST
NTT BELGIUM	BEL
NTT DATA SPAIN SLU (B82387770)	ESP
ORACLE AMERICA, INC.	USA
ORACLE BELGIUM	BEL
OTE (HELLENIC TELECOMMUNICATIONS ORGANIZATION S.A.)	GRC
PA CONSULTING	GBR

PATRIA AVIATION OY	FIN
PROXIMUS	BEL
PWC CANADA	CAN
PWC STRATEGY& GERMANY GMBH	DEU
REPLY DEUTSCHLAND SE	DEU
REPLY LIMITED	GBR
ROWDEN TECHNOLOGIES LTD	GBR
SAVACO	BEL
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION	USA
SECUNET SECURITY NETWORKS AG	DEU
SIRTI DIGITAL SOLUTIONS	ITA
SOPRA STERIA AS	NOR
SOPRA STERIA AS	NOR
SOPRA STERIA BENELUX	BEL
SOPRA STERIA GROUP	FRA
SPEKTRUM MANAGEMENT GROUP LTD	GBR
STM SAVUNMA TEKNOLOJILERI MUHENDISLIK VE TICARET ANONIM SIRKETI	TUR
STUDIOTECH	BEL
SYNTELLIGEN	BEL
TELEBIT S.P.A.	ITA
TELECOM ITALIA S.P.A	ITA
TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U. (A78053147)	ESP
TELEKOM DEUTSCHLAND GMBH	DEU
TELELINK BUSINESS SERVICES	BGR
TELSY S.P.A.	ITA
THALES SIX-GTS FRANCE	FRA
TIETOEVRY FINLAND OY	FIN
T-SYSTEMS INTERNATIONAL GMBH	DEU
TUBITAK BILGEM	TUR
UNI SYSTEMS (MAE)	GRC
UNIKIE OY	FIN
VASS EU SERVICES SA	LUX
VECTOR SYNERGY SP. Z O. O.	POL
VERIZON BELGIUM LUXEMBURG	BEL
VODAFONE BELGIUM	BEL
VODAFONE GROUP ENTERPRISE LIMITED	GBR

NCIA/ACQ/2025/06687
4 April 2025

DISTRIBUTION LIST:

All Prospective Bidders 1

NATO Delegations (Attn: Infrastructure Adviser): 1

Embassies in Brussels (Attn: Commercial Attaché):

Albania	
1	
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1
Estonia	1
Finland	1
France	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
The Netherlands	1
North Macedonia	1
Norway	1
Poland	1

Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Sweden	1
Republic of Türkiye	1
The United Kingdom	1
The United States (electronic copy to **brussels.office.box@mail.doc.gov**)	1
Belgian Ministry of Economic Affairs	1

NATO HQ

Investment Committee Secretariat

NATO Office of Resources, Management and Implementation Branch – Attn: Deputy Branch Chief

NCI Agency – Internal Distribution

REGISTRY (For Distribution)

NATEXs

All NATEXs

RFP-CO-42419-PBN-0

STATEMENT OF WORK

Effective Date: ..... : 4-Apr-25
Version ..... : 0.10 – QA VALIDATION - QA

Document Control

Title:	Annex A to RFP-CO-42419-PBN_0 Statement of work
Version:	0.10 – QA VALIDATION - QA - QA
Date:	3-Apr-25
Classification:	NATO UNCLASSIFIED
Filename:	NU-SOW-Annex A to RFP-CO-424219-PBN_0 SOW.docx
Template:	NU-TPL-Standard Document.dotx - Version 4.3

Table of Amendments

Version	Date	Description

Contents

List of Figures

List of Tables

1. Background Information

1.1. Problem Statement

[0002] The existing IT and networking infrastructure within NATO faces significant challenges that hinder its ability to meet modern operational demands.

[0003] Key issues include:

[0003].A Static Capacity: Current services lack scalability, limiting the ability to adapt to fluctuating demands.

[0003].B Fragmented Network Capacity: Network resources are dispersed, creating inefficiencies and hindering collaboration across the Alliance.

[0003].C Lack of Resilience: The infrastructure is vulnerable to disruptions, affecting operational continuity.

[0003].D Sub-Standard IT Service: Existing IT services fail to meet the required standards of reliability, performance, and user satisfaction.

[0003].E Disconnected from Modern Market: The infrastructure does not leverage mainstream technological advancements, resulting in outdated capabilities.

[0004] The current state of NATO's IT and networking ecosystem leads to a series of adverse effects:

[0004].A High Costs: Maintaining fragmented and outdated systems incurs significant expenses without delivering proportional value.

[0004].B Lack of Scalability: Inability to scale services in response to changing demands restricts operational flexibility.

[0004].C Limited Cost Transparency: The absence of clear cost structures impedes accountability and strategic financial planning.

[0004].D No Access to Modern Tools: NATO users are deprived of advanced tools and technologies necessary for effective collaboration and productivity.

[0004].E Lack of Seamless Collaboration: Disconnected systems create barriers to efficient communication and teamwork across the Alliance.

[0004].F Limited ability to achieve digital transformation and adoption of modern data centric and AI architectures.

[0004].G Inability to Adapt to Political Changes: The rigid and outdated IT structure limits NATO's ability to respond to evolving political and strategic environments rapidly.

1.2. Programmatic Vision

[0005] The Protected Business Network (PBN) vision is to establish an integrated Enterprise platform for developing a classified digital workplace (up to NATO RΞSTRICTED (NR)). Accordingly, the related CPP for PBN, Programme ID#: 9A3101, is intended to deliver flexible and adaptable solutions for IT mobility to the NATO Enterprise at the NATO RΞSTRICTED (NR) and NATO UNCLASSIFIED (NU) levels in support of business processes.

[0006] Within the Capability Package Plan (CPP) for PBN; Project # 0 (*Discover and Accelerate*) is the foundation to establish and deliver the entire PBN. Project # 0 is meant to select the NCIA industry partner (the Industry Service Integrator) who will deliver the NATO Enterprise Cloud Operating Model (NECOM) instrumentation, architecture, implementation plan and contracting framework. The CPP implementation, supported by

the Industry Service Integrator, will require authorization and funding approvals from the NATO Nations that, according to the CPP, will occur after the submission of the following 2 (two) projects:

- Project # 1 (*Implement and Scale*);
- Project # 2 (*Community of Interest (COI) Migration*).

[0007] Accordingly, Project # 1 will represent the pilot for implementing the PBN capability at one selected Headquarter within the NATO Enterprise. Upon successful completion of the pilot implementation foreseen at Project #1; multiple follow-on projects, also foreseen in Project # 1, will follow, allowing the transition of the rest of the NATO Enterprise to the PBN environment, while applications transformation will be managed through parallel activities (foreseen in Project # 2).

1.3. Business Benefit

[0008] The envisioned business benefits to be achieved include:

[0008].A Enterprise-Wide Scalable Network: Implement a unified, scalable network ecosystem that supports the diverse needs of NATO's enterprise community.

[0008].B Resilient Infrastructure: Build a resilient system capable of maintaining operational continuity under various conditions.

[0008].C Top-Tier IT Services: Provide high-quality IT services that meet the performance and reliability expectations of all users.

[0008].D Integration with Modern Market Solutions: Leverage mainstream technological advancements to ensure access to cutting-edge tools and capabilities.

[0008].E Enhanced Collaboration: Enable seamless communication and teamwork across the Alliance through unified platforms and standardized processes.

[0008].F Comprehensive IT Governance: Establish governance tools and processes to manage NATO's entire IT footprint, ensuring accountability, transparency, and rapid transformational alignment with changing organizational objectives.

[0008].G Long Term Industrial Partnerships: Support the transformation of NATO and of the NCIA as Cloud Service Broker to mature cloud adoption experience to people, process and procedures, to allow NATO to take advantage of rapid market developments and large scale industrial investments in cloud service provision.

1.4. NATO Enterprise Cloud Operating Model (NECOM)

[0009] The adoption of cloud service at scale requires the establishment and operationalization of an enterprise cloud operating model. This model serves to define the Enterprise entities and their respective roles and contribution to enable the establishment and operation of a coherent cloud based enterprise environment. NATO has outlined an initial operating model referred to as the NATO Enterprise Cloud Operating Model (NECOM). The Industry Service Integrator will operate and discharge its contract obligations as an integral part of this model in the role of Cloud Service Manager (CSM). This section, supported by the following graphical representation, describes the elements and functions associated with the NECOM.

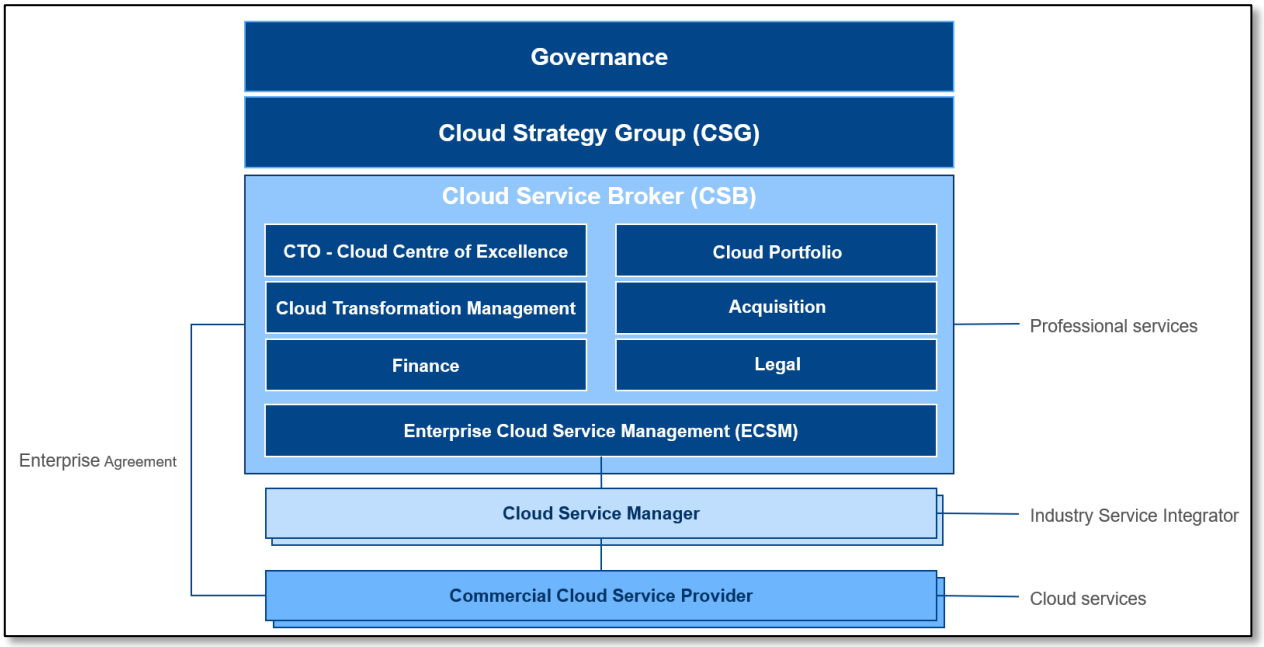

Figure 1: NATO Enterprise Cloud Operating Model (NECOM)

1.4.1. The Cloud Strategy Group (CSG)

[0010] The CSG defines the overarching cloud strategy and direction of the PBN Project. It provides a clear vision and goals for the Cloud Service Broker (CSB) to help achieve the cloud ambitions and empowers the CSB to achieve these goals. Together with other NATO Governance elements, it is accountable for the Cloud Strategy, Policy and coordinating high-level decision making.

