

Amendment 2 to Notification of Intent to Invite Bids

Method: International Competitive Bidding (ICB)

NR Business Network Services

NCI Agency Reference: IFB-CO-115891-REACH

Estimated Amount: EUR 45,000,000 Including Optional Years

PERIOD OF PERFORMANCE: 3 BASE YEARS + 2
OPTION YEARS

NOI Closing Date: 4 April 2024

Solicitation Release Date: Anticipated on Q2 2024

Solicitation Closing Date: Anticipated on Q2 2024

Contract Award Date: Anticipated on Q3 2024

Competition Type: ICB Best Value

NCI Agency Point of Contact
Diana Nedelea, Contracting Officer

Email: IFB-CO-115891@ncia.nato.int

Annexes:

- A. Summary of Requirements
- B. Distribution List

To : Distribution List

Subject : **Amendment 2 to Notification of Intent to Invite International Competitive Bids for NR Business Network Outsourcing - Corrigendum**

Reference(s) A. AC/337-D(2016)0014 dated 16 March 2016
B. BC-D(2018)0004-FINAL dated 29 January 2018
C. BC-D(2019)0129-ADD2 (INV) dated 9 July 2019
D. NCIA/ACQ/2023/0638 dated 22 May 2023
E. NCIA/ACQ/2023/06929 dated 02 June 2023

1. In accordance with References A through E, notice is hereby given of the intent of the NATO Communications and Information Agency (NCI Agency), acting as Host Nation responsible of implementing the subject requirement, to issue an Invitation for Bid (IFB) for the procurement of NR Business Network Outsourcing, hereafter referred to as the "Project".
2. The NATO Communications & Information Agency (NCI Agency) intends to modernise existing NR Business Network services through outsourcing back-end infrastructure as Infrastructure-as-a-Service (IaaS) and front-end client services as Device-as-a-Service NR Business Network back-end infrastructure includes compute, storage and networking elements. Service provision will include agreed availability target set forth in Service Contract and respective SLAs. Front-end managed mobile devices are required to support parallel working in different security domains.
3. A summary of the requirements for this Project is set forth in Annex A hereto. These requirements are being refined and will be included in further details as part of the IFB.
4. The reference for this Project is **IFB-CO-115891-REACH**, and all correspondence concerning this NOI and subsequent IFB should reference this number.
5. The estimated investment cost for the services and deliverables included within the basic scope of the intended contract is not to exceed 45,000,000 EUR over five years comprising a three (3) years base contract and two (2) contract options of one (1) year each.
6. The NCI Agency plans to issue a IFB using the International Competitive Bidding (ICB) Procedure for Best Value (BV) evaluations. The successful bid for this Project, pursuant to the IFB following this NOI, will be the bid that offers the best value in accordance with predefined evaluation criteria prescribed in the IFB. The top-level criteria weighting will be 60% Technical and 40% Price. A single, firm-fixed price contract is planned for the entire scope of work.
7. Eligibility to participate in the subsequent IFB is declared by national authorities. Hence, qualified and certified companies interested in receiving the IFB for this Project are hereby requested to provide a Declaration of Eligibility (DoE), **sent** by their Delegation/Mission to NATO to the NCI Agency contracting authority **not later than 4 April 2024**, which is 28 calendar days after the date of this letter.
 - a. In addition to the certification of the company's security clearances required under this NOI, the DoE should include the following information for each of the nominated companies:

NATO UNCLASSIFIED Releasable to Public

- Company name
 - Company address
 - Point of Contact (PoC)
 - PoC email address
 - PoC telephone number
- b. This information is critical to enable prompt and accurate communication with prospective bidders and should be sent electronically to IFB-CO-115891@ncia.nato.int.
8. In order to maximize competition the NCI Agency may, at its discretion, accept nominations after the deadline, so long as the IFB has not been issued. The NCI Agency may even accept, at its discretion, nominations after the IFB has been issued under the condition that such late nomination will not be used as the basis to request an extension to the bid closing date.
9. Requests for participation in this competition received directly from individual firms cannot be considered.
10. Bidders will be required to declare a bid validity of 12 (twelve) months from bid closing date. Should the selection and award procedure exceed the bid closing date by more than 12 [twelve] months, companies will be requested to voluntarily extend the validity of their bids accordingly. Bidders may decline to do so, withdraw their bid and excuse themselves from the bidding process without penalty.
11. National authorities are advised that the IFB package is anticipated to be NATO UNCLASSIFIED.
12. The successful bidder will be required to handle and store classified information up to the level of NATO RESTRICTED. In addition, contractor personnel will be required to work unescorted in Class II Security areas. Therefore, access can only be permitted to cleared individuals. Only companies maintaining such cleared facilities and the appropriate personnel clearances will be able to perform the resulting contract.
13. Prior to the issuance of the IFB package, the NCI Agency is planning to conduct an **Industry Day** with the identified potential bidders on the **15th of March 2024**. Further details will be sent by email.
14. The NCI Agency is not liable for any expenses incurred by companies in conjunction with their responses to this NOI and such responses shall not be regarded as a commitment of any kind concerning future procurement of the items or services described herein.
15. Your assistance in this procurement is greatly appreciated.

For the Chief of Acquisition:

Diana Nedelea
Contracting Officer

Annex A – Summary of Requirements



NR BUSINESS NETWORK (REACH) SERVICES OUTSOURCING

HIGH LEVEL SCOPE

TABLE OF CONTENTS

1.	OUTSOURCING OF NR BUSINESS NETWORK SERVICES.....	7
1.1.	Problem Definition	7
1.1.1.	Overview	7
1.1.2.	Problem Statement.....	7
1.1.2.1.	Infrastructure	7
1.1.2.1.1.	Obsolescence	7
1.1.2.1.2.	Space and Capacity	7
1.1.2.2.	End User Devices (Laptops, Tablets, Smartphones)	7
1.2.	Goal and expected outcome.....	7
1.3.	Key success factors	8
1.3.1.	Key Success Factors.....	8
1.3.2.	Operational Acceptance Criteria.....	8
1.4.	High Level Outsourced Scope Description	8
1.4.1.	Overall Description	8
1.4.1.1.	Contractor Deliverables	8
1.4.1.1.1.	Infrastructure-as-a-Service (IaaS) and Device-as-a-Service (DaaS)	8
1.4.1.1.1.1.	Phase 1 – Discovery & Planning	8
1.4.1.1.1.2.	Phase 2 – Build	9
1.4.1.1.1.3.	Phase 3 – Transition	10
1.4.1.1.1.4.	Phase 4 – Operations.....	10
1.4.1.1.2.	General Services.....	11
1.4.1.2.	Constraints	12
1.4.1.2.1.	General constraints applicable to all contract	12
1.4.1.2.2.	IaaS.....	12
1.4.1.2.3.	DaaS	12
1.4.1.3.	General Services.....	13
1.4.2.	The Contractor / The Purchaser responsibility sharing	13
1.5.	Overall Implementation Plan	16
1.5.1.	Project Milestones	16
1.5.2.	High level implementation strategy.....	16
1.5.3.	High level plan for integration in enterprise and capability architecture	16
1.5.4.	High level security accreditation plan	17

1. OUTSOURCING OF NR BUSINESS NETWORK SERVICES

1.1. Problem Definition

1.1.1. Overview

The NCI Agency currently operates its main NATO Restricted Business Network (known as REACH) in five main campuses, 15 CSU locations and including three data centres across NATO countries.

The equipment obsolescence, capacity and compatibility issues are constant challenges that REACH is facing. Simultaneously, the usage of the REACH have increased significantly, driven by greater post-COVID mobility, the new international security situation, and a growth in staff and usage.

In order to support growing demand for its services, The NCI Agency is outsourcing its commodity IT services, of which this is one. This work will be outsourced as a managed service.

1.1.2. Problem Statement

1.1.2.1. Infrastructure

1.1.2.1.1. Obsolescence

Within the calendar year 2024, significant portion of the backend infrastructure will be considered obsolete. This includes but is not limited to servers, storage, routers and firewalls.

