

NATO UNCLASSIFIED

## **NCIA Request for Information (RFI)**



### **IT Service Management Solution for Asset and Configuration Management Database**

**MS-424363-ITSM**

## NCIA Request for Information (RFI)

**To: Industry Partners**

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify qualified vendors and gather input on potential solutions to support the upcoming acquisition for IT Service Management Solution for Asset and Configuration Management Database. To that end, we are issuing the attached Request for Information (RFI) MS-424363-ITSM to solicit feedback from capable and interested industry partners.
2. This RFI is issued for planning purposes only and is not a request for bids. It is part of NCIA's effort to ensure it has a clear understanding of the marketplace, available capabilities, and potential acquisition strategies.
3. We value your insight and invite you to:
  - a. Share relevant corporate capabilities and experience;
  - b. Review and comment on our draft requirements (Annexes A and B) with a view in providing recommendations for improving performance outcomes, competition, and efficiency; and identifying any risks or concerns that should be considered during planning.
4. Submission instructions and additional details can be found in the enclosure to this RFI.
5. Only companies from a NATO member country can participate in or respond to this RFI ([https://www.nato.int/cps/en/natohq/nato\\_countries.htm](https://www.nato.int/cps/en/natohq/nato_countries.htm)).
6. Should you have any questions or need clarification, please contact Estefania Nunez at [Estefania.Nunez@ncia.nato.int](mailto:Estefania.Nunez@ncia.nato.int).
7. We thank you in advance for your time and input, and we look forward to engaging with you as we shape this potential acquisition.

For the Chief of Acquisition:

---

Tiziana Pezzi  
Principal Contracting Officer

**Enclosure:**

- Request for Information with Annexes A and B
- Distribution List

**Distribution List**

**1. NATO Delegation (Attn: Infrastructure Adviser)**

- |             |                     |                    |
|-------------|---------------------|--------------------|
| 1. Albania  | 12. Greece          | 23. Poland         |
| 2. Belgium  | 13. Hungary         | 24. Portugal       |
| 3. Bulgaria | 14. Iceland         | 25. Romania        |
| 4. Canada   | 15. Italy           | 26. Slovakia       |
| 5. Croatia  | 16. Latvia          | 27. Slovenia       |
| 6. Czechia  | 17. Lithuania       | 28. Spain          |
| 7. Denmark  | 18. Luxembourg      | 29. Sweden         |
| 8. Estonia  | 19. Montenegro      | 30. Türkiye        |
| 9. Finland  | 20. Netherlands     | 31. United Kingdom |
| 10. France  | 21. North Macedonia | 32. United States  |
| 11. Germany | 22. Norway          |                    |

**2. All NATEXs**

## Table of Contents

<b>REQUEST FOR INFORMATION .....</b>	<b>5</b>
<b>A. Introduction .....</b>	<b>5</b>
<b>B. Purpose.....</b>	<b>5</b>
<b>C. Background .....</b>	<b>5</b>
<b>D. Submission Instructions.....</b>	<b>5</b>
<b>E. Industry Engagement .....</b>	<b>6</b>
<b>F. Disclaimer.....</b>	<b>6</b>
<b>G. Use of Information Provided through Responses.....</b>	<b>6</b>
<b>H. RFI Point of Contact.....</b>	<b>7</b>
<b>Annex A – Requested Information.....</b>	<b>8</b>
<b>Annex B – Draft Requirements.....</b>	<b>12</b>

# REQUEST FOR INFORMATION

## A. Introduction

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify potential sources and gather information regarding industry capabilities to provide an integrated ITSM and Asset and Configuration Management solution for the management of Deployable CIS (DCIS) services and assets in support of NCISG. This Request for Information (RFI) is issued solely for informational purposes and does not constitute a Request for Proposal (RFP), Request for Quotation (RFQ), or invitation for bid.

## B. Purpose

1. The purpose of this RFI is to obtain input from industry to help inform the NCIA's acquisition planning. Responses to this RFI will assist in refining requirements, identifying capabilities, and shaping the strategy for any future solicitation.

## C. Background

1. NCIA NIMSC L&A BU manages a portfolio of Deployable CIS services across four operational domains (Deployable Nodes, Connectivity & SATCOM, Anchor & Infrastructure, and Service & Support), supporting NCISG across 25 units in 14 nations. The portfolio spans over 5000 individual assets requiring lifecycle management across two classification domains: NATO Restricted (NR) and NATO Secret (NS).