1.4.2. The Cloud Service Broker (CSB)

[0011] The CSB is responsible for implementing/realizing the Cloud Strategy of the CSG. It is a collection of different teams with expertise extending across all domains necessary to migrate to, transform and efficiently operate cloud services, such as program and project management, financial management, acquisition, legal and cloud subject matter expertise. It spans the following essential components/functions:

1.4.2.1. The CTO-Cloud Centre of Excellence (CTO-CCoE)

[0012] CTO-CCoE, an organic part of the NCIA, sets cloud architectures, standards, and technical frameworks. It provides technical advice to guide the decisions of the CSG and offers different options to address Enterprise requirements raised by CSG stakeholders. The CTO-CCoE will fulfil the CSB Cloud Technical Design Authority (TDA) function in the context of the PBN program.

1.4.2.2. The Cloud Portfolio

[0013] The Cloud Portfolio, an organic part of the NCIA as it prioritizes and manages cloud projects (including those of the PBN program), ensuring alignment with NATO's Enterprise requirements.

1.4.2.3. The Cloud Transformation Management (CTM)

[0014] The CTM office leads cloud modernization and transformation. It executes cloud transformation initiatives in line with the priorities of the Cloud Portfolio and under the lead of the CTO-CCoE.

1.4.2.4. Key enabling functions

[0015] The key enabling functions within CSB for the PBN programme include **Finance** (responsible, for example, for overseeing budgeting and cost efficiency), **Acquisition** (responsible for example for managing procurement and contracts) and **Legal** (responsible for example for ensuring compliance with regulatory requirements, data sovereignty and exit strategies).

1.4.3. The Enterprise Cloud Service Management (ECSM)

[0016] The ECSM manages large enterprise agreements (for example, direct relationships with the Commercial Cloud Service Providers (CCSPs)) and ensures the compliance (with regards to SLAs, KPIs etc.) of the Cloud Service Manager (CSM). It thereby acts as the primary interface with the CSM. This function can only be executed by the NCIA.

1.4.4. The Cloud Service Manager (CSM)

[0017] The CSM is responsible for migration and managing (designing, building, and operating) the common enterprise cloud services listed at Section 2.2. The Industry Service Integrator will fulfil the CSM role.

1.4.5. The Commercial Cloud Service Providers (CCSP)

[0018] The CCSPs are industry partners providing cloud services that meet NATO's operational and security requirements. These providers offer scalable infrastructure, platforms and software solutions. The CCSPs enable NATO to leverage commercial cloud services as part of large Enterprise Agreements while maintaining control and oversight through the CSM and the ECSM.

1.5. NATO Enterprise Cloud View

[0019] The following graphical representation refers to the NATO Enterprise Cloud View and it showcases the foundational and supporting functions necessary for managing a secure and scalable cloud Enterprise scale environment.

[0020] The Industry Service Integrator, within its role of CSM of NECOM, will establish and operate the cloud operations functions (CloudOps), indicated by the red rectangle within the NATO Enterprise Cloud View. The services that support these functions are listed in Section 2.2.

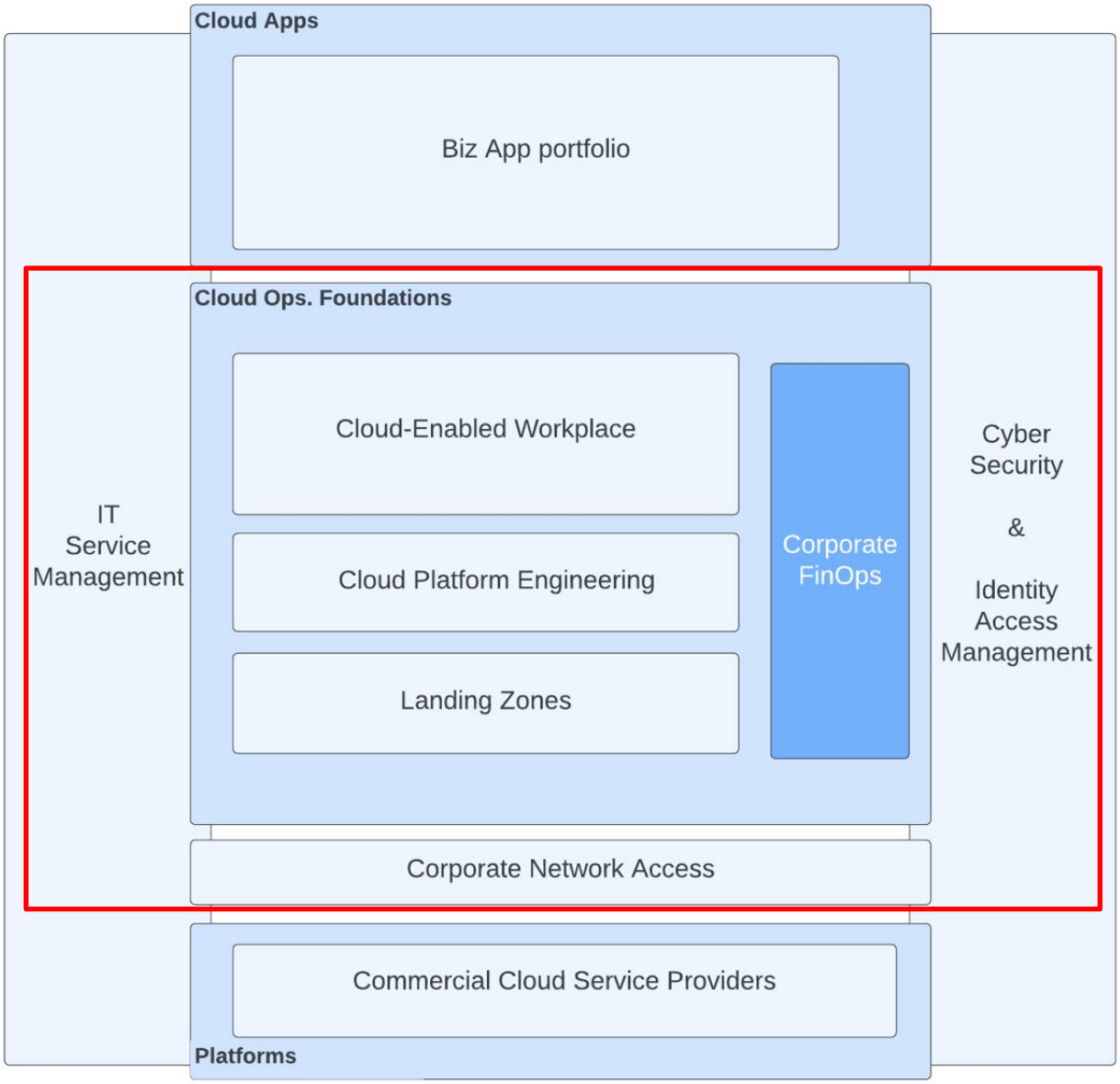

Figure 2: NATO Enterprise Cloud View

1.5.1. Cloud Applications layer (Biz App portfolio)

[0021] The Cloud Applications layer comprises business applications accessible to end users. These applications may be custom-developed or commercial off-the-shelf (COTS) solutions. They operate either within NATO's cloud infrastructure hosted on Infrastructure as a Service (IaaS) and Platform as a service (PaaS) or as Software-as-a-service (SaaS) offerings hosted in the vendor's cloud environment. While the migration of the Biz App portfolio is not in scope, the Industry Service Integrator will need to provide the means to access the Biz Apps on legacy environments as part of the transitional services in Section 2.3.

1.5.2. CloudOps Foundations layer

[0022] The CloudOps Foundations layer comprises the essential enabling services required to establish a secure, scalable, and resilient cloud environment. It forms the operational backbone of NATO's cloud landscape and platforms. Components of the Cloud Ops Foundations are:

1.5.2.1. The cloud-enabled workplace

[0023] The cloud-enabled workplace which is meant to deliver a modern, cloud-based work environment that seamlessly integrates digital tools, platforms, and technologies, empowering NATO Enterprise users to collaborate, communicate, and operate with efficiency.

1.5.2.2. Cloud Platform Engineering

[0024] Cloud Platform Engineering is the discipline of designing, developing, and managing a scalable, efficient, and resilient cloud infrastructure. It enables infrastructure and software development teams to seamlessly deploy, operate, and maintain applications. This practice emphasizes the creation of self-service, automated, and highly reliable cloud environments by leveraging standardized building blocks and compliance frameworks. Additionally, it supports DevSecOps, Site Reliability Engineering (SRE), and modern software delivery methodologies, ensuring agility, security, and operational excellence.

1.5.2.3. Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) Landing Zones

[0025] The Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) Landing Zones deliver pre-configured, secure, and scalable cloud environments specifically designed to accelerate cloud adoption while ensuring adherence to best practices in governance, security, and compliance. These landing zones are deployed using standardized deployment packages within the Platform Engineering environment. They provide a robust, ready-to-use foundation for efficiently deploying workloads in a multi-account or multi-subscription cloud setup, such as applications within the Business Application portfolio.

1.5.2.4. Corporate FinOps

[0026] The Corporate FinOps function encompasses the management, optimization, and control of the financial aspects of cloud computing. It involves the implementation of processes, tools, and strategies designed to plan, monitor, and allocate cloud costs effectively, ensuring the efficient utilization of cloud resources. Additionally, it includes the integration with NATO Enterprise financial systems and processes, aligning cloud financial operations with organizational financial governance and objectives. The Corporate FinOps function is executed by CTO-CCOE supported by services delivered by the Industry Service Integrator depicted in Section 2.2.5.

1.5.2.5. IT Service Management (SM)

[0027] SM encompasses the practices, processes, and tools employed to deliver, manage, and support cloud services. It builds upon traditional SM frameworks, adapting them to address the unique characteristics and requirements of cloud environments. SM is focused on ensuring that cloud-based services effectively meet the needs of both users and the organization. Key components of SM include, but are not limited to: Service Delivery and Support, Incident and Problem Management, Change Management, Monitoring, and Service Catalogue Management.

1.5.2.6. Identity and Access Management (IAM)

[0028] IAM refers to the processes, technologies, and practices used to securely manage user identities and control access to organizational resources. IAM ensures that only authorized users can access systems, applications, and data, while protecting sensitive information and also supports services and device identity integration. Key components include: Authentication, Authorization, User Provisioning, Multi-Factor Authentication

(MFA), and Role-based Access Control (RBAC). IAM also integrates with Enterprise Identity Services to streamline user management, enhance security, and maintain compliance across the organization. Although the IAM provides Cyber Security capabilities, it is important to highlight that a centralized identity management system is envisioned to provide unified access to the Cloud Apps and Cloud-Enabled Workplace capabilities across the NATO Enterprise. The role of the Industry Service Integrator is to establish and operate all cloud based IAM services and integrate with corporate processes and services for identity governance and identity data and data protection as depicted in Section 2.2.2.

