

NCIA Request for Information (RFI)



**DIGITAL SUPPORT TO NATO CAPABILITY DEVELOPMENT
RFI-07732-DSNCD**

NATO UNCLASSIFIED

NCIA/ACQ/2026/07732
Wednesday, 16 September 2026

NCIA Request for Information (RFI)

To: Nations and 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 development of NATO Policy and the upcoming acquisition for the Information Management for Capability Delivery programme. To that end, we are issuing the attached Request for Information (RFI) 07732 to solicit feedback from Nations and 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 provide information that helps NATO understand:
 - a. Whether NATO is addressing the right problems in the context of Digital Support to NATO Capability Development.
 - b. Whether the proposed Digital Processes Framework and Digital Process Operating Model are coherent, useful and implementable.
 - c. Whether the main risks, constraints, inefficiencies and opportunities have been correctly identified.
 - d. What national experience, lessons learned, tooling, organisations, communities and suppliers NATO should consider.
 - e. What tools, methods, services, platforms, toolchains, demonstrations, pilots or implementations industry can provide.
 - f. What NATO should change, clarify or further investigate before moving to any future RFPs.
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).
6. Should you have any questions or need clarification, please contact dcd@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:

Mihaela Zoicas
Contracting Officer

NATO UNCLASSIFIED

NATO UNCLASSIFIED

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

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Table of Contents

REQUEST FOR INFORMATION	7
A. Introduction	7
B. Purpose.....	7
C. Background	7
D. Submission Instructions.....	9
E. Follow-up Engagement	9
F. Disclaimer	10
G. Use of Information Provided through Responses	10
H. RFI Point of Contact	10
Annex A – Requested Information	11
1. How to respond	11
2. Questions for respondents.....	11
a. Questions for all respondents.....	11
b. Questions for NATO Nations and institutional respondents.....	12
c. Questions for industry respondents.....	12
Annex B – Contextual information.....	14
1. Digital Capability Development, DPF and DPOM	14
a. Digital Capability Development and the Digital Engineering Initiative	14
b. Digital Processes Framework.....	14
c. Digital Process Operating Model	15
d. Problems the DPF and DPOM Seek to Address	16
e. Proposed Principles.....	16
f. Confirmed and Candidate Concepts Relevant to the Initiative	17
2. Follow-on RFPs and How RFI Responses Will Be Used.....	19
RFP 1 – Programme Support for Digital Capability Development	19
RFP 2 – Toolchain Demonstrations / Pilot Implementations	20
3. NATO Capability Development Journey	21
Layer 1: Strategic Concepts / Strategic Direction.....	21
Layer 2: Alliance Political-Military Direction and Decision-Making	22
Layer 3: Defence Planning	22
Layer 4: Capability and Portfolio Management / Investment Alignment	23
Layer 5: Programmes	23
Layer 6: Projects	24
Layer 7: Suppliers / Delivery Ecosystem.....	24

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Boundaries, Interfaces and Use Cases	25
4. Use Cases	26
UC 1 – Coordination Across National, Multinational, and Common-Funded Delivery Routes	27
UC 2 – End-to-End Change Impact Assessment and Reprioritisation	28
UC 3 – Translation of Strategic Guidance into NDPP Capability Targets	29
UC 4 – Structured Handover of NDPP Outputs to Delivery Communities.....	30
UC 5 – Alignment of Common-Funded Portfolio Priorities and NSIP Investments to NDPP.....	31
UC 6 – Integrated Programme Delivery of a Federated Capability	32
UC 7 – Closed-Loop Reporting from Delivery to NDPP and Strategic Decision-Making	33
UC 8 – Supplier Deliverables as Governed Evidence of Capability Delivery	34
5. Glossary.....	35

NATO UNCLASSIFIED

Key topics of interest:

Industry area	Capabilities of interest
Digital engineering and MBSE	MBSE, systems-of-systems engineering, mission engineering, architecture modelling, digital twins and simulation.
Enterprise and capability architecture	Enterprise, defence and capability architecture; architecture repositories; coherence across capability portfolios.
Digital thread and lifecycle management	PLM, ALM, configuration management, baselines, engineering change, lifecycle information continuity and impact analysis.
Requirements, verification and assurance	Requirements management, traceability, test, verification, validation, compliance evidence and supplier assurance.
Data integration and information governance	Data integration, metadata, catalogues, ontologies, knowledge graphs, provenance, maturity, authority and ownership of information.
Portfolio, programme and resource management	Capability portfolio management, P3M, dependency tracking, delivery reporting, budget and performance integration.
Workflow, collaboration and secure information exchange	Workflow automation, collaboration platforms, secure multi-network information sharing and governed supplier/Nation exchange.
Interoperability, open standards and toolchain integration	Open standards, interoperability frameworks, modular open systems approaches, APIs, repositories and toolchain integration.
AI, analytics and decision support	AI-assisted engineering, analytics, decision-support tooling, experimentation and wargaming support.
Secure cloud, DevSecOps and managed services	Secure hosting, accreditation support, DevSecOps, continuous delivery, platform operations and managed services.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

REQUEST FOR INFORMATION

A. Introduction

The NATO Communications and Information Agency (NCIA) is conducting market research to identify potential sources and gather information regarding industry capabilities to support the 2026 CDT Digital Engineering Initiative. 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.

This RFI is directed to two principal respondent groups:

- Institutional respondents are invited to provide national or organisational experience, lessons learned, relevant initiatives, tooling, organisations, subject matter experts, communities, and industry contacts that may inform NATO's next steps. NATO Nations are encouraged to distribute this RFI to relevant national defence, digital engineering, capability development, acquisition, science and technology, and industry communities.
- Industry respondents are invited to provide information on tools, platforms, toolchains, methods, services, demonstrations, pilots, examples or implementations that could support one or more parts of the NATO Capability Development Journey.

B. Purpose

This RFI seeks information from NATO Nations, industry respondents, and other relevant organisations on the proposed direction of NATO's Digital Processes Framework (DPF), Digital Process Operating Model (DPOM), Digital Engineering Directive, NATO Capability Development Journey, Information Management for Capability Development programme, and associated methods, tools, services, platforms, toolchains, demonstrations or pilots.

Responses to this RFI will assist in refining requirements, identifying capabilities, and shaping the strategy for any future solicitation.

C. Background

C.1 Context

The initiatives supported by this RFI are concerned with the digital enablement of capability development from strategic direction, political-military guidance and defence planning through portfolio management, programmes, projects and supplier delivery. It is not intended to replace national systems, NATO governance arrangements or existing organisational authorities. Rather, it seeks to improve how information is created, governed, exchanged, traced and reused across existing boundaries.