1.1.2.1.2. Space and Capacity

The NCI Agency's business network REACH capability was designed and delivered in 2017 and sized to support 4500 client devices. Currently, there are approximately 6000+ clients supported by the REACH network, making it no longer able to effectively meet current or future projected growth.

1.1.2.2. End User Devices (Laptops, Tablets, Smartphones)

The current, single-domain (exclusively NR or exclusively NU) end user devices don't meet our current and future business needs, which are calling for multi-domain collaboration capabilities (NR, NU, Internet) on a single end user device.

One identified major business requirement would be to improve our collaboration capabilities (for example being able to use: MS Teams, CISCO WebEx, etc.) across NR and NATO Unclassified (NU) networks with partners (OCIO, Industry, ACO, ACT, etc.).

We also suffer from a lack of coherent approach to the enterprise delivery of end-user devices.

1.2. Goal and expected outcome

The goals of this competition are;

- To replace the current on-premise infrastructure capabilities (processing, storage, backup, networking, security and virtualization) with an off-premise accredited cloud and outsource the management to the industry partner.

- To replace the current end user devices with state of art end user device solution that offers desired internet/NU/NR collaboration capabilities on a single device and to outsource the device management to an industry partner.

The final outcome to be a fully managed service contract delivering Infrastructure as a Service (IaaS) on an accredited cloud and End User Devices (Device as a Service-DaaS) with complete performance metrics and service level agreements to ensure delivery of a quality and stable service.

1.3. Key success factors

1.3.1. Key Success Factors

- Consistency, stability in service delivery,
- Delivery of multi domain capable end user device solution which ensures collaboration on internet/NU/NR,
- Removal of obsolete equipment on our network, and prevent any obsolescence in the duration of the contract,
- Improved end user satisfaction,
- Obsolescence and technology refreshment handled as part of service cost (move from CAPEX to OPEX)
- Elastic IaaS that can grow and sharing on demand with no major implementation timelines,
- Clear and accountable Service Level Agreements,
- Clear and accountable performance metrics.

1.3.2. Operational Acceptance Criteria

Operational acceptance criteria are directly correlated to the contractor service deliverables listed in Section 1.4.1.1.

1.4. High Level Outsourced Scope Description

1.4.1. Overall Description

1.4.1.1. Contractor Deliverables

All deliverables listed are subject to the constraints below in terms of security and other elements.

1.4.1.1.1. Infrastructure-as-a-Service (IaaS) and Device-as-a-Service (DaaS)

1.4.1.1.1.1. Phase 1 – Discovery & Planning

The Contractor SHALL determine/verify current capacity and needs through methods defined by the Contractor with the assistance of the Purchaser where required.

The Contractor SHALL determine future growth needs of the Agency to ensure the necessary capacity is installed and available for the period of performance for this contract. Monitoring the network capacity and growth will be part of the SLA.

The Contractor SHALL provide IaaS and DaaS capabilities that will allow Purchaser staff to be able to work remotely, day to day capacity should be sized to support up to 70% of staff working remotely on a day to day basis, but it should also provide the ability to scale up for 100% of staff working remotely in the event of a crisis situation.

The Contractor SHALL, based on SOW-0001/SOW-0002/SOW-0003, provide a suitable Build and Transition Plan, including a quality assurance plan as part of the transition.

1.4.1.1.1.2. Phase 2 – Build

The Contractor SHALL deliver IaaS services with the latest technologies and innovation IaaS SHALL be deployed on an NR accredited cloud solution. Proposed clouds must already be at NATO NR . Accreditation package preparation and submittal are a part of this procurement

The Contractor SHALL provide high speed connectivity between cloud location and, initially, the five key NCI Agency locations (The Hague, Mons, Oeiras, Braine l'Alleud and Brussels).

The Contractor SHALL ensure/upgrade network bandwidth to meet operating requirements.

The Contractor SHALL upgrade existing Wi-Fi capabilities (if deemed necessary) at, initially, the five key NCI Agency locations to ensure maximum throughput across the network.

The Contractor SHALL provide encryption of all data at rest through the use of NATO issued PKI keys.