1.5.2.7. Cyber Security

[0029] The Cyber Security function refers to the practices, technologies, and strategies used to protect cloud-based systems, data, and applications from cyber threats. It ensures the confidentiality, integrity, and availability of cloud resources while integrating with Enterprise security services for comprehensive protection. It includes the establishment of a cloud-based Security Operations Centre (SOC) for continuous threat monitoring and proactive detection. Additionally, cloud cybersecurity leverages compliance frameworks, threat intelligence, and security automation to proactively manage risks and ensure regulatory compliance with NATO Security policies and directives across cloud environments.

1.5.2.8. Corporate Network Access

[0030] Corporate Network Access refers to the secure and efficient methods employed to connect users, devices, and applications to cloud-based resources and services. It encompasses the management of data flows between on-premises environments, users, and the cloud, ensuring reliable access while maintaining security, performance, and compliance. Key technologies involved in cloud network access include Software-Defined Networking (SDN), Secure Access Service Edge (SASE), and identity-based access controls. Additionally, it facilitates seamless integration with existing NATO Enterprise networks and Internet Gateway Services, ensuring consistent and secure connectivity across multicloud environments, while aligning with NATO policies, directives and operational requirements. The scope for the Industry Service Integrator is limited to Secure Access Service Edge services including Zero Trust Network Access (ZTNA) and Secure Service Edge (SSE).

1.5.3. Platforms layer

[0031] The Platforms layer encompasses the public cloud services offered by Commercial Cloud Service Providers (CCSPs). As NATO moves towards implementing a multicloud architecture within the PBN, this layer will provide services from multiple CCSPs to ensure flexibility, redundancy, and scalability. By leveraging diverse cloud platforms, NATO aims to optimize resource availability, minimize vendor lock-in, and enhance operational resilience. This multicloud strategy allows for the selection of best-in-class services from various providers, ensuring that the NATO Enterprise can meet its evolving requirements for security, compliance, and performance.

[0032] These layers and services form a robust and secure NATO Enterprise Cloud View, ensuring NATO's cloud services are scalable, resilient, and secure for operational use.

1.6. Quality Management

[0033] The purpose of Quality Management is to ensure the quality of products, and services and the compliance to the defined processes and procedures that are used to produce them.

[0034] This document section aims to describe the NCIA requirements with regard to Quality related matters.

1.6.1. Introduction

SOW-0001 Unless otherwise specified in the SoW, the NATO Standardisation Agreement (STANAG) 4107 (Mutual Acceptance of Government Quality Assurance And Usage Of The Allied Quality Assurance Publications (AQAP)) as well as ISO 9001:2015 standard requirements shall apply.

SOW-0002 The Industry Service Integrator shall establish, execute, document and maintain an effective Quality Assurance (QA) program throughout the Contract's lifetime.

SOW-0003 The Industry Service Integrator 's QA effort shall apply to all services and products (both management and specialist) to be provided under the Contract. This includes all hardware, software, firmware and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract (including deliverable and non-deliverable items like test and support hardware and software), without limitation.

SOW-0004 The Industry Service Integrator 's QA efforts shall ensure that procedures are developed, implemented and maintained to adequately control the design, development, production, purchasing, installation, inspection, testing, configuration management and customer support of all services and all products, in accordance with the requirements of this Contract.

SOW-0005 The Industry Service Integrator, through its Quality Representative, shall be responsible for product quality control and for submitting to Purchaser acceptance products, supplies and services which conform to contractual submitting to Purchaser acceptance products, supplies and services which conform to contractual requirements only. The Industry Service Integrator shall maintain and, when required, deliver objective evidence of this conformance.

SOW-0006 The Industry Service Integrator shall include in orders placed with its Sub-Contractor(s) and Supplier(s), the Quality requirements necessary to ensure the supplies and services covered by the Sub-Contract(s) and/or Purchase Orders conform to the requirements of the prime Contract.

1.6.2. Quality Assurance Plan (QAP)

SOW-0007 The Industry Service Integrator shall provide a Quality Assurance Plan (QAP), compliant with AQAP 2105, for review to the Purchaser.

SOW-0008 The Industry Service Integrator QAP shall be consistent with all other plans, specifications, documents, and schedules, which are utilized under the Contract.

SOW-0009 All Industry Service Integrator procedures referenced in the QAP shall either be submitted with the plan or described in the plan and made available for review by the Purchaser upon demand.

SOW-0010 The QA Plan and all related QA procedures, and all their versions/revisions, shall be subject to Purchaser approval based on an agreed checklist.

SOW-0011 Processes and procedures established in the Industry Service Integrator provided QAP shall address all contracted services and include activities such as testing, monitoring and control. The QAP shall also include processes and procedures for reporting creation as part of deployment and delivery activities. This reporting must provide a verifiable, objective evidence for risk assessment in validating the deployment or delivery towards operations.

1.6.3. Quality Assurance Surveillance Plan

[0001] The Quality Assurance Surveillance Plan (QASP) aims to identify the methods and procedures the Purchaser will use to ensure it receives the services/products under the Contract as identified in the Statement of Work.

[0002] The intent of this plan is to hold the Industry Service Integrator accountable for quality control and to encourage the Industry Service Integrator to take appropriate steps to control and improve quality.

[0003] The Industry Service Integrator shall be responsible to develop an efficient methodology to ensure they meet and/or exceed the required thresholds of service as outlined in the Contract.

[0004] The Purchaser intends to perform surveillance on this contract in accordance with this QASP, but reserves the right to monitor the contract in any manner necessary, at any times necessary, and at all places necessary to ensure that the rendered services conform to the Contract requirements.

[0005] The Purchaser reserves the right to perform Quality Assurance at the subcontract level, if applicable. Non-conforming services discovered with sub-contractors will be addressed with the prime Industry Service Integrator for resolution.

2. Contract Performance Scope

[0035] As addressed in this document, the Industry Service Integrator will perform the Cloud Service Manager (CSM) role instituted by virtue of the NATO Enterprise Cloud Operating Model (NECOM). Subject to funds availability resulting from PBN Project # 1 and/or # 2 approval and specific tasking received by the NCIA, the Industry Service Integrator will therefore be required to accomplish a set of preparatory activities (Commissioning Activities) and provide for the follow-on rendering of integrated CloudOps services (Operational Services) throughout the contract. In addition, Transitional Services will be required to facilitate migration of users and applications from the currently existing environments to the PBN once it will be established.

[0036] A list of the Commissioning Activities, Operational and Transitional Services is provided below.

2.1. Commissioning Activities

[0037] The Commissioning activities are intended to serve as preparatory activities that enable the foundational design and commissioning implementation of CloudOps services. While Commissioning Activities will be required at the beginning of contract performance for the purpose stated above; the NCIA will also request the Industry Service Integrator to execute them on an “as-needed” basis for the purpose of implementing cloud service migration to the various entities of the NATO Enterprise.

2.1.1. Performance of “as-is” assessment

SOW-0012 The Industry Service Integrator shall conduct a representative assessment of NATO’s current IT landscape (NU/NR), including infrastructure, applications, and processes. This assessment will serve as the baseline for the transformation.

SOW-0013 The Industry Service Integrator shall systematically discover all existing workloads within the existing NATO’s IT environment, including virtual machines (VMs), applications, databases, network components, cross-domain interfaces and existing cloud services.

SOW-0014 At conclusion of this assessment, the Industry Service Integrator shall deliver a detailed inventory to the NCIA which shall depict all existing workloads, including usage data, application dependencies, data flows and required interconnections.

2.1.2. Development of a “to-be” Service Model Design

SOW-0015 The Industry Service Integrator shall design the future architecture, processes, and governance models based on the NATO Enterprise Cloud View and in line with extant NATO policy and directives.

SOW-0016 The Industry Service Integrator shall deliver:

SOW-0016.A Cloud Solution Architecture: Through adoption of a cybersecurity-by-design approach, the Industry Service Integrator must design and deliver a comprehensive cloud solution architecture that outlines how NATO will transition from its current IT environment to the desired cloud-based service future state enabling the business benefits described in Section 1.3. This architecture needs to be compliant to the relevant NATO security policies and directives. The Industry Service Integrator must deliver a process description on how continuous compliance is achievable. In addition, the Industry Service Integrator must deliver a high-level service transition strategy and action plan that minimizes disruption and ensures continuity of operation.

SOW-0016.B Security Accreditation support and documentation: the Industry Service Integrator must provide all the necessary deliverables to support the Security

Accreditation process. In addition, the Industry Service Integrator must propose a transformation plan for the security accreditation process to enable agile and incremental architecture changes, including continuous compliancy evaluation.

SOW-0016.C Business Continuity Criteria/Plan and Exit Strategy: The Industry Service Integrator must develop a comprehensive Business Continuity Plan (BCP) that includes criteria to ensure operational resilience during and after the cloud transition. This must also include a definition and corresponding action plan for a clear exit strategy for each of the leveraged CCSPs.

SOW-0016.D Costed PBN Service Catalogue: The Industry Service Integrator must, in coordination with the CSB, develop a costed customer service catalogue for NATO's PBN. This catalogue needs to represent the services and corresponding cost model that the NCIA will offer to NATO Enterprise customers.

2.1.3. Implementation of the "to-be" Service Model

SOW-0017 Based on the Cloud Solution Architecture and the service transition strategy and action plan, the Industry Service Integrator shall build the NATO PBN platform, which includes the following components of the NATO Enterprise Cloud View:

SOW-0017.A CloudOps Foundations;

SOW-0017.B Cyber Security;

SOW-0017.C IT Service Management;

SOW-0017.D Corporate Network Access;

SOW-0017.E Identity and Access Management.

SOW-0018 In addition, to facilitate the migration from the legacy to the PBN environment, the Industry Service Integrator shall deliver the following services (further down described in this document at Section 2.3):

SOW-0018.A Migration and transformation planning;

SOW-0018.B Reach-back and reach-forward from/to the legacy environment.

SOW-0019 The Industry Service Integrator shall:

SOW-0019.A operationalize the platform to establish all the necessary interconnections and dependencies;

SOW-0019.B build the platform in accordance with NATO security policies and directives and supported by the Cloud Service Broker;

SOW-0019.C implement the Business Continuity requirements to ensure resiliency.

2.2. Operational Services

[0038] Operational services are those to be performed during the entirety of the contract performance period. These services are listed below.

2.2.1. Iaas and PaaS Landing Zones Management Services

[0039] This service entails the Industry Service Integrator providing comprehensive end-to-end solutions for the design, deployment, operation, maintenance, and management of secure, scalable, and compliant cloud Landing Zones. These Landing Zones are designed to support enterprise-grade Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) workloads. This service leverages standardized infrastructure deployment packages, referred to as "secure products", ensuring compliance with both security and service management requirements.

[0040] These Landing Zones will serve as a robust and modular foundation for hosting and operating workloads across multiple CCSPs. The volume and scope of the service will be determined based on the AS-IS assessment and will be further defined and built in alignment with the TO-BE architecture. The service focuses on leveraging each CCSP's unique strengths while ensuring interoperability and adherence to NATO Policies and Directives.