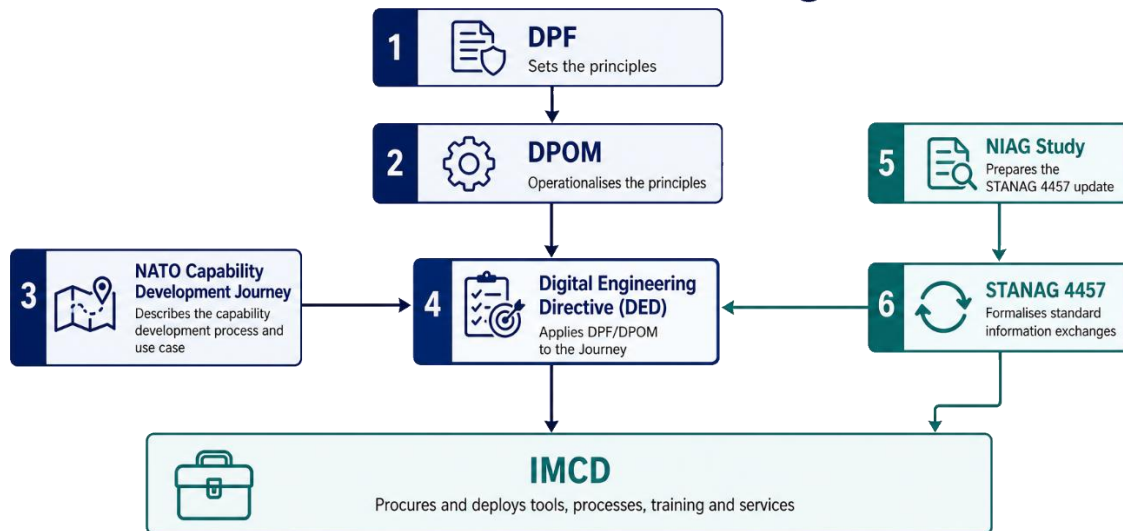
The relationship between these initiatives is as follows: The Digital Processes Framework will set the governing principles for coherent digital processes; the Digital Process Operating Model will describe how those principles operate in practice; and

NATO UNCLASSIFIED

NATO UNCLASSIFIED

the Digital Engineering Directive will specialise the common model for digital engineering and capability-development. The NATO Capability Development Journey document will provide the practical process and use-case view to which the directive should apply. The recently proposed NIAG Digital Engineering Study is expected to inform the standardised Digital Engineering Information Sets and STANAG 4457 update path, while Information Management for Capability Delivery (IMCD) is currently envisaged as the principal NATO Enterprise vehicle for implementing these concepts through practical tools, information environments, processes, training and adoption activities.

How the initiatives link together



C.2 Rationale and main points

NATO capability development depends on information passing across many organisational, procedural, technical, contractual and classification boundaries. As information moves from strategic direction and political-military guidance through defence planning, portfolio management, programmes, projects and supplier delivery, context, provenance, authority, assumptions and traceability can be weakened or lost. This creates practical problems: fragmented tools and data environments, duplicated effort, document-centric handovers, late discovery of integration and interoperability issues, limited visibility across delivery routes, manual reconstruction of decision rationale, and delayed reporting from project and programme levels to portfolio, defence planning and strategic decision-making levels.

The Digital Processes Framework and Digital Process Operating Model were initially conceived as a way to introduce Digital Engineering ways of working into NATO capability development. In that context, they are intended to support authoritative sources of data and models, governed information sets, traceability, configuration control, assurance evidence, interoperability requirements and lifecycle continuity across engineering and delivery activities. However, the same logic is not limited to Digital Engineering. The DPF and DPOM may also be applicable to other process domains where NATO needs coherent digital ways of working, governed information

NATO UNCLASSIFIED

NATO UNCLASSIFIED

exchange, clear ownership, reusable data products, and reliable movement of information across organisational, national, supplier or security boundaries.

The proposed approach is therefore federated rather than centralised. It does not seek to replace NATO processes, national systems, existing governance arrangements or organisational authorities, and it does not prescribe a single tool or platform. Instead, it seeks to improve interoperability, decision support, assurance and lifecycle continuity across heterogeneous NATO, national and supplier environments. Key principles include data as a governed product, interoperability and security by design, constraint-aware implementation, automation where appropriate, human-centred oversight, and progressive learning through demonstrations and pilots. Respondents are asked to comment on whether this framing addresses the right problems, whether the proposed principles are sound, where the DPF and DPOM may be useful beyond Digital Engineering, and which concepts, standards, tools, services or implementation approaches NATO should consider before moving toward any future RFPs.

Further information is available in Annex B.

D. Submission Instructions

Interested parties are invited to respond in accordance with the instructions below:

Submit responses via the email address in section H no later than **23:59 hours Central European Time (CET) on 11 October 2026**.

Responses should be submitted in PDF or Word format and must not exceed **20 pages**, including:

- i. Responses to Annex A and comments on Annex B.

excluding:

- i. Cover page
- ii. Brochures or product literature (if included)
- iii. Attachments such as past performance references

Use the following subject line for submission

- i. "Response to RFI [RFI-07732-DSNCD] – [Organization Name]"

All responses should address the items listed in Annex A – Requested Information.

E. Follow-up Engagement

We would like to engage with industry partners and nations through a combination of written communications, including responses to this Request for Information and any subsequent clarifications, as well as one-on-one meetings held virtually or in person at NCIA premises in The Hague, Netherlands, or Brussels, Belgium. NCIA is also planning a dedicated IMCD workshop at the NATO EDGE 26 Conference, which will be held in Fuar İzmir – Türkiye from the 17th to the 19th of November 2026.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

F. Disclaimer

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.

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. Anamaria Morega – Senior Contracting Officer
2. RFI-07732-DSNCD@ncia.nato.int.

NATO UNCLASSIFIED

Annex A – Requested Information

1. How to respond

Using the material in Annex B as context, respondents may provide either:

- individual, question by question answers;
- combined answers for related questions;
- a lightweight expression of interest, with a concise presentation of your organization and the reason of your interest;
- suggested reference material, contacts, organisations or suppliers; or
- any combination of the above.

Respondents may skip questions that are not relevant for them.

2. Questions for respondents

a. Questions for all respondents

- **A1.** Do you agree with the overall direction of the proposed Digital Processes Framework and Digital Process Operating Model? If not, what should be changed?
- **A2.** Are the main risks, issues and challenges identified in this RFI the right ones? Are any overstated, understated or missing?
- **A3.** Are there missing constraints, dependencies, policy issues, technical risks, organisational barriers or opportunities that NATO should consider, including integration, security, accreditation, data access, classification, export-control, intellectual property, commercial or adoption constraints before moving toward future procurement activity?
- **A4.** Have you implemented, observed or supported similar approaches in national, multinational, defence, public-sector or complex commercial environments? What lessons should NATO consider?
- **A5.** Are the proposed principles appropriate, including federation over centralisation, data as a governed product, interoperability by design, security by design, constraint-aware design, information-centricity and Modular Open Systems Architecture principles where relevant?
- **A6.** Where might the proposed approach fail? What are the most likely causes of failure?
- **A7.** What should NATO change, clarify or test before moving to future RFPs?
- **A8.** What standards, architectures, frameworks, methods or best practices should NATO consider, including standards, interfaces, data models, ontologies, exchange mechanisms or assurance approaches relevant to Digital Engineering Information Sets and especially IMCD-relevant digital threads? Please identify whether these are public, proprietary, national, international or otherwise restricted.
- **A9.** Is NATO asking the right questions in this RFI? What additional questions should NATO be asking?
- **A10.** Which use cases or journey segments appear most important, and why?
- **A11.** Are there use cases, journey layers, interfaces or information flows that should be added, removed, merged or reframed?

