Headquarters Supreme Allied Commander Transformation
Norfolk, Virginia

REQUEST FOR INFORMATION
RFI-ACT-SACT-23-42

This document contains a Request for Information (RFI) Call for Nations and Industry input to provide elements of NATO's

Education, Training, Exercises and Evaluation (ETEE)
Functional Services (FS) Capability

Those wishing to respond to this RFI should read this document carefully and in its entirety, and follow the guidance provided.

This RFI is open to NATO Nations and Industry that originate or are chartered/incorporated within NATO Nations.

HQ Supreme Allied Commander Transformation RFI 23-42 General Information	
Request For Information No.	23-42
Project Title	Request for Nations and Industry input to provide elements of NATO's Education, Training, Exercises and Evaluation (ETEE) Functional Services (FS) Capability.
Due date for questions concerning requested information	0900 hours EST, Norfolk, Virginia, USA on 26 APR 2023 (Phase I Only)
Due date for submission of requested information	0900 hours EST, Norfolk, Virginia, USA on 15 MAY 2023 (Phase I Only)
Contracting Office Address	NATO, HQ Supreme Allied Commander Transformation (SACT) Purchasing & Contracting Suite 100 7857 Blandy Rd, Norfolk, VA, 23511-2490
Contracting Point of Contact	Catherine Giglio Email: Catherine.Giglio@act.nato.int Tel: +1.757.747.3856 Magdalena Ornat Email: Magdalena.Ornat@act.nato.int Tel: +1.757.747.3150 Mark Macsule Email: Mark.macsule@act.nato.int Tel: +1.757.747.3360
Technical Points of Contact	Mr. Craig Ham Email: richard.ham@act.nato.int Tel: +1.757.747.4411 Mr. Paul Thurkettle Email: paul.thurkettle@act.nato.int Tel: +1.757.747.3360 Mr. Stuart Furness Email: stuart.furness@act.nato.int Tel: +1.757.747.3941
All requests for clarifications and responses to this RFI must be sent ***via email*** to ***ALL*** points of contact listed above.	

1 INTRODUCTION

1.1 **Summary.** Headquarters Supreme Allied Commander Transformation (HQ SACT) is issuing this Request for Information (RFI) in order to engage with Nations and Industry. The objective of this RFI is to identify existing and/or emerging technologies, systems and services in the area of Education, Training, Exercises and Evaluation (ETEE) Functional Services (FS). Identification of these capabilities will be used to support the NATO Governance decision-making on Common-Funded Capability Development.

1.2 This in an RFI **ONLY**. This RFI **DOES NOT** constitute a current Request for Proposal (RFP) nor a commitment to issue a future RFP. HQ SACT is not seeking proposals at this time; therefore, HQ SACT will not accept unsolicited proposals in respect to this RFI.

1.3 The purpose of this RFI is to involve Nations and Industry, through collaboration, in the development of the final set of ETEE FS Capability Requirements (CRs), the Capability Architecture, and to identify potential existing solutions for the ETEE FS Capability.

1.4 HQ SACT does not make any commitment to procure any of the systems, products or services described herein, and release of this RFI shall not be construed as such a commitment, nor as authorization to incur cost for which reimbursement will be required or sought. Further, respondents are advised that HQ SACT will not pay for any information or administrative costs incurred in responding to this RFI. The costs for responding to this RFI shall be borne solely by the responding party. Not responding to this RFI does not preclude participation in any subsequent RFP, if issued in the future.

2 PROGRAMME DESCRIPTION

2.1 **Background.** NATO ETEE FS enable the Alliance to conduct the full range of NATO ETEE activities and events to support the NATO ETEE roles and responsibilities and to, ultimately, improve Alliance readiness and operational effectiveness.

2.2 **Current State.** NATO ETEE FS currently consist of a number of disparate, stand-alone and stove piped systems and prototypes across the various areas of ETEE i.e., Education and Individual Training (E&IT), Collective Training & Exercises (CT&E) and Evaluations as well as the associated Lessons Learned (LL) systems.

2.3 **Desired End State.**

a. NATO ETEE FS shall be compliant with applicable C3, CIS Security, Information Management, NISP and STANAG requirements[1].

[1] Applicable sections of these documents are referenced in the Service Policy views in Annex A. The documents can be made available if necessary.

b. NATO ETEE FS shall also ensure data and information exchange with relevant services provided by other capabilities, both current and those currently under development, and commercial services, as necessary.

c. NATO ETEE FS shall provide:

- A coherent federated enterprise architecture that allows 'plug-and-play' interoperability across potentially diverse applications;
- Simultaneous collaborative working environments regardless of location;
- Common data repositories that aggregate local and global data, support automated data exchange and allow personnel across the NATO Enterprise to access, generate, organize, retrieve, exploit, store and dispose of associated data and information;
- Expandable capability and capacity; and
- Full lifecycle support.

2.4 Programme Status

a. At this time, a Capability Programme Plan (CPP) is under development which aims to direct the necessary actions across the NATO-recognised lines of development including: doctrine, organization, training, materiel (including software), leadership, personnel, facilities and interoperability.

b. The CPP will consist of a rigorous Analysis of Alternatives (AoA) intended to assist decision makers in the selection of a solution that offers the Alliance the most value for money. These solutions are informed by this RFI and consider the full spectrum of possible alternatives including considerations of "Adopt"-ing a solution, "Buy"-ing (acquiring a solution from industry), or "Create"-ing (developing a solution bespoke to NATO), known as ABC. Options are evaluated along the lines of operational effectiveness, risk, timeline and life cycle costs.