[0041] The IaaS/PaaS Landing Zone Management service is to:

[0041].A Enable the NATO Enterprise to build scalable multicloud environments that provide high availability, security, and cost efficiency.

[0041].B Establish a secure and governed infrastructure framework for seamless hosting and management of critical workloads.

[0041].C Optimize operational performance and compliance with evolving NATO Security Policies and Directives, such as the Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems (AC/322-D(2021)0032-REV1).

[0041].D Deliver a future-proof cloud architecture that evolves with the NATO Enterprise growing and changing business requirements.

SOW-0020 Accordingly, based on the above, the Industry Service Integrator shall deliver, as part of the developed Cloud Solution Architecture, the following key service components:

SOW-0020.A Multi-Cloud Integration:

SOW-0020.A.1 Build Landing Zones leveraging multiple CCSPs to provide flexibility, resilience, and access to a broader range of tools and services.

SOW-0020.A.2 Implement strategies for cross-cloud compatibility and interoperability which address specific compliance and operational features unique to each CCSP.

SOW-0020.B Security and Compliance:

SOW-0020.B.1 Implement robust security protocols, including encryption, network segmentation, and automated security monitoring and logging.

SOW-0020.B.2 Integrate audit-friendly configurations and continuous monitoring and logging to ensure compliance with applicable standards and regulations.

SOW-0020.C Infrastructure Automation and Scalability:

SOW-0020.C.1 Use Infrastructure as Code (IaC) tools to automate infrastructure versioning, provisioning and configuration.

SOW-0020.C.2 Architect the environment for dynamic scalability to accommodate varying workloads and peak demands.

SOW-0020.D Governance and Operational Excellence:

SOW-0020.D.1 Establish governance frameworks for resource allocation, role-based access control, and budget tracking to prevent overspending and resource sprawl.

SOW-0020.D.2 Leverage cloud-native tools for real-time monitoring, logging, and alerting to maintain operational continuity and mitigate risks.

SOW-0020.E Maintenance and Support :

SOW-0020.E.1 Provide 24/7 monitoring, incident management, and support for workload operations.

SOW-0020.E.2 Regularly update Landing Zone configurations to align with CCSP updates, NATO security advisories and best practices.

SOW-0020.F Knowledge Transfer and Documentation:

SOW-0020.F.1 Provide and automate the detailed documentation of architecture, design, processes, playbook, Standard Operating Procedure (SOP) information.

SOW-0020.F.2 Conduct training sessions to empower internal teams to manage, scale, and secure the cloud environments effectively.

SOW-0020.G Disaster Recovery (DR) and Business Continuity (BC):

SOW-0020.G.1 Develop and implement resilient disaster recovery plans with defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

SOW-0020.G.2 Build processes to secure availability of robust failover mechanisms and to implement backup strategies for the purpose of maintaining business continuity.

SOW-0020.G.3 Periodically exercise and demonstrate the various DR and BC plans and processes orchestrated through NECOM.

SOW-0020.H Patching and Updates:

SOW-0020.H.1 Implement automated patch management processes to ensure all operating systems, applications, and infrastructure components are up to date with the latest security patches and updates.

SOW-0020.H.2 Establish periodic patching schedules while ensuring minimal disruption to workloads and operations.

SOW-0020.H.3 Monitor CCSP updates and vulnerabilities, applying timely security updates to prevent exploitation or breaches.

2.2.2. Cloud Identity Access Management (IAM) Services

[0042] This service entails the Industry Service Integrator providing multicloud IAM services for personnel, devices, and services within the multicloud environment. This must encompass various factors, including the type of identity (who/what), location (from where), connectivity (via which network access), device (with what), and credentials (through which Multi-Factor Authentication methods) required to access authorized cloud-based services. The governance of cloud IAM must align with the NATO Enterprise IAM framework, ensuring proper identity data brokering, standardization, and protection.

SOW-0021 Accordingly, based on the above, the Industry Service Integrator shall deliver, as part of the developed Cloud Solution Architecture, the following key service components:

SOW-0021.A Single-Sign-On: sign in using one set of credentials to multiple independent cloud and software systems in a federated multi-cloud environment.

SOW-0021.B Authentication: Manage self-service password reset, Multi-Factor Authentication, custom banned password list, and smart lockout.

SOW-0021.C Conditional access: control access based on identity-driven signals.

SOW-0021.D Implement device access controls that determine and evaluate the conditions for accessing corporate data.

SOW-0021.E Identity governance: implement control mechanism to ensure the right users have access to the right resources and ensure compliance with NATO Enterprise Identity Data Brokering, Standardisation and Protection processes and services.

SOW-0021.F Identity protection: detect potential vulnerabilities affecting identities and respond to suspicious actions.

SOW-0021.G Privileged identity and access management.

SOW-0021.H Federated IAM solution for external identity providers.

SOW-0021.I Monitoring and health: provide real-time dashboards to get insights into the security and usage patterns of the IAM platform.

2.2.3. Cloud Enabled Workplace Services

[0043] This service entails the Industry Service Integrator providing digital workplace services to NATO Enterprise users to increase productivity and digital dexterity to support the organization's digital business strategy. The Industry Service Integrator must deliver a virtual work environment that brings together technology, people, and business processes to facilitate communication, collaboration, and productivity within the organization.

SOW-0022 This virtual work environment, as provided by the Industry Service Integrator, shall provide the following capabilities:

SOW-0022.A Implement digital workplace services to enable communication and collaboration for NATO Enterprise users.

SOW-0022.B Promote best practices for content and knowledge management (KM).

SOW-0022.C Facilitate administration, management, governance, and reporting oversight.

SOW-0022.D Provide contextual integration with line-of-business applications.

SOW-0023 Accordingly, based on the above, the Industry Service Integrator shall deliver, as part of the developed Cloud Solution Architecture, the following key service components:

SOW-0023.A Provide onboarding for all NATO Enterprise users into the cloud environment and integrate with the PBN IAM functions.

SOW-0023.B Migrate users and community data to the new collaboration services. This excludes the Cloud Applications layer as depicted in the NATO Enterprise Cloud view in Section 1.5.

SOW-0023.C Implements, delivers and maintains the following digital workplace functionalities (services to be delivered are provided per each functionality/sub-functionality):

SOW-0023.C.1 Workplace Content Management such as content creation, versioning, content topology, metadata tagging, information protection, records management and archive and backup.

SOW-0023.C.2 Workplace Collaboration and Productivity such as document sharing and co-authoring, real-time collaboration and collaboration workspaces.

SOW-0023.C.3 Workplace Communication and Messaging such as communication and messaging solutions to allow end user interaction with internal and external contacts, email, chat, videoconferencing, telephony, calling and unified communications as a service (UCaaS) and capabilities to connect with meeting room and conferencing equipment.

SOW-0023.C.4 Unified Endpoint Management (note: this service does not require the Industry Service Integrator to supply and delivery user endpoints such as laptops and mobile devices).

SOW-0023.C.5 Workplace Automation such as low-code and development capabilities for NATO Enterprise users to automate their

workplace processes and any repeatable or laborious manual processes in order to improve efficiency.

SOW-0023.C.6 Business and technical support to ensure comprehensive support for end users by providing tools and services that enhance business operations, and address business-specific requirements. This includes dedicated resources to handle queries, guide users in leveraging digital capabilities effectively, and support the adoption of workplace technologies.

SOW-0023.C.7 Knowledge Management to provide capabilities supporting the sharing of knowledge and know-how end implement solutions to capture and curate knowledge in order for end users to be able to efficiently edit, organize, update and retire knowledge management content.

SOW-0023.C.8 Cloud Printing Services to enable end-users to print documents and other materials on any device associated with the cloud.

2.2.4. Corporate Network Access Services

[0044] This service entails the Industry Service Integrator to provide Secure Access Secure Service Edge (SASE) capabilities to ensure secure and reliable connectivity to the cloud resources. This includes integration with existing Enterprise networks.

SOW-0024 Accordingly, based on the above, the Industry Service Integrator shall deliver, as part of the developed Cloud Solution Architecture, the following key service components:

SOW-0024.A Design, operate and maintain a SASE solution including Zero Trust Network Access (ZTNA) and Secure Service Edge (SSE) functions.

2.2.5. Cloud Cost Optimization Services

[0045] The Industry Service Integrator must provide, under the governance guidance of the CTO-CCOE, Cloud Cost Optimization services that enable comprehensive cost management and billing services for the PBN, thus including planning, monitoring, optimizing, and forecasting of cloud costs.

SOW-0025 Accordingly, based on the above, the Industry Service Integrator shall deliver the following key service components:

SOW-0025.A Cloud Visibility and Transparency: leverage cost visualization tools with dynamic dashboards, cost analysis, cost incidents, showback and chargeback information.

SOW-0025.B Cost Optimization: implement waste management strategies for proactive consumption management and savings tracking in coordination with the application's teams.

SOW-0025.C Forecast: deliver forecast capabilities, including budget management, consumption estimation, and project cost estimation.

SOW-0025.D Enhance Cloud Governance: define and apply a comprehensive tagging strategy, alerts, and monitoring mechanisms, ensuring alignment with organizational policies and enabling efficient cost control and accountability.

2.2.6. Cloud Platform Engineering Services

[0046] The Industry Service Integrator must provide operation services and perform continuous improvement activities of a Platform Engineering environment leveraging the existing NATO Software Factory (NSF) for developing, testing, and integrating secure cloud infrastructure components, using a centralized DevSecOps toolchain to enable self-service capabilities for software engineering thereby improving and standardizing security, compliance, reliability and costs.

[0047] The Industry Service Integrator must deliver, through a qualified commercial partner, agile, development-focused platform engineering service support to cope with fast-paced infrastructure and software development requirements.

SOW-0026 Accordingly, based on the above, the Industry Service Integrator shall deliver, as part of the developed Cloud Solution Architecture, the following key service components:

SOW-0026.A Cloud Architecture and Design:

- SOW-0026.A.1 Develop customized cloud architecture and deployment artefacts (‘secure products’) compliant with security and service management requirements that align with the business goals and NATO standards.
- SOW-0026.A.2 Design scalable and resilient secure products for the supported Commercial Cloud Service Providers.
- SOW-0026.A.3 Implement multi-cloud architectures to enhance flexibility, scalability and redundancy.
- SOW-0026.A.4 Design and implement a DevSecOps framework for deliverables, including testing and comprehensive reporting.

SOW-0026.B Infrastructure as Code (IaC):

- SOW-0026.B.1 Utilize IaC tools to version control, validate, manage, and automate the provisioning of standardized cloud resources.
- SOW-0026.B.2 Ensure consistent and repeatable deployments, reducing the risk of human error.

SOW-0026.C Continuous Integration and Continuous Delivery (CI/CD):

- SOW-0026.C.1 Set up CI/CD pipelines to streamline the development, testing, and deployment of applications and cloud resources.
- SOW-0026.C.2 Automate deployment and tear-down of test environments, with the possibility to integrate this into CI/CD pipelines.

SOW-0026.D Security and Compliance:

- SOW-0026.D.1 Implement security measures, including IAM, encryption, and network security.
- SOW-0026.D.2 Ensure continuous compliance with applicable security frameworks.