NATO UNCLASSIFIED

- **A12.** What would be a practical first step for NATO to validate the approach through a demonstration, pilot or structured engagement?
- **A13.** What NATO EDGE workshop discussion, bilateral meeting, demonstration or follow-on engagement would most effectively test the assumptions, risks and feasibility of the proposed approach?

b. Questions for NATO Nations and institutional respondents

- **N1.** What relevant national or institutional initiatives exist in digital engineering, digital capability development, model-based systems engineering, acquisition reform, portfolio management, information governance or related areas?
- **N2.** What national or institutional lessons learned should NATO consider, including unsuccessful approaches or implementation difficulties?
- **N3.** What tools, systems, methods, standards, architectures or frameworks are used nationally or institutionally that may be relevant to the NATO Capability Development Journey?
- **N4.** What organisations, agencies, communities, programmes, laboratories, centres of excellence or subject matter experts should NATO engage?
- **N5.** What industries, suppliers, small and medium-sized enterprises, research organisations or consortia should receive this RFI or be considered for future engagement?
- **N6.** Can your Nation or organisation distribute this RFI to relevant industry and internal stakeholders?
- **N7.** Are there national or organisational constraints, risks, classification issues, export-control issues, data-sovereignty issues, releasability constraints, intellectual property concerns or other limitations that NATO should consider?
- **N8.** Are there examples of toolchain integration across defence planning, portfolio management, programmes, projects and suppliers that NATO should study?
- **N9.** Are there approaches to supplier evidence, digital assurance, traceability or governed information exchange that may be relevant?
- **N10.** Would your Nation or organisation be willing to participate in follow-on discussions, workshops, demonstrations or information exchanges related to this initiative?

c. Questions for industry respondents

- **I1.** What tools, platforms, methods, services or toolchains can your organisation provide that may support the DPF, DPOM, use cases or NATO Capability Development Journey?
- **I2.** Which use cases, journey layers, journey segments or interfaces can your solution support?
- **I3.** Can your solution support multiple use cases coherently? If so, which ones and how?
- **I4.** How does your solution preserve information continuity, context, provenance, authority, maturity, ownership and traceability?
- **I5.** How does your solution support an information-centric approach?
- **I6.** How does your solution support Modular Open Systems Architecture principles,

NATO UNCLASSIFIED

NATO UNCLASSIFIED

where relevant?

- **I7.** Can your solution integrate with existing NATO systems, repositories, workflows or tool environments? What assumptions or constraints would apply?
- **I8.** Can your solution integrate with national or supplier-owned systems while preserving security, sovereignty, classification, export-control and intellectual property constraints?
- **I9.** Can your solution be demonstrated in a NATO-relevant environment, subject to confirmation?
- **I10.** What would a meaningful pilot, demonstration, example or implementation look like?
- **I11.** What data, access, users, interfaces, infrastructure, security conditions, assumptions or dependencies would be required for a demonstration or pilot?
- **I12.** What implementation or piloting approach should NATO take to reduce risk and learn quickly?
- **I13.** Is NATO's framing too narrow, too broad, technically problematic or commercially impractical?
- **I14.** What are the main risks to interoperability, scalability, usability, security, certification, accreditation or long-term sustainment?
- **I15.** What commercial models or engagement structures would best support modular demonstrations or pilots, without assuming any final contracting model?
- **I16.** Would your organisation be interested in RFP 1, RFP 2 or both?
- **I17.** If interested in RFP 1, which areas are most relevant to your organisation: programme support, stakeholder engagement and reporting, planning, monitoring and control, concept development, culture change, stakeholder needs and requirements solicitation, tooling survey and trade-off analysis, roles, skills and operating model support, or other areas?
- **I18.** If interested in RFP 2, which demonstrations, pilots, toolchains or use cases would you propose?
- **I19.** Would your organisation prefer to participate as a prime contractor, subcontractor, consortium member, technology provider, demonstration provider or other role?
- **I20.** If your organisation cannot provide a full response, would you like to register interest and remain informed of future activity?
- **I21.** Which aspects of your organisation, experience, tools, services or methods are most relevant to IMCD as a practical implementation context for governed capability-delivery information?
- **I22.** Would your organisation be interested in participating in or contributing to the proposed NIAG Digital Engineering Study? If so, what expertise or evidence could you contribute?

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Annex B – Contextual information

This annex provides the background, description of the “NATO Capability Development Journey”, use cases, exploratory future RFP considerations, and glossary needed to answer the questions in the response brief.

Respondents do not need to address every section of this context pack. They should use it to identify the journey layers, use cases, interfaces, concepts, assumptions, constraints, standards, or terms most relevant to their response.

This context pack is provided for information and planning purposes only. It does not create requirements, define a final procurement scope, or commit NATO or NCIA to any future RFP, demonstration, pilot, contract, award, or funding decision.

1. Digital Capability Development, DPF and DPOM

a. Digital Capability Development and the Digital Engineering Initiative

The Digital Capability Development / Digital Engineering Initiative is intended to support NATO in improving how information is created, governed, exchanged, traced, and reused across capability development activities.

The initiative is concerned with digital enablement of the capability development journey from strategic direction, political-military guidance, and defence planning through portfolio management, programmes, projects, and supplier delivery. It is not intended to replace national systems, NATO governance arrangements, or existing organisational authorities. Rather, it seeks to improve the way information moves across existing boundaries.

The central concern is that capability development depends on information passing through many organisational, procedural, technical, contractual, and classification boundaries. At each boundary, context, provenance, authority, assumptions, and traceability can be weakened or lost. The proposed approach seeks to reduce that loss and support more coherent, information-centric capability development.

For the purposes of this RFI, **Digital Engineering** is understood as an integrated digital approach using authoritative sources of data and models as a continuum across disciplines to support lifecycle activities. Respondents are invited to comment on how their experience, tools, methods, or services may support this direction.

b. Digital Processes Framework

The **Digital Processes Framework (DPF)** provides the proposed framework for bringing NATO digital processes into greater coherence. It is a strategic enabler, not only a technical initiative. It is intended to support decision-makers, planners, process owners, and delivery organisations by focusing on outcomes, responsibilities, information flows, and value rather than prescribing a single tool or platform.

For the purposes of this RFI, the DPF is intended to help NATO:

- govern and continuously improve digital processes across the Alliance;

NATO UNCLASSIFIED

NATO UNCLASSIFIED

- promote interoperability and collaboration among organisations and systems under real operational constraints;
- support existing strategic processes, including requirements management and capability planning, without creating parallel systems;
- reduce fragmented digitalisation, duplicated effort, and disconnected process data;
- clarify roles, responsibilities, and accountability for digital process management;
- support information continuity, traceability, and evidence-based decision-making;
- provide a basis for future demonstrations, pilots, or toolchain implementations.

The DPF does not replace NATO capability development processes, acquisition procedures, workforce policy instruments, national implementation measures, or existing organisational authorities. It also does not prescribe specific tools or platforms. It is presented in this RFI as an approach for review and validation.

c. Digital Process Operating Model

The **Digital Process Operating Model (DPOM)** is the proposed common operating model for the digital process domains governed under the DPF. It sits beneath the DPF and above individual process-domain directives. Its purpose is to describe, in terms common to every domain, how a digital process is run in practice so that each domain directive specialises a shared model rather than creating its own from a blank page.