Asset tracking is currently performed using an interim Configuration Management System (iCMS). NCIA requires a strategic, purpose-built ITSM and Asset Management solution to replace this interim capability and provide full lifecycle visibility, integrating with existing enterprise systems: Oracle EBA (financial management, NR network) and BMC Remedy (incident and change management, NS network).

The solution must be operational within 12 months of contract award, including full migration of existing data, completion of physical inventory, and delivery of all documentation.

## D. Submission Instructions

1. Interested parties are invited to respond in accordance with the instructions below:
  - a. Submit responses via the email address in section H no later than **12:00 hours Central European Time (CET) on 02 June 2026**.
  - b. Responses should be submitted in PDF or Word format and must not exceed **15 pages**, including:
    - i. Responses to [Annex A](#) and comments on [Annex B](#)  
excluding:
      - i. Cover page
      - ii. Company brochures or product literature (if included)

- iii. Attachments such as past performance references
  - c. Use the following subject line for submission
    - i. “Response to RFI [RFI Number] – [Company Name]”
  - d. All responses should address the items listed in [Annex A](#) – Requested Information.
  - e. Respondents are also encouraged to review and comment on the draft requirements in [Annex B](#) – Draft Statement of Work (SOW)/Performance Work Statement (PWS).

## E. Industry Engagement

1. Not Applicable

## F. Disclaimer

1. This RFI is for planning and informational purposes only and shall not be construed as a solicitation or obligation on the part of the NCIA. The NCIA does not intend to award a contract based on responses to this RFI. Respondents are solely responsible for all costs incurred in responding to this RFI. The NCIA will consider and analyse all information received from this RFI and may use these findings to develop a future solicitation. The NCIA will consider all responses as confidential commercial information and will protect it as such.
2. NCIA reserves the right, at any time, to cancel this informal market survey, partially or in its entirety. No legal liability on the part of NCIA for payment of any sort shall arise and in no event will a cause of action lie with any prospective participant for the recovery of any costs incurred in connection with the preparation of documentation or participation in response hereto. All effort initiated or undertaken by prospective informal market survey participants shall be done considering and accepting this fact.

## G. Use of Information Provided through Responses

### 1. Confidentiality of Responses

The NCIA may incorporate industry comments and responses, in part or in whole, into a future release of a solicitation. Should respondents include proprietary data in their responses that they do not wish to be disclosed to the public for any purpose, or used by NCIA (except for internal evaluation purposes), they must:

- a. **Mark the title page with the following legend:**

*This document includes data that shall not be disclosed outside NATO and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than for NCIA internal evaluation purposes, unless otherwise expressly authorised by [insert company name]. This restriction does not limit the NCIA’s right to use information contained in this data without restriction if it is obtained from another source. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]*

- b. **Mark each sheet of data it wishes to restrict with the following legend:**

*Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.*

## **H. RFI Point of Contact**

1. Estefania Nunez
2. Estefania.nunez@ncia.nato.int.

## Annex A – Requested Information

1. Respondents are encouraged to provide the following information in their response:

**a. Company Information**

- i. Legal Business Name
- ii. Address
- iii. Website
- iv. Primary Point of Contact
- v. Email address

**b. Technical Capability**

- i. Confirmation of multi-domain (dual on-premise instance) support — one instance for NR, one for NS, each independently deployed. Describe the proposed architecture and how classification separation is enforced.
- ii. Description of CMDB capabilities including modular and hierarchical asset structure: Module → Product → Component, with documentation attachable at each level
- iii. Stock and spare parts management capabilities, including: consolidated catalogue, threshold alerts, stock tracking per location and classification domain, and pre-positioning support
- iv. Physical inventory tools and field mobility support — confirm barcode and/or QR code scanning capability for field inventory operations
- v. Documentation management at component level: version control, classification-aware access controls, bulk upload, and metadata tagging
- vi. PMI and CMI scheduling and tracking: configurable PMI frequency, advance notification (minimum 21 calendar days), maintenance task libraries, post-maintenance report generation
- vii. Describe your integration approach for Oracle EBA (NR domain): API type (REST/SOAP or equivalent accredited method), data model, bidirectional synchronisation method, and conflict resolution rules
- viii. Describe any existing certified integrations with Oracle E Business Suite — provide integration architecture and reference deployments if available
- ix. Describe your integration approach for BMC Remedy (NS domain): API type, bidirectional status synchronisation for maintenance tickets, CMI workflow triggering, and boundary controls ensuring no data leaves the NS domain
- x. Describe any existing certified integrations with BMC Remedy — provide integration architecture and reference deployments if available
- xi. Confirm support for STANAG 2290 / NATO UID from initial asset registration. Describe how NATO UIDs are managed across the asset lifecycle.
- xii. Confirm support for location hierarchy: Theatre → Country → Site → Building → Room → Rack/Position
- xiii. Existing NATO or defence customer references (anonymised if required)
- xiv. Number of deployments at comparable scale (distributed, multi-site, multi-classification domain)