SOW-0026.E Monitoring and Optimization:

- SOW-0026.E.1 Integrate with applicable monitoring and logging solutions to gain real-time insights into cloud infrastructure performance.
- SOW-0026.E.2 Optimize resource utilization and cost management through continuous monitoring and analysis.

SOW-0026.F Disaster Recovery and Backup:

- SOW-0026.F.1 Design and implement disaster recovery plans to ensure business continuity in case of unexpected failures.

SOW-0026.F.2 Set up automated backup solutions to protect critical data and applications.

SOW-0026.G DevSecOps and Collaboration:

SOW-0026.G.1 Onboard BizApps teams to the DevSecOps toolchain in the Platform Engineering environment.

SOW-0026.G.2 Handle incidents and service requests raised by users of the platform engineering environment (including NATO Enterprise, industry and academia).

SOW-0026.G.3 Design and support an onboarding process for new teams and users.

2.2.7. Service Management Services

[0048] The Industry Service Integrator must provide Service Management (SM) services to address the planning, delivery, operation, and control of the NATO services provided to its customers. Service Management provides the governance and control of a variety of practices aimed at maximizing service quality and ensuring efficient use of IT resources.

[0049] SM-by-Design is defined as a service integration model based on several SM components, such as: configuration management, request fulfilment, incident management, change management, service level management, service monitoring and analysis, and service transition. This integration model is scalable, allowing incorporating new services management practices into the existing service management toolset and practices.

[0050] SM-by-Design provides building blocks, affecting costs and design solutions. The service integration model assists in deciding which SM components can be implemented in the three main topology levels (enterprise level, domain level, or element level) and their interactions with other services.

SOW-0027 Accordingly, based on the above, the Industry Service Integrator shall deliver, as part of the developed Cloud Solution Architecture and for the entire NATO Enterprise Cloud View stack, the following key service components:

SOW-0027.A Configuration Management: ensure accurate and reliable information about Configuration Items (CIs) and their relationships throughout the service lifecycle, enabling effective service delivery and decision-making. Includes all CIs enabling and supporting the service provisioning, and their relationships and dependencies between industry and the NCIA elements, including the service delivery points.

SOW-0027.B Service modelling: provide a complete and accurate inventory of all services offered and their dependencies with existing ones to enable clear visibility of service components and their relationships down to the CIs.

SOW-0027.C Incident Management, Request Fulfilment, Change Management and Service Level Management: ensure the restoration of services timely and according to agreed contract performance standards; ensure the efficient fulfilment of service requests while minimizing disruptions. Problem Management shall provide root-cause-analysis, knowledge base and a structured approach to manage incidents and service requests across all support levels. The Industry Service Integrator shall provide service quality reporting based on agreed contract performance standards.

SOW-0027.D Service Monitoring performance, service capacity and service availability, by implementing a service let monitoring framework. The Industry Service Integrator shall provide root cause analysis material and evidence, based on contractually agreed KPIs and KQIs for service availability, service capacity and service performance. The Industry Service Integrator shall provide

evidence of escalation capability in order to provide centralized service status awareness.

SOW-0027.E Service Performance Visualization and Reporting: ensure all services are monitored in accordance with contractually agreed service levels. It establishes consistent metrics and definitions checked against customers and stakeholders' expectations.

2.2.8. Cyber Security Services

[0051] The Industry Service Integrator must ensure that the security of all services and components in the PBN are provided at the required level by effectively responding to changes in the cloud environment. The Cyber Security by Design principle must be followed, in addition to ensuring compliance to relevant NATO policy requirements and enabling security accreditation of PBN. All cyber security services that provide the level of security required by the Enterprise business services, and based on the related operational objectives, must be designed and implemented. The Industry Service Integrator must deliver cyber security services ensuring that the right level of security is provided continuously during operation and in response to changes in the cloud operational environment.

[0052] At all times during contract execution, the Industry Service Integrator must be able to assess and report on the cyber security risk of PBN through a process that enables Continuous Risk Assessment (CRA) and Automated Compliance Audit (ACA). To ensure compliance with the CRA methodology; the process established by the Industry Service Integrator must allow execution of independent security audits, in line with [AC/322-D(2021)0032-REV1]).

[0053] The Industry Service Integrator's provided PBN Cyber Security Operating Model shall support unified multi-cloud security operations ensuring a coherent delivery of cyber security services in a multi-cloud environment while NATO Cyber Security Centre (NCSC) can maintain an overall view of the security posture of PBN, and accountability for the delivery of cyber security services.

SOW-0028 The cyber security services provided by the Industry Service Integrator shall encompass cyber security of all public cloud environments managed by the Industry Service Integrator including development, testing, staging, and operational environments, and include the following service components:

SOW-0028.A Cyber security monitoring and detection.

SOW-0028.B Cyber security incident response.

SOW-0028.C Cyber security (forensic) analysis.

SOW-0028.D Continuous security posture assessment.

SOW-0028.E Cryptography, and key and certificate management.

SOW-0028.F Cyber security information sharing.

SOW-0028.G Gateway security, and cyber security provided by Secure Access Service Edge (SASE) providers and Cloud Access Security Brokers (CASBs), including the security of SaaS.

SOW-0028.H Cyber Security required to address any risk (to NATO information, assets or services) arising from the communication path between PBN public cloud environments, clients, and on-premise infrastructure.

SOW-0028.I Cyber security of cloud managed endpoints.

SOW-0028.J Integration between PBN cyber security operations and NCSC SOC operations with respect to processes, technology, roles, and responsibilities.

SOW-0028.K Support to PBN security compliance, audit and accreditation.

SOW-0028.L Integration into the Cloud IAM and corporate IAM services and processes.

2.3. Transitional Services

[0054] Transitional services are those to be delivered as part of the contract performance period, however, execution will last up to the moment that all users and applications are migrated from the legacy environment to the newly established PBN.

2.3.1. Migration and transformation planning services

[0055] The migration and transformation planning services ensure a smooth, secure, and cost-effective transition. These services include assessing cloud readiness, defining migration strategies, prioritizing workloads, and estimating costs. Transformation planning focuses on modernizing the IT landscape, optimizing data migration, redesigning operational models, and ensuring compliance. The process involves pilot testing, phased execution, governance, and ongoing optimization to maximize cloud benefits while minimizing risks and disruptions.

SOW-0029 The Industry Service Integrator shall deliver migration and transformation planning services to enable the user, user data and community data migration as depicted in Section 2.2.3, and to enable the application modernization and migration as part of Project # 2 in close collaboration with the BizzApp Teams and Project # 2 contractor(s). This includes delivery of the following:

SOW-0029.A Communication plan. The Industry Service Integrator must develop a comprehensive communication plan to ensure all stakeholders and business users are kept informed throughout the transformation and migration projects lifecycle. This will include regular updates on progress, challenges, and key milestones via meetings, reports, and digital channels to foster transparency and collaboration.

SOW-0029.B Cloud Readiness Assessment Report:

- SOW-0029.B.1 Based on the AS-IS assessment, evaluation of current IT infrastructure, applications, and workloads.
- SOW-0029.B.2 Identification of cloud migration feasibility and potential challenges.
- SOW-0029.B.3 Security, compliance, and risk assessment.

SOW-0029.C Migration Strategy and Roadmap:

- SOW-0029.C.1 Detailed migration approach.
- SOW-0029.C.2 Prioritization of workloads based on business impact and technical complexity.
- SOW-0029.C.3 Phased migration plan with key milestones, timelines and rollback strategy.

SOW-0029.D Data Migration and Integration Plan:

- SOW-0029.D.1 Data governance.
- SOW-0029.D.2 Strategy for data transfer, cleansing, and synchronization.
- SOW-0029.D.3 Security measures and compliance considerations for data movement.
- SOW-0029.D.4 Integration with existing systems and third-party applications.

SOW-0029.E Data governance strategy.

SOW-0029.F Execution and Governance Plan:

- SOW-0029.F.1 Change management and risk mitigation strategies.
- SOW-0029.F.2 Governance framework for ongoing cloud operations.

SOW-0029.G Training and Knowledge Transfer Materials:

SOW-0029.G.1 User adoption and change management strategies.

SOW-0029.H Continuous Optimization and Post-Migration Support Plan:

SOW-0029.H.1 Performance monitoring and cost optimization recommendations.

SOW-0029.H.2 Automation strategies for scaling and managing cloud resources.

SOW-0029.H.3 Ongoing compliance, security audits, and policy updates.

2.3.2. Reach back and reach forward services

[0056] Reach back and reach forward services are connectivity solutions designed to ensure seamless interoperability during a cloud migration process. Reach back services enable users or applications that have already migrated to the cloud to securely access and interact with legacy or on-premises systems that have not yet been transitioned, while reach forward services allow users still operating in the legacy environment to access applications and services that have already moved to the cloud. Both approaches facilitate a hybrid operating model, ensuring business continuity and reducing disruption by providing secure connectivity between migrated and non-migrated environments until the full migration is complete.

SOW-0030 Accordingly, based on the above, the Industry Service Integrator shall deliver, as part of the developed Cloud Solution Architecture, the following key service components:

SOW-0030.A Secure user connectivity tooling: ensure NATO Enterprise users can seamlessly consume applications hosted in both the legacy environments and the PBN.

SOW-0030.B Data synchronization and integration: establish a secure method for data synchronization between the legacy environments and the PBN.

SOW-0030.C Application dependencies: establish secure connectivity between migrated and non-migrated applications and services.

Appendix A Abbreviations

[0057] This appendix aims to list the abbreviations used in this document and their respective meaning.

Table 1 - List of abbreviations

Abbreviation	Full Text
ACA	Automated Compliance Audit
BC	Business Continuity
BCP	Business Continuity Plan
CASB	Cloud Access Security Brokers
CCSP	Commercial Cloud Service Providers
CCSP	Commercial Cloud Service Providers
CI	Configuration Items
CloudOp	Cloud Operations Functions
COTS	commercial off the shelf
CPP	Capability Package Plan
CRA	Continuous Risk Assessment
CSB	Cloud Service Broker
CSG	Cloud Strategy Group
CSM	Cloud Service Manager
CTM	Cloud Transformation Management
CTO	Chief Technology Office
CTO-CCoE	CTO Cloud Centre of Excellence
DR	Disaster Recovery
ECSM	Enterprise Cloud Service Management
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity Access Management
KM	knowledge management
MFA	Multi Factor Authentication
NCSC	NATO Cyber Security Centre
NECOM	NATO Enterprise Cloud Operating Model
NR	NATO RΞSTRICTED
NSF	NATO Software Factory
NU	NATO UNCLASSIFIED
PaaS	Platform as a service
PAN	Public Access Network
PBN	Protected Business Network
QA	Quality Assurance
QAP	Quality Assurance Plan
QASP	Quality Assurance Surveillance Plan
RBAC	Role based Access Control

Abbreviation	Full Text
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SaaS	Software as a service
SASE	Secure Access Service Edge
SDN	Software Defined Networking
SOC	Security Operations Centre
SOP	Standard Operating Procedure
SRE	Site Reliability Engineering
SSE	Secure Service Edge
STANAG	Standardisation Agreement
TDA	Technical Design Authority
UCaaS	unified communications as a service
VM	virtual machines
ZTNA	Zero Trust Network Access

BIDDERS PAST PERFORMANCE QUESTIONS

1. For each of the 3 (three) references listed below, Prospective Bidders are required to explain what aspects of the referenced contracts relate to the technical/management questions listed further down in this document.