For the purposes of this RFI, the DPOM describes how digital work operates as the transformation of information. It is intended to explain how information assets are:

- drawn from authoritative sources by reference, rather than unnecessarily copied;
- transformed through defined process activities;
- declared, owned, versioned, matured, approved, exchanged, retained, and reused;
- linked to upstream and downstream information;
- exchanged across domain, organisational, supplier, and classification boundaries as governed exchange packages;
- managed with sufficient identity, provenance, standing, and handling rules for another party to rely upon them.

The DPF explains why NATO must bring digital processes into coherence and what must be governed. The DPOM explains how those principles may operate in practice across process domains. Individual directives, including a future Digital Engineering Directive if approved, would specialise the shared model for a specific domain.

Respondents should consider not only the DPOM itself, but also how this operating model could support related parts of the wider ecosystem: the Digital Engineering Directive as a domain-specific specialisation; Digital Engineering Information Sets and governed exchange packages; toolchains and authoritative sources used across NATO, Nations and suppliers; and practical implementation contexts such as IMCD. NCIA is particularly interested in whether the proposed operating model is sufficient to make information assets findable, understandable, trusted, reusable, traceable and governable across the NATO Capability Development Journey.

The DPOM is presented in this RFI for respondent review. It carries no procurement implication and should not be read as a final implementation instruction.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

d. Problems the DPF and DPOM Seek to Address

The DPF and DPOM are intended to help address recurring issues in capability development, including:

- uneven digitalisation, where tools are introduced in isolation and do not connect across organisations or process domains;
- fragmented process and data environments that cause inefficiency, duplicated effort, and delayed integration;
- reliance on sequential, document-centric handovers where structured, governed, and traceable information would be more useful;
- late discovery of interoperability and integration problems, when remediation is more costly;
- limited visibility across national, multinational, and common-funded delivery routes;
- inconsistent traceability from strategic direction and political-military guidance to defence planning, portfolio decisions, programmes, projects, contracts, supplier evidence, and delivery outcomes;
- manual reconstruction of decision rationale, assumptions, provenance, and status;
- difficulty integrating supplier deliverables into NATO-governed information flows;
- delayed or incomplete reporting from project and programme levels to portfolio, defence planning, and strategic decision-making levels;
- difficulty assessing the impact of changes across the end-to-end journey;
- classification, sovereignty, intellectual property, export-control, vendor, and security constraints being treated too late rather than as design conditions.

Respondents are asked to comment on whether these are the right issues and whether NATO has framed them appropriately.

e. Proposed Principles

The following principles are proposed for respondent review. They reflect the current direction of the DPF and DPOM source material but should not be read as final NATO policy or final procurement requirements.

Principle	Description
Federation over centralisation	Digital process management should enable interoperability across heterogeneous NATO, national, and supplier implementations without requiring uniform approaches or unnecessary centralisation.
Data as a governed product	Data and information assets should be managed with defined ownership, lifecycle, quality expectations, accountability, provenance, and traceability.
Concurrent and incremental delivery	Digital process transformation should reduce sequential, handoff-based working and support concurrent, continuously improved practice where dependencies permit.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Principle	Description
Automation and shift-left assurance	Requirements, standards, controls, and conformance evidence should become increasingly machine-processable and verifiable earlier in the lifecycle where tooling allows.
Human-centred design	Digital processes and decision-support environments should strengthen human oversight and judgement, particularly as automation increases.
Interoperability by design	Interoperability should be designed through shared standards, common data models, and governed interfaces, rather than imposed through a single mandated tool or platform.
Security by design	Classification, access, releasability, national data sovereignty, intellectual property, cyber security, and supply-chain considerations should be addressed from the outset.
Constraint-aware design	Solutions should function under operational, industrial, political, contractual, classification, intellectual property, vendor, and sovereignty constraints rather than depending on those constraints being removed.
Progressive demonstration and learning	NATO should use demonstrations, pilots, and structured examples to test assumptions before committing to larger implementation decisions.

Respondents are invited to identify missing principles, unsuitable principles, implementation risks, or alternative approaches.

f. Confirmed and Candidate Concepts Relevant to the Initiative

The following concepts may be relevant to the wider initiative. Some are confirmed as part of the current DPF or DPOM source material; others remain subject to further decision before they can be treated as requirements.

Concept	Current status for this RFI
Digital Engineering Directive	Source material identifies the Digital Engineering Directive as a potential first worked instance of a domain directive under the DPOM. Its status, authority, scope, approval route, and applicability remain [TBD – to be confirmed].
Architecture for Interoperability of Digital Technologies within the Alliance (AIDA)	Source material identifies AIDA as an authoritative integration point for Information Exchange Requirements and Interoperability Requirements generated through DPF-governed processes. Respondents should not assume any specific implementation requirement unless confirmed in a future RFP.
Digital Interoperability Framework for the Alliance (DIFA)	Source material identifies DIFA as a reference for interoperability principles and requirements, including

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Concept	Current status for this RFI
	interoperability across policy, organisational, semantic, syntactic, and technical layers.
Information Exchange Requirements and Interoperability Requirements	Source material identifies Information Exchange Requirements and Interoperability Requirements as structured, traceable artefacts through which interoperability obligations are made explicit. The extent to which future RFPs will require them is [TBD – to be confirmed].
Lifecycle information handling levels	Source material identifies five handling levels: working information, approved baseline, retained record, published product, and transient display. These are included in this RFI for respondent review and are not final procurement requirements.
DPF components	Source material identifies DPF components including workforce and digital process competency, digital process standards, process platform management, data interoperability architecture, capability development and planning integration, emerging technology adoption, and industry and ecosystem integration.
DPF implementation programmes	Source material identifies candidate implementation programmes including workforce transformation, digital process standards and transition, industry and ecosystem integration, emerging technology adoption, process platform management and data architecture, and NATO Defence Planning Process (NDPP) and acquisition integration. Whether these will be reflected in future RFP structures remains [TBD – to be confirmed].
Specific standards and frameworks	Source material refers to, among others, the Digital Transformation Implementation Strategy, DIFA, AIDA, ISO/IEC/IEEE 15288:2023, ISO 15489, and AAP-48. Respondents may comment on their relevance. Future RFPs will confirm any applicable standards or compliance requirements.
Modular Open Systems Architecture (MOSA)	Modular Open Systems Architecture (MOSA) principles are relevant where toolchains, interfaces, and implementation approaches need to remain modular, open, interoperable, and resistant to unnecessary lock-in. The exact wording and applicability of MOSA requirements remain subject to confirmation.

Respondents may comment on these items if relevant, but they should not assume that they represent final NATO requirements.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

2. Follow-on RFPs and How RFI Responses Will Be Used

NATO and NCIA may use RFI responses to:

- validate or revise the proposed DPF and DPOM direction;
- refine the NATO Capability Development Journey and associated use cases;
- identify missing risks, assumptions, constraints, dependencies, and opportunities;
- shape future requirements and RFP scope;
- identify potential demonstration or pilot areas;
- identify suppliers, industries, national bodies, communities, or subject matter experts for possible future engagement;
- assess whether future work should be structured as full-scope, partial, modular, option-based, demonstration, or pilot activity.