The Contractor SHALL provide hypervisor infrastructure.

The Contractor SHALL provide a block-level infrastructure backup solution.

The Contractor SHALL provide centrally managed DaaS solution integrated with IaaS.

The Contractor SHALL provide an implementation plan for regular patching, including reporting on the status of patching. The Contractor SHALL execute patching.

The Contractor SHALL provide end user device provisioning procedures and remote support capabilities for all Agency locations including the five NCI Agency primary locations and all additional satellite offices.

The Contractor SHALL develop and execute a strategic communications campaign to inform the Agency staff of the plan and process of this major change project. This includes but is not limited to using Agency communication channels and developing messaging and graphics.

The Contractor SHALL develop the full Security Accreditation package for submittal to NATO Office of Security and support a stakeholder management approach with NOS to ensure the elements of the SAP are known and understood by NOS.

1.4.1.1.1.3. Phase 3 – Transition

The Contractor SHALL provide a transition plan to address all phases of the contract, training, delivery, deployment and quality assurance, according to industry standards.

The Contractor SHALL provide all deliverables being in compliance with the appropriate NATO standards in relation to, but not limited to: security/patching/cyber security etc.

The Contractor SHALL provide all necessary instructional materials for the proposed solution, for end-users/technicians and administrators.

The Contractor SHALL execute the transition plan together with the Purchaser, and demonstrate to the Purchasers satisfaction that services are delivered and ready for operation as per service-requirements.

The Contractor SHALL deliver NATO-accredited end-user devices, which allow end users to work across multiple different network security levels (Internet/NU/NR).

1.4.1.1.1.4. Phase 4 – Operations

The Contractor SHALL provide secure device-disposal services in accordance with NATO standards for disposal of equipment and data [AC/322-D(2012)0011, AC/322-D(2012)0012]

The Contractor SHALL provide continuous monitoring and re-scaling of the solution on a regular basis with agreement of the Purchaser as per Service Level Agreement (SLA) term.

The Contractor SHALL provide needed rescaling of IaaS and DaaS on demand.

The Contractor SHALL provide clear and concise costing model/calculator for expanding IaaS and DaaS.

The Contractor SHALL provide immutable storage capabilities to protect against ransomware attacks on backups.

The Contractor SHALL provide a patching services.

The Contractor SHALL replace obsolete infrastructure and end user devices to ensure no obsolete equipment remains in operation on NATO networks as per NATO directive

The Contractor SHALL provide an asset management capability for DaaS assets: tag each device in order to ensure full accountability and traceability, in accordance with the NCI Agency regulations and in coordination with the CIS Sustainment Support Centre (CSSC) [AD 06.00.15 and SOP 09.02]

The Contractor SHALL deploy the Purchaser's delivered baseline images onto all DaaS devices.

The Contractor SHALL provide an advisory and optimization service to work with the Purchaser to ensure that any base images used for end user devices is optimized for both performance and deployment.

1.4.1.1.2. General Services

The Contractor SHALL manage service and incident tickets to meet agreed SLAs (Contractor shall either use the existing Purchaser provided IT Service Management (ITSM) system, or use their own).

Contractor SHALL support the NCI Agency's Business Change Management Office on Strategic Communication (StratCom) with appropriate material.

The Contractor SHALL provide Project Management Plan in keeping with PRINCE2 or equivalent industry standard project management methodology deemed efficient for this effort as long as there is a single POC for the project.

The Contractor SHALL provide, in consultation with the Purchaser an exit strategy in the event it is necessary for either the Contractor or the Purchaser to terminate the contract agreement.

1.4.1.2. Constraints

1.4.1.2.1. General constraints applicable to all contract

These constraints applicable to IaaS, DaaS and general services.

The Contractor SHALL ensure all Purchaser data at rest & in transit must be encrypted using NATO Public Key Infrastructure (PKI) keys.

The Contractor SHALL provide services to ensure that there is Data Loss Prevention and Anti-malware tools to protect the network – on persistent basis and also at all network boundaries and interactions with other security domains within NATO.

The Contractor SHALL ensure all Purchaser data must be hosted within NATO nations – both primary and secondary sites.