2. Bidders are permitted to provide Annex B information related to contracts performed, within the last 6 (six) years from the date of issuance of this RFP and with a minimum of 12 (twelve) months performance period, by the Bidder and/or any sub-Contractor the Bidder proposes to use when performing the scope under competition through this RFP. In this case, Bidders shall submit in their RFP response a **formal joint statement or agreement**, signed by the Bidder and its 2 (two) proposed sub-Contractors named in this Annex B, confirming the Bidder, and its proposed sub-Contractors, irrevocably commit to maintaining the proposed cooperation arrangement, including related services/deliverables by the Prime Contractor or its sub-Contractors, throughout the entire competition and in case of award throughout contract performance. This commitment is a prerequisite for the Bidder advancing to subsequent stages in the selection process. Bidders shall be allowed to propose additional sub-Contractors at a later stage of the competition, up to and until completion of the RFP process and, in case of award, throughout contract performance.

3. **At least one of the 3 past performance contracts listed below shall be where the Bidder itself (and not any of its proposed sub-Contractors) was a Prime Contractor.** For the remaining 2 past performance contracts listed below, Bidders (and/or any Bidder's proposed sub-Contractor) are allowed to make reference to contracts performed by the Bidder (and/or any Bidder's proposed sub-Contractor) as a significant teaming partner or a significant sub-Contractor. The NCIA considers a significant teaming partner or a significant sub-Contractor to be a company which is able to demonstrate having:

   3.1. Provided 30% or more (based on the referenced contract monetary value) of the entire scope;

   3.2. Provided a critical portion of the effort required such as: CloudOps activities, including cloud-enabled workplace and landing zone management, Enterprise service integration and transformation.

4. Please review and answer each listed technical/management question addressed in this document, ensuring each answer provides valuable, appropriate content, matching the 3 (three) referenced contracts to the maximum extent practicable. **Any information filled in this Annex B shall be provided by the Bidder who will be ultimately responsible for its response to this RFP thus including any information the Bidder will present for any of its proposed sub-Contractor(s).**

5. When responding to Annex B; prospective Bidders shall therefore submit the following:

   5.1 An executive summary, elaborating on Bidder's overall expertise and capability to deliver project similar in scope, complexity and magnitude to the requirement competed in this RFP. The executive summary shall not-to-exceed overall 5,000 words;

5.2. Answers to the totality of all technical/management questions listed below with a content that shall not-to-exceed overall 10,000 words, covering the 3 (three) referenced contracts to the maximum extent practicable;

5.3. Documentation supporting answers to questions 1A, 3B and 6A;

5.4. The formal joint statement or agreement, as per Paragraph 2. above, if required.

5.5. Bidders shall note that submission of graphical drawings, illustrations, diagrams will not account for the total number of words of the Annex B response. Also Bidders shall note that while submission of the executive summary is mandatory requirement to achieve administrative compliance; information submitted by the Bidder in the executive summary will not be evaluated for the purpose of determining the Bidder's Overall Technical Score used by the NCIA for the RFP Step 1 down-selection process.

Referenced Contract Number 1:			
Customer (company name/Agency, Address:			
POC		Phone Number:	
Title:			
E-Mail Address:			
Contract Title, Scope:			
Contract No:/Type			
Contract POP(*):		(EUR) Contract Value:	
Does this referenced contract refer to the Bidder or to any of its proposed sub-Contractor?			
Was the referenced contract scope delivered in the role of a Prime or as sub-Contractor?			
If the referenced contract scope was not delivered in the role of a Prime, indicate % of the overall scope executed (monetary value)			
If the referenced contract scope was not delivered in the role of a Prime; was a critical portion of the required contractual effort provided? Briefly explain the support provided to deliver the entire scope			
(*) POP = Period of Performance			

Referenced Contract Number 2:			
Customer (company name/Agency, Address:			
POC		Phone Number:	
Title:			
E-Mail Address:			
Contract Title, Scope:			
Contract No:/Type			
Contract POP(*):		(EUR) Contract Value:	
Does this referenced contract refer to the Bidder or to any of its proposed sub-Contractor?			
Was the referenced contract scope delivered in the role of a Prime or as sub-Contractor?			
If the referenced contract scope was not delivered in the role of a Prime, indicate % of the overall scope executed (monetary value)			
If the referenced contract scope was not delivered in the role of a Prime; was a critical portion of the required contractual effort provided? Briefly explain the support provided to deliver the entire scope			
(*) POP = Period of Performance			

Referenced Contract Number 3:			
Customer (company name/Agency, Address:			
POC		Phone Number:	
Title:			
E-Mail Address:			
Contract Title, Scope:			
Contract No:/Type			
Contract POP(*):		(EUR) Contract Value:	
Does this referenced contract refer to the Bidder or to any of its proposed sub-Contractor?			
Was the referenced contract scope delivered in the role of a Prime or as sub-Contractor?			
If the referenced contract scope was not delivered in the role of a Prime, indicate % of the overall scope executed (monetary value)			
If the referenced contract scope was not delivered in the role of a Prime; was a critical portion of the required contractual effort provided? Briefly explain the support provided to deliver the entire scope			
(*) POP = Period of Performance			

EXECUTIVE SUMMARY:	
Word count for Executive Summary (not-to-exceed 5,000 words):	

TECHNICAL/MANAGERIAL QUESTIONS TO PROSPECTIVE BIDDERS:

QUESTION 1:	
Ability to Demonstrate Financial Strength and Similar Governance Delivery Experience at Corporate Level: 1A - **Management**) What is your global annual revenue at Corporate Level? Please also indicate the global annual revenue for public cloud IT transformation services (services designed to deliver transformational outcomes via the utilization of cloud-native professional and managed services, excluding CSP cloud consumption)? **Please demonstrate the declared global annual revenue and the global annual revenue for public cloud IT transformation services, leveraging an official attestation in the name of the Bidder**. The desirable level is expected to be above 4 BEUR (for the global annual revenue) and 1BEUR (for the portion of the global annual revenue related to public cloud IT transformation services). 1B - **Management**) Have you previously adopted and implemented a Cloud Operating Model, preferably for a national and/or multinational and/or governmental organisation, across people, project and technology? Please elaborate.	
Referenced Contract (FOR QUESTION 1B ONLY - indicate if applicable to 1 and/or 2 and/or 3 otherwise state "non-applicable"). If non-applicable, please provide the contact name/details of the previous customer for which the answer to this question does apply (to allow NCIA cross-check verifications):	
Write below your Answer to Question 1A: **Write below your Answer to Question 1B:**	
Word count for Answer to Question 1:	

QUESTION 2:	
Ability to Demonstrate Cloud Transformation Approach: 2A - **Technical**) Could you please elaborate on the level of automation and use of AI, such as the development of proven assets and methodologies in the areas of virtual agents, AI-assisted solutions for ongoing support, optimization and post migration services? 2B - **Management**) How does your company stay ahead of cloud technology trends, and how does your company incorporate them into the services that are provided to your customers? 2C - **Technical**) How did you leverage platform engineering principles when building and operating the cloud environment to version control, validate, manage and automate the provisioning of standardized cloud resources? 2D - **Technical**) How did you apply DevSecOps principles to reduce development cycles and speed up product releases while maintaining quality and security? Please elaborate. 2E - **Management**) How did you adopt digital engineering practices, drive modernization and transition change management for challenging customers geographically dispersed, with multiple governance structures, with possibly competing requirements, reluctant to change or operating as “silos”?	
Referenced Contract (FOR QUESTION 2C, 2D and 2E - indicate if applicable to 1 and/or 2 and/or 3 otherwise state “non-applicable”). If non-applicable, please provide the contact name/details of the previous customer for which the answer to this question does apply (to allow NCIA cross-check verifications):	
Write below your Answer to Question 2A: **Write below your Answer to Question 2B:** **Write below your Answer to Question 2C:** **Write below your Answer to Question 2D:** **Write below your Answer to Question 2E:**	
Word count for Answer to Question 2:	

QUESTION 3:	
Ability to Demonstrate Multicloud Capabilities: 3A - **Management**) Please describe your Company's organizational structure to support delivering multicloud capabilities such as dedicated business units for specific CCSPs[1] (for example: established highly integrated structure with specialized units for each CCSP with proven frameworks for inter-cloud collaboration)? 3B – **Technical**) What Managed Service Partner programs of the following 4 listed CCSPs (AWS Managed Service Provider Program, GCP Managed Services Provider initiative, Azure Expert MSP certification and Oracle MSS partner) is your Company part of? Please list all applicable affiliation and supplement your answer through **submission of copies of certifications or links to partner listings or evidence of advanced specializations or awards from the listed CCSPs**. Evidence of affiliation to at least 2 out of the 4 listed CCSPs is desirable. 3C - **Technical**) Which high-level selection criteria did you use for workload placement on the different CCSPs? Please describe examples of successful workload distribution across multiple CCSPs, including documentation of decision frameworks. 3D – **Management**) Have you previously developed a CCSP exit strategy and how did you prevent vendor lock-in? Please describe main drivers.	
Referenced Contract (FOR QUESTIONS 3C and 3D ONLY - indicate if applicable to 1 and/or 2 and/or 3 otherwise state "non-applicable"). If non-applicable, please provide the contact name/details of the previous customer for which the answer to this question does apply (to allow NCIA cross-check verifications):	
Write below your Answer to Question 3A: **Write below your Answer to Question 3B:** **Write below your Answer to Question 3C:** **Write below your Answer to Question 3D:**	
Word count for Answer to Question 3:	

[1] Cloud Service Providers (CSP) are defined as Commercial Cloud Service Providers (CCSPs) in the terminology adopted by the NATO Directive AC/322-D(2021)0032-REV1.