RFI responses may help NCIA identify organisations for possible future engagement or invitation to future RFPs, subject to applicable procurement rules and future acquisition decisions. Submission of a response does not guarantee inclusion in any future activity.

RFP 1 – Programme Support for Digital Capability Development

NCIA currently anticipates a future RFP for programme support to the DCD Team. This RFP would support the DCD Team in running and maturing the next phase of the Digital Capability Development / Digital Engineering Initiative.

Based on currently available planning information, RFP 1 is supposed to contain:

- a core contract for programme support, consisting of:
 - stakeholder engagement and reporting support;
 - planning, monitoring, and control support;
 - concept development support;
 - culture-change or adoption support, subject to confirmation;
 - long-term support to help run and mature the initiative;
- optional work packages, that may be exercised zero or more times;
- partial bidding, allowing respondents to bid for the core contract, one or more options, or combinations of core and options, subject to the final RFP structure.

The final number of options is TBD. Current planning material identifies the following potential repeatable option areas:

- conceptual foundation revision;
- innovation and proof-of-concept or demonstration activity;
- tooling survey and trade-off analysis;
- roles, skills, profiles, and training analysis;
- tailored migration playbooks;
- stakeholder needs and requirements solicitation.

All option structures, bidding rules, evaluation methods, contract terms, timelines, award arrangements, and eligibility conditions remain subject to confirmation.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

RFP 2 – Toolchain Demonstrations / Pilot Implementations

NCIA currently anticipates a second RFP focused on demonstrations, pilots, examples, or toolchain capabilities that support specific subsets of the NATO Capability Development Journey.

Based on currently available planning information, RFP 2 should include:

- multiple awards, subject to confirmation;
- demonstrations or pilots supporting one or more journey layers, journey segments, or use cases;
- toolchains or methods aligned with the proposed DPF and DPOM;
- information-centric approaches that preserve context, provenance, authority, maturity, ownership, and traceability;
- modular open systems architecture principles, where relevant;
- minimal or limited customisation, where appropriate, to support repeatability and portability;
- demonstration or pilot implementation in the NATO Software Factory (NSF) or another NATO-relevant environment, subject to confirmation;
- modular or partial approaches that allow different suppliers to address different journey segments or use cases.

NCIA is interested in understanding what industry can provide, what a meaningful demonstration or pilot would require, and what assumptions, constraints, data, access, environments, or dependencies would need to be addressed.

All demonstration environments, technical constraints, data conditions, award structures, timelines, licensing arrangements, security conditions, accreditation conditions, and evaluation approaches remain subject to confirmation.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

3. NATO Capability Development Journey

For this RFI, the **NATO Capability Development Journey** describes how strategic intent is translated into capability delivery activity, implementation evidence, and supplier outputs. The journey is used as a practical organising framework for this RFI. It helps structure the use cases in **Chapter 4** and helps respondents identify where their national experience, tools, methods, services, demonstrations, pilots, or industry capabilities may be relevant. It is not intended to redefine NATO governance or national responsibilities. The journey is also used to identify where digital support, toolchains, information governance, and improved traceability may be required.

The journey is described through seven layers. Each layer produces information that may become an input to adjacent layers. The boundaries between layers are especially important because information context, provenance, authority, and traceability may be lost at those points.

The interfaces between these layers are not administrative details. They are central to the digital capability development problem.

Layer	Primary purpose	Digital support focus
Strategic concepts / strategic direction	Establish high-level strategic intent and priorities.	Preserve intent, assumptions, priorities, constraints, and rationale.
Political-military guidance or decision-making	Convert strategic direction into authoritative guidance and decisions.	Link decisions to downstream planning and delivery consequences.
Defence planning	Translate guidance into capability planning outputs, including Capability Targets where applicable.	Preserve traceability from guidance to planning artefacts, gaps, priorities, and Capability Targets.
Portfolio management, including national, multinational, and common-funded portfolios	Align delivery routes, investments, and initiatives against capability needs.	Provide visibility across portfolios and trace investments to capability needs.
Programmes	Coordinate delivery across related projects.	Maintain alignment between programme objectives, project execution, dependency management, and portfolio reporting.
Projects	Execute delivery and manage technical baselines and evidence.	Link requirements, designs, risks, evidence, decisions, accepted deliverables, and changes.
Suppliers / delivery ecosystem	Provide products, services, artefacts, and evidence.	Integrate supplier outputs as governed information.

Layer 1: Strategic Concepts / Strategic Direction

This layer establishes broad Alliance strategic intent, defence priorities, and long-term direction.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Its role is to define strategic concepts, priorities, threats, risks, objectives, and required strategic outcomes. The stakeholders for this layer include the North Atlantic Council and Allied national authorities, supported by the Secretary General and International Staff, the Military Committee and International Military Staff, and the NATO Strategic Commands, with contributions from relevant NATO committees and expert communities.

The main information inputs may include political direction and national positions, intelligence and strategic assessments, threat and risk assessments, strategic foresight and future operating environment analysis, military advice, existing Alliance policy and strategy, and relevant lessons and assessments. The main outputs may include the Strategic Concept and other agreed political and military strategies, concepts and strategic direction; strategic priorities and objectives; assessments of the future security and operating environment; and high-level assumptions and constraints for subsequent planning.

This layer provides the context for political-military guidance and defence planning. Digital support is needed to preserve strategic intent, assumptions, constraints, priorities, and rationale so they can be traced through later planning and delivery activity.

Layer 2: Alliance Political-Military Direction and Decision-Making

This layer converts strategic direction into authoritative political-military guidance, decisions, and direction for subsequent planning and implementation. Some products generated in this layer, including Political Guidance for Defence Planning, may formally constitute part of processes represented in the next layer.

Its activities include developing guidance, approving priorities, setting direction for planning and implementation, and resolving major trade-offs. The stakeholders for this layer include the North Atlantic Council and Allied national delegations, the Secretary General and International Staff, the Military Committee and International Military Staff, relevant senior committees such as the Defence Policy and Planning Committee, and the Strategic Commands where military advice is required.

The main information inputs may include strategic direction and concepts, national policy positions, political and military assessments, military advice, threat and risk assessments, planning assumptions, capability information, resource considerations, and proposals from subordinate committees and NATO bodies. The main outputs include political-military guidance, decisions, priorities, constraints, and direction to planning communities.

This layer connects strategic intent to defence planning activity. Digital support is needed to ensure that decisions, assumptions, constraints, authority, and downstream consequences are visible to planning and delivery layers.

Layer 3: Defence Planning

This layer translates guidance into planning outputs, including capability-related requirements and Capability Targets where applicable.

Its activities include analysing capability needs, developing planning outputs, assessing gaps,

NATO UNCLASSIFIED

NATO UNCLASSIFIED

identifying priorities, and informing planning cycles. Key stakeholders include Allies and their national defence-planning authorities; the North Atlantic Council and Defence Ministers; the Defence Policy and Planning Committee, including in Reinforced format; the NATO International Staff; the Military Committee and International Military Staff; Allied Command Transformation and Allied Command Operations; and the NATO planning domains and associated expert communities.

The main information inputs include political-military guidance, strategic priorities, assessments, capability information, and planning assumptions. The main outputs include Minimum Capability Requirements, Capability Targets where applicable, defence-planning assessments and reviews, identified shortfalls, priorities, implementation guidance, assumptions, and other planning artefacts.