### c. Security Accreditation

- i. Confirm full compliance with NATO INFOSEC policy (AC/35) and all subsidiary directives applicable to the NR and NS classification domains
- ii. Confirm compliance with NATO CIS Security Baseline (NCSB) requirements for information systems operating on classified networks
- iii. Describe your approach to ensuring the solution is fully accreditation-ready on day one of operational use. Systems that are not accreditation-ready at go-live will not be accepted.
- iv. Confirm ability to obtain and maintain CIS accreditation from NCSA or delegated Designated Accreditation Authority (DAA) for both the NR and NS instances
- v. Confirm compliance with NATOEX/SECAN cryptographic and emanations security requirements applicable to the NS instance
- vi. Describe your role-based access control (RBAC) model and mandatory NATO personnel security clearance verification at each classification level
- vii. Describe full audit logging capability: user actions, configuration changes, data access events, and tamper-evident log storage
- viii. Confirm encryption of data at rest and in transit using NATO-approved cryptographic standards
- ix. Confirm that all personnel requiring access to NR or NS systems hold or are able to obtain the appropriate NATO security clearance. Describe your security clearance management process.
- x. Describe your experience delivering or supporting the formal CIS accreditation process for NATO-classified systems. Prior NATO accreditation experience is a mandatory requirement — respondents with no such experience will not be considered for any subsequent procurement.

### d. Deployment and Hardware

- i. Confirm that your solution supports on-premise deployment exclusively. Cloud-based, SaaS, or externally hosted models are not acceptable and will not be considered.
  1. **Option A — Contractor-Provided Hardware:**
    - a. Describe the hardware you would propose for each instance (NR and NS), including: server specifications, storage capacity and type, redundancy model (HA/DR), estimated delivery lead time, and confirmation that hardware meets NATO physical security requirements for each domain
    - b. Provide indicative hardware cost as part of your ROM estimate
  2. **Option B — NCIA-Provided Hardware:**
    - a. Provide minimum hardware specifications required per instance: server CPU/RAM/storage, network infrastructure, redundancy requirements
    - b. Describe your process for validating that NCIA-provided hardware meets your requirements before installation begins, and how you would manage non-conforming hardware
    - c. Respondents must provide a response for both options. NCIA will make a final selection at the time of procurement.

### e. Implementation Approach

1. Brief description of the proposed ITSM / Asset and Configuration Management solution

**f. Standards and Compliance**

- i. Confirm support for STANAG 2290 (NATO UID) from initial asset registration
- ii. List applicable industry standards supported by your solution (e.g. ISO 55000 asset management, ITIL, ISO/IEC 27001, ISO 9001)
- iii. Describe compliance with relevant NATO security policies and standards for classified system operation
- iv. Confirm your solution's compliance with GDPR and applicable data protection regulations for any personal data processed

**g. Feedback and Recommendations**

- i. Responses to the following RFI Questions

Field	Response
Company Name	
Country of Registration	
NATO Member Nation?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Solution Name	
Current Version	
Contact Name	
Contact Email	
Contact Phone	
Can you meet the 12-month implementation constraint?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Conditional (explain in response)
Can you support Option A — Contractor-Provided Hardware for both NR and NS instances?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial (explain)
Can you support Option B — Installation on NCIA-Provided Hardware?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial (explain)
Can the system be delivered fully accreditation-ready on day one of operational use?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Conditional (explain)
Do you have an existing certified integration with Oracle E Business Suite?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In development
Do you have an existing certified integration with BMC Remedy?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In development
Do relevant personnel hold or can obtain NATO security clearance (NR and NS levels)?	<input type="checkbox"/> Yes <input type="checkbox"/> Partial <input type="checkbox"/> No
Have you previously delivered solutions in NATO classified environments?	<input type="checkbox"/> Yes (provide reference) <input type="checkbox"/> No