QUESTION 4:	
Demonstrating the Cloud Native Capability: 4A – **Technical**) How did you provide Cloud operational services emphasizing cloud-native concepts when designing infrastructure architectures and operational models, maximizing the benefit of the cloud? 4B – **Technical**): In the contracts previously performed, how did you handle service disruptions and ensure minimal downtime (i.e.: Disaster Recovery (DR) strategies, High Availability strategies)? What is your experience and level of confidence with disaster recovery and backup capabilities? Were you engaged in training and or live-exercises for DR? Please elaborate. 4C - **Technical**) Have you adopted a data-centric approach, detailing leveraged data governance models? Did you deal with different data classification levels? Please elaborate.	
Referenced Contract (indicate if applicable to 1 and/or 2 and/or 3 otherwise state "non-applicable"). If non-applicable, please provide the contact name/details of the previous customer for which the answer to this question does apply (to allow NCIA cross-check verifications):	
Write below your Answer to Question 4A: **Write below your Answer to Question 4B:** **Write below your Answer to Question 4C:**	
Word count for Answer to Question 4:	

QUESTION 5:	
Demonstrating the Cloud Financial Management Strategy: 5 – **Management**) Have you leveraged a specific Cloud Financial Management strategy, including FinOps models, tools and processes. How did you integrate with existing organizational financial management processes? Could you describe the main drivers / principles?	
Referenced Contract (indicate if applicable to 1 and/or 2 and/or 3 otherwise state "non-applicable"). If non-applicable, please provide the contact name/details of the previous customer for which the answer to this question does apply (to allow NCIA cross-check verifications):	
Write below your Answer to Question 5:	
Word count for Answer to Question 5:	

QUESTION 6:
Demonstrating the Cyber Security Compliance and Past Experience 6A - **Technical**) How do you ensure continuous compliance to industry-recognized security certifications and standards? (i.e. CSA, SOC2, ISO27000, C5, FedRAMP). What tools and processes did you use for performing automated compliance audits and continuous risk assessment? What experience do you have with independent security audits being performed? Please describe process including response to mitigation plans. Please supplement your answer through **submission of copies of certifications.** 6B - **Technical**) Which tools and processes did you leverage to proactively identify cybersecurity threats , improve anomaly detection, and response through use of automated security controls, AI, and machine learning? Please provide examples. 6C – **Management**) How did you demonstrate a successful working relationship with other entities responsible for security in a shared responsibility model (for example industry partners, security authorities, operational authorities, external incident responders, auditors)? Describe how your cybersecurity tools, processes, and training were integrated with those of external entities also responsible for security in a shared responsibility model. 6D – **Technical**) Have you been able to integrate the public cloud identity solutions with existing Enterprise Identity and Access Management functions? Did you achieve single sign-on and multi-factor authentication across multiple cloud and on-premise environments?
Referenced Contract (indicate if applicable to 1 and/or 2 and/or 3 otherwise state "non-applicable"). If non-applicable, please provide the contact name/details of the previous customer for which the answer to this question does apply (to allow NCIA cross-check verifications):
Write below your Answer to Question 6A: **Write below your Answer to Question 6B:** **Write below your Answer to Question 6C:** **Write below your Answer to Question 6D:**

Word count for Answer to Question 6:	

Word count overall for Answer to Questions 1 to 6 (not-to-exceed 10,000 words):	

I hereby declare that I have provided (3) three referenced contracts and I have addressed all questions listed above in this Annex B to the RFP CO-424219-PBN_0. The content of this Annex B is supplemented by the following:

- ☐ Documentation supporting answers to questions 1 A, 3 B and 6A (**mandatory**)
- ☐ Formal joint statement or agreement, signed by the Bidder and all of the Bidder's proposed sub-Contractors named in Annex B (**if required**)

Bidder's Name:	
Signature Date:	
Signature of Bidder's Authorized Representative:	
Printed Full Name:	
Title:	

Once filled in, the Bidder shall submit to the NCIA the Annex B documentation by the Bid Closing Date and time which is: **Monday, 26 May 2025, 15:00 hours Central European Summer Time (CEST):**

- without password protection and/or encryption
- using the following email address: **RFPCO424219PBN@ncia.nato.int**
- with email subject: ***Bidder's Company Name*–Annex B**
- using the file naming convention for the email attached Annex B documentation (one merged PDF file): **RFP-CO-424219PBN-*Bidder's Company Name*-Step1-Annex B**

PAST PERFORMANCE PACKAGE

CONSENT LETTER

TO: BIDDER'S (AND/OR BIDDER'S PROPOSED SUB-CONTRACTORS') CUSTOMERS

Dear Madam/Sir,

The NATO Communications and Information Agency (NCIA) is currently conducting the Request for Proposals (RFP) reference RFP-CO-424219-PBN_0 to select the Industry Service Integrator who will support the cloud operations functions required to establish and maintain the NATO Protected Business Network (PBN).

Services the Industry Service Integrator will be requested to provide include:

- **Commissioning Services** such as:
  - performance of an "as-is" assessment,
  - development of a "to-be" service model design and
  - implementation of the "to-be" service model.

  Operational Services such as**:**
  - Iaas and Paas Landing Zones management services,
  - Cloud Identity Access Management (IAM) services,
  - Cloud Enabled Workplace services,
  - Corporate Network Access services,
  - Cloud Cost Optimization services,
  - Cloud Platform Engineering services,
  - Service Management services,
  - Cyber Security services.

- **Transitional Services** such as**:**
  - Migration and Transformation Planning services,
  - Reach back and Reach Forward services.

A key consideration for proposal evaluation is the verification of the Bidders' (and/or of the Bidder's proposed sub-Contractors') past and present performance on contracts reflecting the ability to successfully and effectively perform the services that the Industry Service Integrator (and/or its proposed industry partners) will be called upon to deliver in case of contract award.

This questionnaire highlights the areas of interest to the NCIA. **Please submit your response to this questionnaire directly to the NCIA by no later than Monday, 26 May 2025, 15:00 hours Central European Summer Time (CEST) and using the following email address:**

RFPCO424219PBN@ncia.nato.int

IMPORTANT: Please do not send this questionnaire to the Bidder or to the Bidder's proposed sub-Contractor (for any of them to submit it to the NCIA on your behalf). **Once completed, you must send this questionnaire via email and directly to the NCIA**.

Please ensure this questionnaire is sent without password protection and/or encryption and that it includes the name of the firm being evaluated.

Your email to the NCIA:

- must have in the subject: ***Bidder's Company Name***–Past Performance Questionnaire

- must provide, in attachment, this questionnaire (once completed) using the following file naming convention: **RFP-CO-424219PBN-*Bidder's Company Name*-Step1-Annex C**

Once completed, this questionnaire is considered "Source Selection Sensitive Information" and it will be used to assess Bidder's technical compliance for the first step of the down-selection process envisaged by the NCIA in the aforementioned RFP.

Your participation in responding to this questionnaire is greatly appreciated.

The undersigned Bidder and, whether applicable, the undersigned Bidder's proposed sub-Contractor(s) (named below), do hereby authorize release of past performance information to the NCIA.

Sincerely,

Bidder's Name:	
Signature Date:	
Signature of Bidder's Authorized Representative:	
Printed Full Name:	
Title:	

IMPORTANT: The Bidder must ensure the following tables are completed if this questionnaire refers to any of its proposed sub-Contractor(s) named in the Annex B to the RFP:

Bidder's proposed sub-Contractor's Name:	
Signature Date:	
Signature of Bidder's proposed sub-Contractor's Authorized Representative:	
Printed Full Name:	
Title:	

Bidder's proposed sub-Contractor's Name:	
Signature Date:	
Signature of Bidder's proposed sub-Contractor's Authorized Representative:	
Printed Full Name:	
Title:	

PAST PERFORMANCE QUESTIONNAIRE RATING SHEET

RATING SCALE

Please use the following ratings to answer the questions. If you are unable to rate an item because it was not a requirement, never an issue, or you have no knowledge of the item in question, please mark "Non-Applicable". The term "Contractor" used below refers to the Bidder (or any Bidder's proposed sub-Contractor) you are evaluating by means of this Past Performance Questionnaire.

EVALUATION CRITERIA

ADJECTIVAL	DEFINITION
Excellent (E) **Score: 5**	The contractual performance exceeds or exceeded the contractual requirements. The requirement was accomplished with few minor issues for which the Contractor took corrective actions that were very effective.
Very Good (VG) **Score: 4**	The contractual performance of the element or sub-element being assessed was accomplished with some minor problems for which corrective actions taken by the Contractor was effective.
Satisfactory (S) **Score: 3**	The contractual performance of the element or sub-element being assessed contained some minor problems for which corrective actions taken by the Contractor appear or were satisfactory.
Marginal (M) **Score: 2**	The contractual performance of the element or sub-element being assessed reflects a serious problem for which the Contractor has not yet identified corrective actions. The Contractor's proposed actions appear only marginally effective or were not fully implemented.
Unsatisfactory (U) **Score: 0**	Performance does not or did not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance of the element or sub-element contains serious problem(s) for which the Contractor's corrective actions appear or were ineffective.
Not Applicable (N/A) **No Score. Not included in the total score.**	Unable to provide any score.

NOTE: When indicating an "Unsatisfactory" rating, please provide a brief explanation in the comments section of the questionnaire referencing the question number.

PAST PERFORMANCE QUESTIONNAIRE

SECTION I: CONTRACT IDENTIFICATION **(Only this SECTION I is to be filled out by the Bidder)**	
1. BIDDER'S (OR BIDDER'S PROPOSED SUB-CONTRACTOR'S) CUSTOMER NAME AND ADDRESS:	
2. CONTRACT NUMBER:	3. AWARD ENVIRONMENT: ☐ COMPETITIVE ☐ NON-COMPETITIVE ☐ SOLE SOURCE
4. CONTRACT TYPE: ☐ FIRM FIXED PRICE ☐ FIXED PRICE + FEE ☐ COST or COST SHARING ☐ COST + FEE ☐ LABOR HOUR ☐ TIME & MATERIALS ☐ OTHER _____	5. PERIOD OF PERFORMANCE (including options):
6. INITIAL CONTRACT VALUE (including options):	7. CURRENT/FINAL CONTRACT VALUE (including options):
8. REASONS FOR DIFFERENCES BETWEEN INITIAL CONTRACT VALUE AND FINAL CONTRACT VALUE:	
9. DESCRIPTION OF PRODUCTS/SERVICE PROVIDED:	10. LOCATION SERVICES PROVIDED (local, worldwide, etc.):

SECTION II. EVALUATOR AND COMPANY/AGENCY IDENTIFICATION (This SECTION II is to be filled out by the Bidder's Customer or the Bidder's proposed sub-Contractor's Customer)	
1. COMPANY or AGENCY (BIDDER'S OR BIDDER'S PROPOSED SUB-CONTRACTOR'S CUSTOMER NAME):	2. EVALUATOR NAME & TITLE:
3. EVALUATOR CONTACT INFORMATION: TEL NO.: E-MAIL:	4. NUMBER OF YEARS EVALUATOR WORKED ON SUBJECT CONTRACT:

	E	**VG**	**S**	**M**	**U**	**N/A**
MANAGEMENT						
1. Has the Contractor assisted your organization in adopting a Cloud Operating Model? Please describe your level of satisfaction with their support in this area. **Please do rating taking into account also the narrative answer per question # A below.**	☐	☐	☐	☐	☐	☐
2. Did the Contractor effectively support your organization's adoption process through training and mentoring? Please indicate your level of satisfaction with their support in this area.	☐	☐	☐	☐	☐	☐
3. Has the Contractor provided effective support for your enterprise-level change management initiatives? Please indicate your level of satisfaction with their performance in this area.	☐	☐	☐	☐	☐	☐
4. Has the Contractor utilized industry-standard methodologies for planning and implementing cloud changes? How satisfied were you with the agility and responsiveness of their approach?	☐	☐	☐	☐	☐	☐
5. Did the Contractor deliver a cloud service provider exit strategy as part of the contracted effort? Please rate the effectiveness and efficiency of this strategy.	☐	☐	☐	☐	☐	☐

	E	VG	S	M	U	N/A
TECHNICAL						
6. Has the Contractor successfully executed the Operations & Maintenance tasks for your technical solution? Please indicate your level of satisfaction with their performance in this area.	☐	☐	☐	☐	☐	☐
7. Did the Contractor demonstrate the capability to effectively manage landing zones? Please indicate your level of satisfaction with their performance in this regard.	☐	☐	☐	☐	☐	☐
8. Was the Contractor able to successfully achieve seamless single sign-on (SSO) and multi-factor authentication (MFA) across multiple cloud and on-premise environments? If so, please indicate your level of satisfaction with their performance in this area.	☐	☐	☐	☐	☐	☐
9. Did the Contractor apply platform engineering principles when building and operating the cloud environment, including version control, validation, management, and automation of standardized cloud resource provisioning? Please indicate your level of satisfaction with their approach in this area.	☐	☐	☐	☐	☐	☐
10. What is your level of confidence in the Contractor's implemented solution for Disaster Recovery, including the backup strategy, in terms of service restoration?	☐	☐	☐	☐	☐	☐
11. Has the Contractor demonstrated the ability to proactively identify cybersecurity threats and implement effective mitigations? Additionally, has the Contractor been able to detect, respond to, and adapt to emerging and zero-day threats? **Please do rating taking into account also the narrative answer per question # B below.**	☐	☐	☐	☐	☐	☐
12. Did the Contractor demonstrate the ability to comply with applicable laws, rules, and regulations during the performance of the contract (e.g., in relation to security standards such as CSA, SOC2, ISO27000, C5, FedRAMP)? Please indicate your level of satisfaction with their compliance efforts.						