This layer provides structured planning outputs to portfolio management and receives feedback on progress, gaps, and implementation constraints. Digital support is needed to maintain traceability between strategic guidance, planning artefacts, gaps, priorities, Minimum Capability Requirements, Capability Targets, and later evidence-based updates.

Layer 4: Capability and Portfolio Management / Investment Alignment

This layer covers capability and portfolio management across national, multinational, jointly funded, and NATO common-funded portfolios. It aligns investments and initiatives across those delivery routes without assuming that they are governed through a single NATO-wide portfolio authority.

Its activities include prioritising investments, mapping initiatives to capability needs, identifying gaps, managing dependencies, and assessing affordability, risk, and delivery routes. Key stakeholders vary by delivery route and include Allied national capability, investment and portfolio authorities; participating nations and governance bodies for multinational or jointly funded initiatives; capability and portfolio owners; and, for NATO common-funded capabilities, the North Atlantic Council, Resource Policy and Planning Board, Budget and Investment Committees, Military Committee, NATO Office of Resources, Strategic Commands, relevant NATO agencies, and host or user nations and other implementing authorities.

The main information inputs include defence planning outputs, Capability Targets where applicable, existing investment data, constraints, dependencies, affordability information, and risks. The main outputs include portfolio priorities, investment alignment, gap analysis, dependency maps, recommendations, and portfolio decisions.

This layer connects defence planning to programmes and receives delivery evidence from programmes and projects. Digital support is needed to provide coherent visibility across different funding and delivery routes, preserve traceability to planning outputs, and trace investments to capability needs.

Layer 5: Programmes

This layer coordinates related projects and delivery activities to deliver capability outcomes.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Its activities include defining programme plans, managing dependencies, aggregating project status, coordinating stakeholders, managing risks and issues, and supporting decisions. Key stakeholders include programme directors and programme managers, capability requirement and user authorities, programme governance and steering bodies, participating nations where applicable, the Strategic Commands, implementing organisations and host nations, relevant NATO agencies, project managers, operational users, and supporting resource, engineering, procurement and assurance functions.

The main information inputs include portfolio priorities, programme mandates, requirements, constraints, dependency information, and project information. The main outputs include programme plans, capability programme plans where applicable, dependency views, consolidated reporting, resource requirements, delivery milestones, risk and issue information, decisions, and updated constraints.

This layer connects portfolio-level objectives to project execution and reports progress upward. Digital support is needed to maintain continuity between portfolio decisions and project delivery, support dependency management, and enable timely, evidence-based reporting.

Layer 6: Projects

This layer executes delivery activity, including engineering, procurement, integration, verification, and deployment-related work.

Its activities include managing project baselines, requirements, schedules, risks, technical artefacts, acceptance, verification, validation, and supplier interaction. Key stakeholders include project managers; requirements, architecture and engineering teams; implementing authorities and host nations; operational users and acceptance authorities; procurement, commercial and financial functions; security, quality, verification, validation and assurance functions; programme management; and suppliers, integrators and other delivery partners.

The main information inputs include programme plans, requirements, constraints, supplier inputs, technical artefacts, risks, and acceptance criteria. The main outputs include project baselines, delivery status, evidence, risks, accepted deliverables, change information, and assurance records.

This layer receives direction from programmes, provides evidence to programmes and portfolios, and interfaces directly with suppliers. Digital support is needed to preserve traceability from requirements to designs, risks, evidence, decisions, delivered artefacts, accepted deliverables, changes, and assurance records.

Layer 7: Suppliers / Delivery Ecosystem

This layer provides products, services, technical solutions, evidence, and implementation support.

Its activities include developing deliverables, providing evidence, supporting integration, demonstrating compliance, maintaining technical data, and supporting acceptance. Key stakeholders include industry suppliers, integrators, service providers, specialist vendors,

NATO UNCLASSIFIED

NATO UNCLASSIFIED

subcontractors, and delivery partners.

The main information inputs include contractual requirements, technical requirements, project baselines, standards, acceptance criteria, and interface requirements. The main outputs include products, services, design artefacts, test evidence, compliance records, support information, and supplier-managed technical data.

This layer interfaces with projects and may provide evidence that supports programme, portfolio, defence planning, and strategic assurance. Digital support is needed to ensure supplier outputs are usable as governed information and can be integrated without loss of context or excessive manual rework.

Boundaries, Interfaces and Use Cases

The boundaries between journey layers are central to this RFI.

They are the points at which:

- authority may become unclear;
- assumptions may be lost;
- provenance may be weakened;
- information may be converted into less useful formats;
- traceability may be broken;
- reporting may become delayed or distorted;
- supplier evidence may become disconnected from upstream intent.

At each boundary, NATO may need to preserve:

- information authority;
- provenance;
- assumptions;
- decision rationale;
- version history;
- maturity and trust;
- classification and releasability constraints;
- links to upstream requirements and downstream evidence;
- ownership and accountability;
- confidence that information remains usable after transfer.

Use-cases may therefore relate either to activities within a layer or to the connection, boundary, handover, or information flow between two or more layers.

Respondents are invited to describe tools, methods, standards, or practices that improve these boundary exchanges. Respondents should refer to **Chapter 4** when identifying which journey layers, boundaries, or use cases their national experience, tools, methods, services, demonstrations, or pilots may support.

NATO UNCLASSIFIED

4. Use-Cases

This chapter describes a set of use-cases associated with the NATO Capability Development Journey.

For this RFI, a use case may be:

- an activity within a single journey layer; and/or
- a connection, boundary, handover, or information flow between two or more journey layers.

NATO is interested in:

- solutions supporting individual use-cases;
- toolchains supporting multiple use-cases;
- approaches that preserve information continuity and traceability across the journey;
- demonstrations or pilots that test whether information can move through one or more journey segments without loss of context, provenance, authority, maturity, or trust.

The use case names are drawn from current planning material. The descriptions below are provided to structure respondent feedback and remain subject to validation through this RFI. Respondents may propose changes, additions, removals, or alternative groupings.

NATO UNCLASSIFIED

UC 1 – Coordination Across National, Multinational, and Common-Funded Delivery Routes

Field	Description
Use-case name	Coordination Across National, Multinational, and Common-Funded Delivery Routes
Journey layers involved	Defence planning; portfolio management; programmes
Description	NATO capability development depends on national, multinational, and common-funded delivery routes that may operate through different governance cycles, funding mechanisms, data structures, and reporting approaches. This use case concerns the coordination of those routes against common capability needs and planning outputs.
Stakeholders involved	Portfolio owners and stakeholders across national, multinational, and common-funded routes [TBD – to be confirmed].
Information inputs	Defence planning outputs, Capability Targets where applicable, existing investments, proposed initiatives, constraints, risks, dependencies, affordability information, and delivery-route information.
Information outputs	Cross-route portfolio views, investment alignment, gap analysis, dependency maps, delivery-route recommendations, and decision-support information.
Current pain points, issues, or risks	Different delivery routes may use different cycles, structures, and reporting formats. Cross-route traceability may be inconsistent. Gaps, overlaps, and dependencies may be difficult to identify early.
Expected digital enhancement	A coherent, evidence-based view of how national, multinational, and common-funded initiatives contribute to capability needs.
Type of tool or toolchain support sought	Portfolio mapping, dependency analysis, data integration, traceability, dashboarding, and decision-support tools.
Questions for respondents	How can NATO maintain traceability from capability needs to multiple delivery routes? What portfolio practices, methods, or tools should be considered?