Have you previously supported a formal NATO CIS accreditation process?	<input type="checkbox"/> Yes (provide reference) <input type="checkbox"/> No
Have you conducted multi-nation physical inventories?	<input type="checkbox"/> Yes <input type="checkbox"/> No
STANAG 2290 / NATO UID support?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial
ISO 55000 Asset Management compliance?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress
ITIL-aligned service management?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial

- ii. Innovations or alternatives
- iii. Rough Order Magnitude (ROM), including any assumptions upon which they are based.
  1. Indicative cost structure broken down by: software licence / subscription, implementation services, hardware (Option A only), training, and annual support and maintenance
  2. Please provide separate ROM estimates for Option A (Contractor-Provided Hardware) and Option B (NCIA-Provided Hardware)
  3. Indicative implementation effort in person-months, broken down by phase
  4. Annual support and maintenance cost model post go-live

#### **h. Questions or Concerns**

- i. Risks, concerns, or barriers
- ii. Suggestions for risk mitigation or enhancing competition

## Annex B – Draft Requirements

Note: This is a DRAFT and subject to change. The NCIA is seeking industry feedback.

### 1. Background

The NATO Communications and Information Agency (NCIA) requires an integrated ITSM and Asset Management solution to replace the existing interim Configuration Management System (iCMS) used to support the management of Deployable CIS (DCIS) services and assets in support of NCISG. The solution must support NCIA's mission to deliver reliable, secure, and mission-ready Deployable CIS services to NCISG.

### 2. Scope

The scope includes, but is not limited to:

- a. Asset and Configuration Management (CMDB) for all DCIS assets across NS and NR classification domains
- b. Inventory Management — physical and logical, per asset, per location, per classification
- c. Stock and Spare Parts Management
- d. Incident, Change, and Service Request Management
- e. Preventive Maintenance Inspection (PMI) and Corrective Maintenance Inspection (CMI) scheduling and tracking
- f. Integration with Oracle EBA (NR) for financial and property accounting data
- g. Integration with BMC Remedy (NS) for incident and change management data
- h. Documentation Management at Module, Product, and Component level
- i. Reporting, dashboards, and KPI tracking — separate instances per domain
- j. User access control and role-based permissions aligned to NATO security policies

### 3. Technical Requirements – Multi-Domain Architecture

The solution must operate across two classification domains via two independent on-premise instances:

Attribute	NR Domain (NATO Restricted)	NS Domain (NATO Secret)
Network	NR (Unclassified / Restricted)	NS (Secret)
Primary data	Asset inventory, financials, change history, logistics	Operational configuration, security posture, DCIS baseline, incident records
Integration	Oracle EBA (financial / property accounting)	BMC Remedy (incident and change management)
User access	SDMs, PSM, logistics, financial controllers	SDMs, Field Engineers (OCMs/FSPs), ESOC

The solution must enforce classification boundaries. No automated data transfer shall occur between NS and NR domains without an accredited, auditable transfer mechanism approved by the relevant Security Accreditation Authority. The architecture must support an air-gap model between domains where required.

### 4. Asset and Configuration Management

- a. Recording and tracking all DCIS assets across their full lifecycle (acquisition, deployment, maintenance, disposal)
  - b. Hierarchical asset structures: Module → Product → Component level, with documentation attachable at each level
  - c. Managing asset relationships (parent-child, dependency, location)
  - d. NATO UID tracking in compliance with STANAG 2290 from initial asset registration
  - e. Asset status recording: Serviceable, Unserviceable, In-Repair, In-Storage, Disposed, On-Loan
  - f. Asset types and classes — definitions and classification schema to be established by the Contractor (see Contractor Responsibilities)
  - g. Version control and audit trail for all configuration changes
- 5. Stock and Spare Management**
- h. Consolidated spare parts catalogue linked to parent assets and service families
  - i. Stock levels tracked per location, per storage facility, and per classification domain
  - j. Minimum stock threshold alerts and reorder workflows
  - k. Receipt, issue, return, and disposal transactions with full audit trail
  - l. Spare part consumption linked to PMI/CMI records
  - m. Stock status reports and consumption trend analysis
  - n. Pre-positioning of spare parts across geographically distributed NCISG locations
- 6. Inventory Management**
- o. 100% physical inventory capability per location, scheduled or ad-hoc
  - p. Barcode and/or QR code scanning support for field inventory operations
  - q. Discrepancy management workflow — missing, damaged, or found assets with formal reporting
  - r. Integration with Oracle EBA for property accounting reconciliation on the NR domain
  - s. Location hierarchy: Theatre → Country → Site → Building → Room → Rack/Position
- 7. Modular Product and Documentation Management**
- t. Assets defined as Modules (e.g. DCIS node), composed of Products (e.g. server, radio unit), composed of Components (e.g. PSU, card, cable assembly)
  - u. Technical documentation (manuals, datasheets, SOPs, certificates) attachable at Module, Product, and Component level
  - v. Documentation version control — previous versions retained
  - w. Documentation access controls aligned to classification domain (NR/NS)
  - x. Bulk document upload and structured metadata tagging
- 8. Maintenance Management (PMI/CMI)**
- y. PMI scheduling per asset with configurable frequency and advance notification (minimum 21 calendar days)
  - z. CMI registration, tracking, and resolution linked to incident records
  - aa. Maintenance task libraries — standard checklists linked to asset types
  - bb. Technician assignment and work order management
  - cc. Post-maintenance report generation and attachment to asset record
  - dd. Integration with BMC Remedy (NS) for incident-triggered CMI workflow
- 9. Integration – Oracle E Business Suite (EBA)**
- ee. Bidirectional synchronisation of asset records and property accounting data between ITSM tool and Oracle EBA
  - ff. Financial valuation data (acquisition cost, depreciation, book value) linked to asset records
  - gg. Automated reconciliation of physical inventory results against EBA financial records
  - hh. Documented, auditable API (REST/SOAP or equivalent accredited method)