The Contractor SHALL ensure all hardware and components are from NATO nations only.

The Contractor SHALL ensure all personnel working on the contract must be citizens of a NATO country only.

The Contractor SHALL ensure all personnel who might have access to NATO data or NATO facilities must have security clearance.

1.4.1.2.2. IaaS

The Contractor SHALL ensure the cloud infrastructure allocated to this contract must be accredited up to NATO Restricted level.

1.4.1.2.3. DaaS

The Contractor SHALL ensure management of CIS for DaaS must be accredited up to NATO Restricted level.

The Contractor SHALL ensure no end-user device shall be older than 4 years.

The Contractor SHALL ensure secure disposal of obsolete/unusable devices and peripherals in accordance with NATO regulations.

The Contractor SHALL ensure all devices must be provided with multi-factor authentication.

1.4.1.3. General Services

If the Contractor decides to use their own ITSM toolset to manage service requests and incidents, and this is accepted by the Purchaser, the Contractor SHALL ensure a seamless integration with the Purchaser's ITSM system so that the end user only has a single point of entry.

1.4.2. The Contractor / The Purchaser responsibility sharing

The diagram below outlines initial assessment of the division of responsibility within this contract including shared responsibility. These responsibilities may be adapted/updated during Phase 1 of the project to ensure both Contractor and Purchasers needs are met in accordance with Service Level Agreements and also ensuring compliance with NATO regulations/directives.