NATO UNCLASSIFIED

UC 2 – End-to-End Change Impact Assessment and Reprioritisation

Field	Description
Use-case name	End-to-End Change Impact Assessment and Reprioritisation
Journey layers involved	Strategic concepts / strategic direction; political-military guidance or decision-making; defence planning; portfolio management; programmes; projects; suppliers / delivery ecosystem
Description	NATO must be able to assess how changes in strategic direction, operational need, risk, affordability, dependency, or delivery status affect the full capability development journey.
Stakeholders involved	Stakeholders across all journey layers [TBD – to be confirmed].
Information inputs	New or changed strategic direction, political-military decisions, changed priorities, operational lessons, risk information, portfolio data, delivery status, project baselines, supplier constraints, and evidence.
Information outputs	Impact assessments, reprioritisation options, updated plans, changed baselines, revised delivery forecasts, risk updates, and decision records.
Current pain points, issues, or risks	Change impacts may be difficult to trace across layers. Reprioritisation may be slow, manually intensive, or based on incomplete visibility of dependencies and consequences.
Expected digital enhancement	Auditable impact assessment and reprioritisation with visible links across strategic, planning, portfolio, programme, project, and supplier information.
Type of tool or toolchain support sought	Impact analysis, dependency mapping, traceability, scenario analysis, change control, portfolio optimisation, and reporting tools.
Questions for respondents	How can NATO rapidly assess the effect of change across the full journey? What information must be linked to make this possible?

NATO UNCLASSIFIED

NATO UNCLASSIFIED

UC 3 – Translation of Strategic Guidance into NDPP Capability Targets

Field	Description
Use-case name	Translation of Strategic Guidance into NATO Defence Planning Process Capability Targets
Journey layers involved	Strategic concepts / strategic direction; political-military guidance or decision-making; defence planning
Description	Strategic direction and political-military guidance must be translated into NATO Defence Planning Process (NDPP) outputs, including Capability Targets where applicable.
Stakeholders involved	Strategic, political-military, and NDPP stakeholders [TBD – to be confirmed].
Information inputs	Strategic concepts, strategic direction, political-military guidance, assumptions, constraints, threat and risk information [TBD – to be confirmed].
Information outputs	NDPP outputs, Capability Targets where applicable, planning assumptions, capability gaps, and priorities.
Current pain points, issues, or risks	Strategic direction may be broad, abstract, or document-centric. Assumptions and rationale may not be explicitly traceable. Downstream planning may require reinterpretation or reconstruction of context.
Expected digital enhancement	Improved traceability from strategic guidance to NDPP outputs and Capability Targets, with preserved context, assumptions, authority, and rationale.
Type of tool or toolchain support sought	Tools or methods for structured planning artefacts, traceability, decision mapping, requirements derivation, and information provenance.
Questions for respondents	How can strategic intent be digitally linked to NDPP outputs and Capability Targets? What methods have worked in comparable environments? What should NATO avoid?

NATO UNCLASSIFIED

NATO UNCLASSIFIED

UC 4 – Structured Handover of NDPP Outputs to Delivery Communities

Field	Description
Use-case name	Structured Handover of NDPP Outputs to Delivery Communities
Journey layers involved	Defence planning; portfolio management; programmes; projects
Description	NDPP outputs must be handed over to the communities responsible for portfolio management, programme definition, project execution, acquisition, and delivery. These handovers should preserve context, authority, assumptions, and traceability.
Stakeholders involved	NDPP stakeholders, portfolio stakeholders, programme and project communities [TBD – to be confirmed].
Information inputs	NDPP outputs, Capability Targets where applicable, decisions, priorities, risks, assumptions, and constraints.
Information outputs	Structured handover packages, baselined information, linked artefacts, decision records, downstream planning inputs, and delivery community tasking information.
Current pain points, issues, or risks	Handovers may be document-centric and inconsistent. Context and provenance may be lost. Delivery communities may need to reconstruct the rationale behind upstream outputs.
Expected digital enhancement	Structured handovers that preserve meaning, provenance, authority, maturity, and traceability.
Type of tool or toolchain support sought	Tools for information exchange, digital thread management, artefact linking, structured workflow, metadata management, and controlled baselining.
Questions for respondents	What is the most practical way to structure handovers from defence planning to delivery communities? What information should always be preserved?

NATO UNCLASSIFIED

NATO UNCLASSIFIED

UC 5 – Alignment of Common-Funded Portfolio Priorities and NSIP Investments to NDPP

Field	Description
Use-case name	Alignment of Common-Funded Portfolio Priorities and NATO Security Investment Programme Investments to NATO Defence Planning Process
Journey layers involved	Defence planning; portfolio management; programmes
Description	Common-funded portfolio priorities and NATO Security Investment Programme (NSIP) investments must be aligned with NDPP outputs and Capability Targets where applicable.
Stakeholders involved	Common-funded portfolio stakeholders, NSIP stakeholders, NDPP stakeholders, programme stakeholders [TBD – to be confirmed].
Information inputs	NDPP outputs, Capability Targets where applicable, common-funded portfolio data, NSIP investment data, programme information, constraints, risks, and dependencies.
Information outputs	Portfolio alignment views, investment priorities, gap analysis, dependency maps, recommendations, and decision-support information.
Current pain points, issues, or risks	Common-funded portfolio priorities and NSIP investments may be difficult to trace consistently to NDPP outputs. Dependencies and trade-offs may be manually maintained or incompletely visible.
Expected digital enhancement	Improved evidence-based alignment of common-funded portfolio priorities and NSIP investments to NDPP outputs and capability needs.
Type of tool or toolchain support sought	Portfolio mapping, dependency analysis, investment traceability, dashboarding, analytics, and decision-support tools.
Questions for respondents	How can NATO maintain traceability from NDPP outputs to common-funded portfolio priorities and NSIP investments? What methods or tools should be considered?

NATO UNCLASSIFIED

UC 6 – Integrated Programme Delivery of a Federated Capability

Field	Description
Use-case name	Integrated Programme Delivery of a Federated Capability
Journey layers involved	Portfolio management; programmes; projects; suppliers / delivery ecosystem
Description	Federated capabilities may require coordinated delivery across multiple programmes, projects, suppliers, organisations, and delivery routes. This use case concerns the digital support required to maintain alignment, dependency visibility, and evidence across that federation.
Stakeholders involved	Programme managers, project managers, portfolio stakeholders, technical stakeholders, assurance stakeholders, suppliers [TBD – to be confirmed].
Information inputs	Portfolio priorities, programme objectives, project baselines, supplier artefacts, dependency data, risk and issue information, delivery evidence, and constraints.
Information outputs	Programme plans, consolidated reporting, dependency views, risk escalation, programme decisions, updated constraints, and delivery evidence.
Current pain points, issues, or risks	Programme teams may reconstruct upstream context. Dependency visibility may be manual or delayed. Reporting may lag behind project reality. Supplier and project evidence may not be linked consistently to programme objectives.
Expected digital enhancement	Continuous alignment between programme objectives and project execution, with more timely dependency, risk, and evidence visibility.
Type of tool or toolchain support sought	Programme and project integration tools, dependency mapping, reporting automation, risk aggregation, baseline management, evidence integration, and supplier data exchange.
Questions for respondents	How can programme-level decision-making be supported by current project and supplier information without imposing excessive reporting burden?