- ii. Conflict resolution rules explicitly defined and agreed with NCIA prior to implementation

## 10. Integration - BMC Remedy

- jj. Asset records created and updated in the ITSM tool from Remedy incident and change data
- kk. Remedy incident tickets linked to affected assets in the CMDB
- ll. CMI workflows triggered from Remedy corrective maintenance requests
- mm. Bidirectional status synchronisation for maintenance-related tickets
- nn. No data shall leave the NS domain through this integration
- oo. Integration mechanism approved by the relevant NS Security Accreditation Authority prior to deployment

## 11. Reporting KPIs and Dashboards

- pp. Configurable dashboards for PSM, SDM, Field Engineer, and Management roles
- qq. Standard DCIS KPI reports: asset availability (%), PMI completion rate (%), incident backlog, stock levels, obsolescence status
- rr. Exportable reports in PDF and Excel formats
- ss. QSLR report packs auto-generated from live data
- tt. Trend analysis over rolling 12-month periods
- uu. Separate dashboard instances per classification domain (NR and NS)

## 12. Contractor Responsibilities

### a. Asset Type and Class Definition

- i. Conducting a discovery exercise with NCIA NIMSC L&A BU to understand the DCIS asset portfolio structure
- ii. Proposing and agreeing an asset taxonomy — defining all asset types and classes appropriate to the DCIS portfolio
- iii. Documenting the agreed taxonomy in a formal Asset Classification Schema, approved by NCIA before system configuration begins
- iv. Updating the schema at any point during the contract term where new asset types are introduced, at no additional cost

### b. Physical Inventory

- i. Planning and executing a 100% physical inventory across all NCISG locations (up to 25 units in 14 nations)
- ii. Coordinating site access with NCIA and NCISG — minimum 21 calendar days advance notice per site
- iii. Recording each asset: NATO UID, serial number, location, status, and condition
- iv. Reconciling findings against iCMS and Oracle EBA records; formally reporting all discrepancies
- v. Completing initial physical inventory, no later than Month 6
- vi. Delivering a formal Physical Inventory Report, validated by Contractor and NCIA

### c. Documentation

- i. Sourcing, organizing, and uploading all available technical documentation for DCIS assets
- ii. Defining and applying a documentation metadata schema (document type, version, classification, applicability)
- iii. Producing and maintaining: Implementation Plan, Asset Classification Schema, Data Migration Plan, Physical Inventory Report, Integration Test Reports, UAT Report, System Administration Guide, End-User Training Materials

### d. Training

- i. Role-based training: System Administrators, SDMs/PSM, Field Engineers (OCMs), read-only management users
- ii. Training in English; delivery format agreed with NCIA (on-site, virtual,

or hybrid)

- iii. Train-the-trainer capability to enable NCIA to onboard future users independently