A. With reference to Question #1 above, please provide a high-level description of the processes and procedures that define your Cloud Operating Model. How did the Contractor contribute to the adoption of this model? Additionally, is there a clear delineation of roles and responsibilities between your organization and the Contractor?

B. With reference to Question #11 above, please describe how the Contractor has supported you to implement proactive cyber security threat detection and mitigation strategies.

C. Please provide a brief description of the organizational structure employed by the Contractor in relation to the referenced Contract. Did the Contractor utilize best-in-class resources to address specific challenges (e.g., Cyber Security, FinOps, Service Management) through alliances, sub-Contractors, or other means?

D. How many end-users did the Contractor support under the referenced contract? Additionally, what was your total average monthly cloud consumption cost?

E. If you have indicated an 'Unsatisfactory' rating for any of the questions above, please provide a brief explanation in the comments section below, referencing the corresponding question number:

Evaluator's Signature:	
Full Name, Title:	
Date:	

NATO Communications and Information Agency

RFP STEP 1 EVALUATION CRITERIA AND METHODOLOGY

1. Prior to conduct RFP Step 1 evaluation, the NCIA will first verify timely submission and completeness of any received RFP Step 1 response. These activities will also include verification of Past Performance information recency. These verifications may also result in the NCIA submitting clarification requests to Bidders, as/if required. The table below summarizes the administrative (pass/fail) compliance verifications the NCIA will conduct to assess Bidders' RFP Step 1 responses:

RFP-CO-424219-PBN_0 - Step 1 Administrative Compliance Verifications (Pass/Fail):	
Question	**RFP reference(s)**
Has the RFP response for Step 1 been received by the NCIA on time?	Paragraph 12.20.
Has the RFP response for Step 1 been received by the NCIA in its entirety? Does the submission comply with the instructions to Bidders provided in the RFP?	Paragraphs 12.5., 12.6., 12.7., 12.9., 12.10., 12.11., 12.12., 12.13., 12.14., 12.15., 12.16., 12.17., and 12.19.
Is the **Power of Attorney** (if any submitted by the Bidder) compliant with the RFP provisions? Does it give evidence of Bidder's authority to act on behalf of its proposed consortium?	Paragraph 7
Is the **Formal Joint Statement** (if any submitted by the Bidder) compliant with the RFP provisions? Does it give evidence of irrevocable Bidder's commitment to maintain the proposed cooperation arrangement, including related services/deliverables by the Prime Contractor or its sub-Contractors, throughout the entire RFP competition up to and until completion of the RFP process and in case of award?	Paragraph 12.2.
Does the **official attestation** supporting Bidder's Annex B response demonstrate the declared global annual revenue and the global annual revenue for public cloud IT transformation services (in response to Annex B, Question 1A)?	Paragraph 12.7.3.
Do the **certifications or links** provided by the Bidder as part of its Annex B response give evidence of its partner listings or evidence of advanced specializations or awards from Commercial Cloud Service Providers (in response to Annex B, Question 3B)?	Paragraph 12.7.4.
Do the copies of **certifications** provided by the Bidder as part of its Annex B response give evidence of its continuous compliance to industry-recognized security certification and standards (in response to Annex B, Question 6A)?	Paragraph 12.7.5.

2. At conclusion of the administrative compliance verifications and only for those Bidders who will have successfully passed these verifications, the NCIA will:

   a) numerically score, on a scale from 0 to 5, the Technical and Management questions answered by the Bidder in the Annex B response, including the supporting documentation and certifications received by the Bidder as part of the Annex B submission (for questions 1A, 3B and 6A);

   b) numerically score, on a scale from 0 to 5, the Bidder's Customer's (or the Bidder's proposed sub-Contractor's Customer's) answers to Questions A, B, C and D from the 3 (three) received Annexes C (one per each contract referenced in Annex B).

The above raw scoring will be based on the following rating scale:

ADJECTIVAL	DEFINITION
Excellent **Score: 5**	Past performance information (and any supporting documentation, as applicable) is highly comprehensive, exhaustive and supports excellent record of successful past performance and competence. This is an indication of the ability to significantly exceed the contractual requirements described in this solicitation. Bidder's declared global annual revenue at Corporate level to include the specific revenue for Cloud IT transformation services exceed the desirable values indicated in this solicitation.
Very Good **Score: 4**	Past performance information (and any supporting documentation, as applicable) is strongly supported by a detailed and clear elaboration of the questions. Answer to questions demonstrate proactive, data-driven, strategic thinking approach thus providing evidence of very good record of successful past performance and competence.
Good **Score: 3**	Past performance information (and any supporting documentation, as applicable) is well structured and it sufficiently demonstrates an acceptable level of technical knowledge and competence. Bidder's declared global annual revenue at Corporate level to include specific revenue for Cloud IT transformation services meets the desirable values indicated in this solicitation.
Fair **Score: 2**	Past performance information (and any supporting documentation, as applicable) is still considerable acceptable however it is basic in its elaboration and it fairly addresses the content of questions with some noticed lack of details and incomplete answers. This translates into a fair level of technical knowledge and competence.
Poor **Score: 1**	Past performance information (and any supporting documentation, as applicable) is below acceptable levels due to unclear, incomplete elaboration/analysis, resulting in insufficient response. This translates into a insufficient level of technical knowledge and competence. Bidder's declared global annual revenue at Corporate level to include specific revenue for Cloud IT transformation services is below the desirable values indicated in this solicitation.
Unsatisfactory/No evidence **Score: 0**	Past performance information (and any supporting documentation, as applicable) is either missing or highlights serious concerns on the quality and/or correctness of information provided. This translates into an unacceptable technical knowledge and competence.

c) add raw scores assigned by the Bidder's Customer (or the Bidder's proposed sub-Contractor's Customer) to the questions addressed in the 3 (three) received Annexes C (one per each contract referenced in Annex B).

3. Once each Technical and Management question from Annexes B and C has been scored, evaluation score per Bidder and per Annex will then be calculated as follows:

a) **Annex B weighted score calculation**:

1. For each category of question (Management and Technical), a sub-score expressed as a percentage of the maximum score per category will be calculated (these sub-scores named: ***AnB_Man*** and ***AnB_Tech***);

a. Sub-score for each category of question residing below 60%, may lead to the Bidder being declared as non-compliant;

2. Final score (***AnB_FS***) calculation for Annex B:

a. ***AnB_FS*** = ***AnB_Tech*** x ***AnB_TW*** + ***AnB_Man*** x ***AnB_MW***

where ***AnB_TW*** and ***AnB_MW*** are the associated weights (as per table below):

RFP Annex B	=	Management	AnB_MW	50%
		Technical	AnB_TW	50%

b) Annex C weighted score calculation:

1. For each category of question (Management and Technical), an average (amongst the 3 received Past Performance Questionnaires) sub-score expressed as a percentage of the maximum score per category will be calculated (these sub-scores named: ***AnC_Man*** and ***AnC_Tech***);

a. Sub-score for each category of question residing below 60%, may lead to the Bidder being declared as non-compliant;

2. Final score (***AnC_FS***) calculation for Annex C:

a. ***AnC_FS*** = ***AnC_Tech*** x ***AnC_TW*** + ***AnC_Man*** x ***AnC_MW***

where ***AnC_TW*** and ***AnC_MW*** are the associated weights (as per table below):

RFP Annex C	=	Management	AnC_MW	50%
		Technical	AnC_TW	50%

4. Bidders shall note that the NCIA will finally apply a relative weight of Annex B (in total) and Annex C (in total) in order to determine each Bidder's Overall Technical Score (***Step1_FS***). This final relative weight is not known to any of the NCIA staff beyond the originator and the Chairperson of the Contracts Award Board. This relative weight remains sealed until the RFP Step 1 responses evaluation is completed and are referred as to as: ***AnB_SealedW*** (Annex B sealed weight) and ***AnC_SealedW*** (Annex C sealed weight). Final score (***Step1_FS***) will be calculated as follows:

Step1_FS = ***AnB_FS*** x ***AnB_SealedW*** + ***AnC_FS*** x ***AnC_SealedW***

5. A notional example of the evaluation score calculation is given in table below where ***AnB_SealedW*** and ***AnC_SealedW*** are respectively sealed weights for Annex B and C as per paragraph above:

	Non weighted Score	Weight	Weighted score	-
AnB_Man	80%	50%	40.0%	
AnB_Tech	80%	50%	40.0%	
AnB_FS				**80%**
AnC_Man	80%	50%	40.0%	
AnC_Tech	80%	50%	40.0%	
AnC_FS				**80%**
Step1_FS				AnB_FS_% x AnB_sealedW + AnC_FS_% x AnC_sealedW

6. A statistical tie is deemed to exist when the Overall Technical Score are within one percent (1 %) of each other. For example, an Overall Technical Score of 60.30% and 61.31% are more than one point apart and would not be considered a statistical tie. On the contrary, Overall Technical Scores of 60.30% and 61.30% are within one point of each other and would therefore be considered a statistical tie. The NCIA will then resolve the statistical tie between the 5th and the 6th highest ranked Bidders using the following tie-breaking procedure in order to achieve the objective of down-selecting, at completion of the RFP Step 1, a total of up to 5 Bidders:

    a) The total weighed score achieved on the Annex B responses assessment will be considered first;

    b) If ties persist, the total weighted score achieved for Annex C will be considered second.

7. Only the top 5 (five) highest ranked Bidders having achieved the top 5 (five) highest Overall Technical Score will then proceed to Step 2. Without commitment from the NCIA's end; it is estimated that Step 1 procedures will be completed during Q2 2025 and that in same Q2 2025 the NCIA will release Step 2 information to Bidders deemed eligible to receive it.