NATO UNCLASSIFIED

UC 7 – Closed-Loop Reporting from Delivery to NDPP and Strategic Decision-Making

Field	Description
Use-case name	Closed-Loop Reporting from Delivery to NATO Defence Planning Process and Strategic Decision-Making
Journey layers involved	Projects; programmes; portfolio management; defence planning; political-military guidance or decision-making; strategic concepts / strategic direction
Description	Delivery evidence and status information must move upward through the journey to support portfolio, NDPP, political-military, and strategic decision-making. Decisions and updated priorities must then flow back down.
Stakeholders involved	Project, programme, portfolio, NDPP, political-military, and strategic decision stakeholders [TBD – to be confirmed].
Information inputs	Project status, test evidence, risks, issues, delivery forecasts, supplier evidence, programme reports, portfolio assessments, and capability progress information.
Information outputs	Aggregated delivery status, capability progress assessments, risks, gaps, recommendations, updated priorities, revised guidance, and decision records.
Current pain points, issues, or risks	Reporting may be manually aggregated, delayed, inconsistent, or disconnected from underlying evidence. Fidelity may be lost as information moves upward. Updated decisions may not be traceably connected to delivery evidence.
Expected digital enhancement	More reliable, evidence-based reporting that preserves links to source information and supports informed decision-making and feedback to delivery layers.
Type of tool or toolchain support sought	Evidence aggregation, reporting, dashboarding, traceability, analytics, decision-support, and feedback-loop tools.
Questions for respondents	How can NATO aggregate delivery information without losing evidence and context? What level of automation is realistic and useful?

NATO UNCLASSIFIED

UC 8 – Supplier Deliverables as Governed Evidence of Capability Delivery

Field	Description
Use-case name	Supplier Deliverables as Governed Evidence of Capability Delivery
Journey layers involved	Suppliers / delivery ecosystem; projects; programmes; portfolio management
Description	Supplier outputs should be usable not only as contractual deliverables but also as governed evidence that supports traceability through the capability development journey.
Stakeholders involved	Suppliers, contracting authorities, project teams, programme teams, assurance stakeholders [TBD – to be confirmed].
Information inputs	Contractual requirements, technical requirements, project baselines, supplier deliverables, evidence artefacts, acceptance criteria, and compliance information.
Information outputs	Governed supplier artefacts, accepted evidence, traceability links, assurance records, project baselines, and delivery status inputs.
Current pain points, issues, or risks	Supplier deliverables may be treated as static documents rather than reusable information assets. Provenance, format, versioning, metadata, and integration readiness may be insufficient. Evidence may not remain linked to requirements, acceptance criteria, or upstream objectives.
Expected digital enhancement	Supplier deliverables that retain provenance and can be integrated into NATO information flows without unnecessary rework.
Type of tool or toolchain support sought	Digital thread tools, controlled repositories, requirements/evidence linkage, supplier data exchange, configuration management, acceptance workflow support, and assurance repositories.
Questions for respondents	How can contracts and toolchains encourage supplier deliverables to function as governed evidence? What minimum metadata, structure, or traceability should be required?

NATO UNCLASSIFIED

5. Glossary

Term / Acronym	Definition
AAP-48	NATO publication referenced in source material as relevant to the Digital Process Operating Model. Applicability to future RFPs remains subject to confirmation.
AIDA	Architecture for Interoperability of Digital Technologies within the Alliance. Identified in source material as an authoritative integration point for certain interoperability artefacts.
Capability Target	A capability-related planning output used in the NATO Defence Planning Process where applicable.
CFCDGM	Common Funded Capabilities Development Governance Model. Referenced in source material in relation to common-funded capability governance.
DCD	Digital Capability Development. In this RFI, the NCIA team and initiative area concerned with digitally supporting capability development.
DIFA	Digital Interoperability Framework for the Alliance. Referenced in source material as a framework for digital interoperability.
DIOR	Digital Interoperability Roadmap. Referenced in source material in relation to interoperability sequencing and prioritisation.
Digital Engineering	An integrated digital approach using authoritative sources of data and models as a continuum across disciplines to support lifecycle activities.
DPF	Digital Processes Framework. The proposed framework for bringing digital processes supporting capability development into greater coherence.
DPOM	Digital Process Operating Model. The proposed operating model describing how digital work and information exchange may operate under the DPF.
DTIS	Digital Transformation Implementation Strategy. Referenced in source material as part of the wider digital policy context.
Industry respondents	Commercial or industrial organisations responding to this RFI, including large firms, small and medium-sized enterprises, integrators, consultancies, tool vendors, and specialist providers.
Information Exchange Requirement	A structured artefact through which information exchange obligations may be made explicit. Applicability to future RFPs remains subject to confirmation.
Interoperability Requirement	A structured artefact through which interoperability obligations may be made explicit. Applicability to future RFPs remains subject to confirmation.
MOSA	Modular Open Systems Architecture. In this RFI, used to refer to modular, open, interoperable approaches that reduce unnecessary lock-in where relevant.

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Term / Acronym	Definition
NATO Capability Development Journey	The journey described in this RFI from strategic direction through political-military guidance, defence planning, portfolios, programmes, projects, and suppliers.
NATO Nations	NATO member Nations responding directly or distributing the RFI to relevant national stakeholders.
NIAG	NATO Industrial Advisory Group.
IMCD	Information Management for Capability Delivery. In this RFI, the currently envisaged principal NATO Enterprise vehicle for implementing DPF, DPOM and Digital Engineering Directive concepts through practical information environments, tooling, processes, training, adoption and decision-support capabilities.
NATO EDGE	NATO industry engagement event referenced in this RFI as a potential route for structured market engagement, workshop discussion, demonstration scoping and follow-on dialogue, subject to applicable engagement and procurement rules.
Digital Engineering Directive	A domain-specific directive expected to specialise the common DPOM model for digital engineering and capability-development information. Its status, authority, scope, approval route and applicability remain subject to confirmation.
Digital Engineering Information Sets	Standardised sets of digital engineering information that NATO may need to require, exchange, create, manage, preserve and assure across lifecycle activities, including through NIAG and STANAG 4457-related work.
STANAG 4457	NATO standardisation agreement referenced in relation to Digital Engineering Information and potential future updates informed by NIAG study activity.
NCIA	NATO Communications and Information Agency.
NDPP	NATO Defence Planning Process.
NSF	NATO Software Factory. Referenced in this RFI only as a potential NATO-relevant environment for demonstrations or pilots, subject to confirmation.
NSIP	NATO Security Investment Programme.
RFI	Request for Information. A non-binding information-gathering request.
RFP	Request for Proposal. A potential future solicitation, subject to confirmation.
Use-case	An activity within a journey layer and/or a connection, handover, boundary, or information flow between journey layers.

NATO UNCLASSIFIED