### 13. Deployment and Security Requirements

- i. On-premise deployment only — cloud-based, SaaS, or externally hosted models are not acceptable
- ii. Two independent instances required (NR and NS) — no automated cross-domain data exchange
- iii. Option A (Contractor-Provided Hardware): Contractor supplies, installs, and configures all hardware for both instances
- iv. Option B (NCIA-Provided Hardware): Contractor defines specifications (Hardware Specification Document, Month 1), installs and configures both instances
- v. Full compliance with NATO INFOSEC policy (AC/35), NCSB, NATOEX/SECAN
- vi. Accreditation from NCSA or delegated DAA required for both instances before operational use
- vii. All security accreditation documentation to be delivered by Contractor no later than Month 10

### 14. Objectives

- a. Create a scalable service management area, supported by the right tools and processes, capable of growing with the DCIS portfolio and adapting to evolving mission requirements.
- b. Provide the service management function with the processes and tooling needed to manage assets and configurations effectively, consistently, and in full compliance with NATO standards.
- c. Improve asset lifecycle management across the full DCIS portfolio — from initial registration through deployment, maintenance, and disposal — with complete traceability at every stage.
- d. Improve configuration management maturity, establishing a single authoritative source of truth for all DCIS assets across both the NR and NS classification domains.

### 15. Performance Requirements

Category	Performance Metric	Target / Requirement
Availability	System availability — NR instance	>= 99.5% per calendar month, measured during business hours
Availability	System availability — NS instance	>= 99.5% per calendar month, measured during business hours
Availability	Planned maintenance window	Maximum 4 hours per month, outside business hours, with 5 working days advance notice
Response Time	Page and search response time (standard queries)	<= 3 seconds under normal load (up to 50 concurrent users)
Response Time	Report and dashboard generation time	<= 10 seconds for standard KPI dashboards; <= 30

		seconds for full QSLR report pack
Capacity	Concurrent user capacity	>= 50 concurrent users per instance without degradation of response time
Data Quality	Asset record accuracy	>= 95% of asset records complete, correctly classified, and reconciled against Oracle EBA within 30 days of go-live
Data Quality	CMDB data completeness	>= 98% of in-scope DCIS assets registered in the system within 60 days of go-live
Integration	Oracle EBA integration reliability (NR)	>= 99% of scheduled synchronisation transactions completed without manual intervention
Integration	BMC Remedy integration reliability (NS)	>= 99% of incident and change data exchanges completed without manual intervention
Integration	Integration error resolution	All failed transactions flagged with alert within 15 minutes; root cause identified within 4 business hours
Backup & Recovery	Backup frequency	Daily automated backup for both NR and NS instances
Backup & Recovery	Recovery Time Objective (RTO)	<= 4 hours from declared failure to full system restoration
Backup & Recovery	Recovery Point Objective (RPO)	<= 24 hours maximum data loss in the event of a system failure
Security & Audit	Audit log retention	Minimum 3 years; tamper-evident; accessible to authorised administrators within 1 business day of request
Security & Audit	Unauthorised access attempt alerting	Alert generated within 5 minutes of any failed authentication threshold breach (5 consecutive failures)
Security & Audit	Security patch application	Critical security patches applied within 30 calendar days of release, following NATO change management process

## 16. Deliverables

Deliverable	Description	Due
Implementation Plan	Full project plan covering all phases for both instances	Month 1
Asset Classification Schema	Agreed asset types and classes taxonomy, approved by NCIA	Month 1
Hardware Specification Document (Option B only)	Minimum HW specs per instance (NR and NS)	Month 1
Data Migration Plan	Approach, tools, validation criteria	Month 2
NR Instance — Deployed and Configured	Including Oracle EBA integration tested	Month 4
NS Instance — Deployed and Configured	Including BMC Remedy integration tested	Month 5
Physical Inventory Report	100% inventory — all NCISG locations, validated by NCIA	Month 6
Migration Validation Report	Data validated post-migration, approved by NCIA	Month 7
Integration Test Reports	EBA (NR) and Remedy (NS) integration test results	Month 9
Security Documentation Package	SDD, Risk Assessment, SECEMP, Evidence of Testing	Month 10
UAT Report	User acceptance test results	Month 10
Training Delivery	All user roles trained, Training materials delivered	Month 11
System Administration Guide	Full admin and user documentation	Month 11
Full Go-Live (NR + NS)	iCMS decommissioned, system documentation finalised	Month 12

## 17. Period of Performance

- a. 12 months from contract award (base period). No extension to the 12-month constraint will be accepted at time of proposal. Post-implementation support period to be defined in a subsequent procurement.

## 18. Place of Performance

- a. The works are going to be performed Mainly at NCIA Belgium and The Netherlands. The inventory will take place at other NATO Locations in Europe to be disclosed at bid phase.