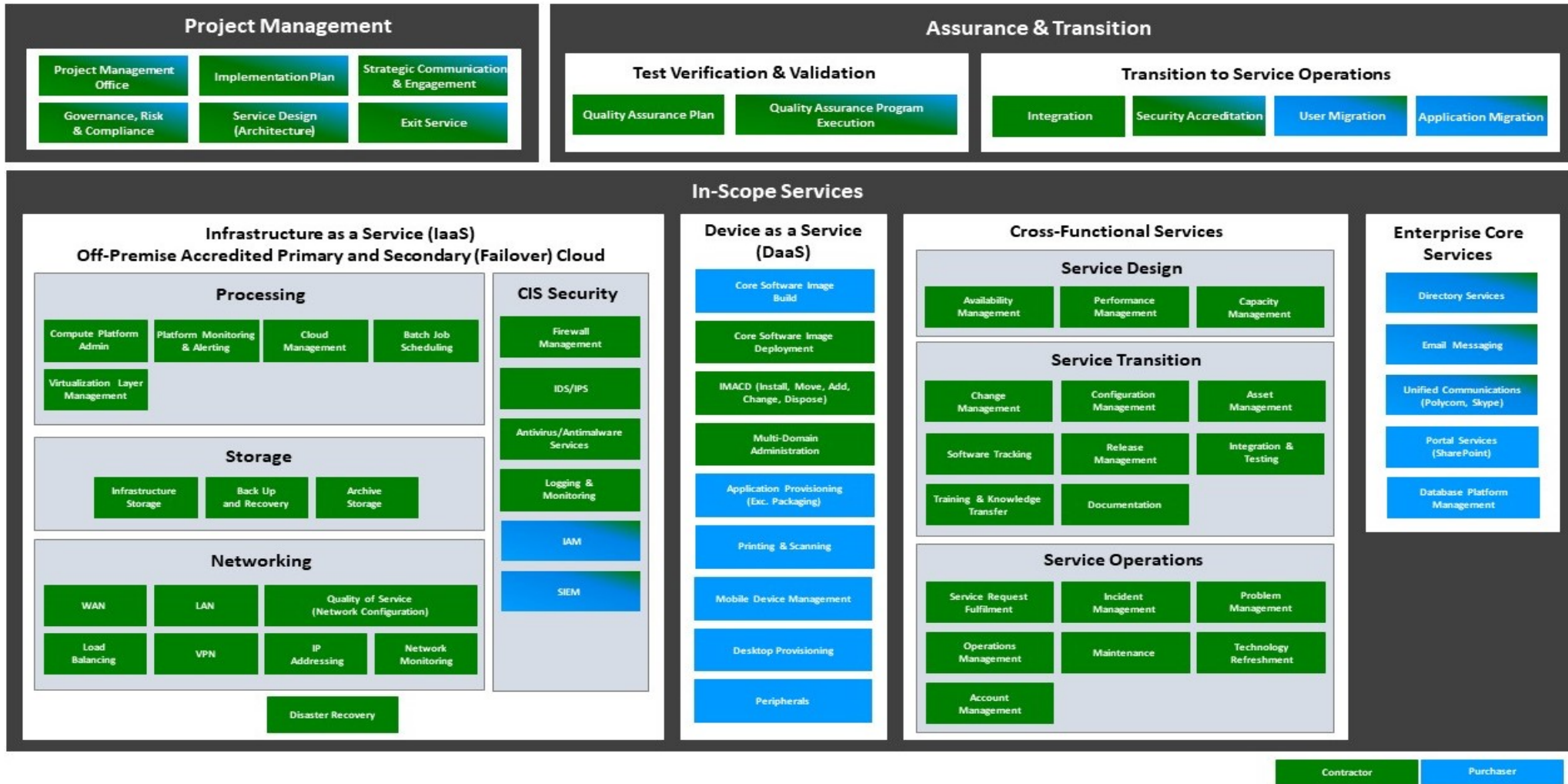


Figure 1 - NR Business Network Future Service Model

1.5. Overall Implementation Plan

1.5.1. Project Milestones

The delivery timelines for the project will be ambitious and the Contractor shall make every effort necessary to avoid delays in execution of the Contract. The phases and delivery milestones of the project are reflected in below table. The Effective Date of Contract (EDC) will be established at the time of Contract Award.

Milestone	Delivery Date
MS1 - Discovery & Planning	EDC + 4 Months
MS2 - Build	MS1 + 3 Months
MS3 - Transition	MS2 + 3 Months
MS4 - Operations	MS3 + 3 Months
MS5 - Final Operating Capability	MS4 + 6 Months

Table 1 - Milestones

1.5.2. High level implementation strategy

Phase 1 Discovery & Planning – In this phase the expectation is for the Contractor to work with the Agency to complete site surveys as needed to establish the current capacity and needs of the current REACH service, as well as establish short to medium term requirements to enable the Contractor to correctly size their offering. The primary deliverables from this phase will be a Build plan to meet the capacity needs, in addition to a Transition plan for moving the Agency’s IT assets into the new service.

Phase 2 Build – This phase is about implementing the above mentioned build plan – key part of this phase will be quality assurance and testing to ensure build is fit for purpose prior to initiating the transition plan.

Phase 3 Transition – This phase involves transitioning the Agency’s IT assets from existing ecosystem into the new Contractor owned ecosystem – transition will require continued testing & quality assurance to ensure service operations are not affected after transition is complete. Transition of the assets to the new service **MUST** be done in a staged manner.

Phase 4 Operations – The Contractor and the Purchaser will monitor the new service provided to ensure that the services being provided are meeting the requirements from the contract and ensure that the service level agreements are being met as well as the necessary performance metrics.

1.5.3. High level plan for integration in enterprise and capability architecture

- The Contractor SHALL ensure all provided services and equipment continue to integrate seamlessly with all existing infrastructure that remains under the control of the NCI Agency.
- The Contractor SHALL ensure that all current capabilities/capacity as discovered in Phase 1 are met and plan for future requirements in resources and capacity.
- The Contractor SHALL ensure with the Purchaser that all current integrations continue to operate as expected (network/routers/firewalls/switches correctly configured for the integration traffic).

1.5.4. High level security accreditation plan

- The Contractor SHALL ensure that security accreditation shall be performed by a National Security Accreditation Authority (SAA) (or their delegated SAA) for all contractors' CIS including Data Centres that are used to handle (store, process or transmit) NATO data up to an equivalent level of NATO Restricted. Security accreditation process for outsourced capabilities is the Contractor's responsibility and shall ensure that NATO's minimum security standards are met as per documents.
- The Contractor shall provide necessary support for the security accreditation processes of the NATO owned CIS with the documentation and paper work.