3 HQ SACT FRAMEWORK FOR COLLABORATIVE INTERACTION

3.1 ACT has implemented a Framework for Collaborative Interaction (FFCI) to increase opportunities for industry to contribute to ACT's capability development efforts through collaborative work. Extensive information on the HQ SACT FFCI initiative can be found on the ACT website being developed to support FFCI projects at http://www.act.nato.int/ffci.

3.2 No FFCI agreement is required to respond to this RFI. However, the principles underlying the FFCI initiative apply to this RFI.

4 REQUESTED INFORMATION

4.1 This RFI will be conducted in three (3) distinct phases:

a. **Phase I:** The first phase will consist of an "Industry Day" to be held 11 – 13 JUL 2023 at the Joint Force Training Centre (JFTC) in Bydgoszcz, POL. This event will be an open Question and Answer (Q&A) session during which stakeholders will be available to discuss and answer questions on the draft CRs and Capability Architecture[2] included at Annex A. The goal of this event is to engage with Industry and Nations in an effort to finalise the CRs such that they are relevant and clear not only to stakeholders but also to potential vendors and suppliers. While in-person participation at the Industry Day is preferred and encouraged, given current real-word situations and constraints, the event will be conducted in a hybrid format.

The **required responses for Phase I** shall be notifications of intent to participate in the Industry Day to be held 11 – 13 JUL 2023 at JFTC in Bydgoszcz, POL. The response shall include your intent to participate in the Industry day, whether you will be participating in-person or virtually, and primary and secondary POCs for your organisation.

NOTE: Confirmed in-person participants for Phase I will be provided specific information for the event once final arrangements are made, and confirmed virtual participants will be provided the GoTo Meeting link. Information will be distributed to the points of contact (POCs) provided.

NOTE: While participation in Phase I is encouraged, it is **NOT** required for participation in Phase II.

b. **Phase II:** Once Phase I is complete, feedback from the Industry Day will be incorporated, and the CRs will be finalised and the architecture revised. Once finished, a revision to this RFI will be submitted in July 2023 to include:

- The final requirements set,
- A requirements survey,
- The revised Capability Architecture, and
- Proposed Project Description Sheets (PDS).

The requirements survey will allow respondents to offer a self-assessment of potential solutions for consideration to meet the ETEE FS CRs, while the proposed PDS will allow respondents to provide initial project estimates. The information

[2] The Capability Architecture is in accordance with the NATO Architecture Framework (NAF), Version 4. For the purpose of this RFI, the Capability Architecture is limited to Standard Processes, Service Functions, Service Policy, Node Types and Logical Activities.

collected in this survey will be used to support identification of participants for Phase III, and to inform the AoA for the CPP.

The **required responses for Phase II** shall include survey inputs and initial project estimates for potential solutions. Responses shall not contain any classified information. For the survey, information shall be entered into the Microsoft Excel spreadsheet that will be provided in the revision to this RFI. The information provided in the survey shall include:

- A Capability Overview, and
- A Capability Requirements Self-assessment.

For the initial project estimates, information shall be entered into the Microsoft Word template that will be provided in the revision to this RFI. The information provided in the project estimates shall be based on the survey responses, and shall include, at a minimum:

- Estimated timeframe for implementation,
- License Options (to include bulk options, and options by location and/or number of users),
- Estimated initial investment costs (to include license, software, and hardware (if applicable) costs), and
- Estimated lifecycle operation and maintenance (O&M) costs (to include license renewal, technology upgrade/refresh, and change management costs).

NOTE: Participation in Phase II is **mandatory** for potential selection for participation in Phase III. Participants for Phase III will be selected based on an analysis of the responses received in Phase II.

NOTE: Combined responses from industries, Nations, industries and Nations, etc., to fulfil all or sections of the requirements will be acceptable in Phase II.

c. **Phase III:** Phase III will consist of trials and demonstrations of potential solutions and is currently scheduled to be held 3 – 5 OCT 2023 at the Joint Force Training Centre (JFTC) in Bydgoszcz, POL. As noted previously, participants for Phase III will be selected based on an analysis of the responses received in Phase II.

The **required responses from selected participants for Phase III** shall be notifications of intent to participate in the Demonstrations currently scheduled to be held 3 – 5 OCT 2023 at JFTC in Bydgoszcz, POL. The response shall include

your intent to participate in the demonstrations, the expected number of participants from your organisation and any specific requirements for demonstrating potential solutions.

NOTE: The dates and/or location for Phase III are subject to change. Selected participants will be notified via the POCs provided (refer to Paragraph 4.1.a of this RFI) of the confirmed dates and location, as well as specific information for the event.

NOTE: Combined demonstrations from industries, Nations, industries and Nations, etc., to fulfil all or sections of the requirements will be acceptable in Phase III.

4.2 **Eligibility to Respond.** Only NATO Nations and Industry that originate or are chartered/incorporated within NATO Nations are eligible to respond to this RFI. Companies from Partner Nations who want to participate should partner with a primary company headquartered within a NATO Nation.

4.3 **Responses to the RFI.** The response(s) to this RFI may be submitted via e-mail to ***all*** the POCs listed on page 2 of this RFI.

4.4 **Response Dates.** Responses for Phase I of this RFI must be received by **0900 hours EST, Norfolk, Virginia, USA on 15 MAY 2023**. The response date for Phase II will be set in the revision to this RFI. The response date for Phase III will be set once participants are selected.

4.5 **Clarifications and Questions.**

a. Inquiries of a technical nature about this RFI shall be submitted by e-mail to ***all*** the POCs listed on page 2 of this RFI by **0900 hours EST, Norfolk, Virginia, USA on 26 APR 2023.** Additionally, questions shall not contain proprietary and/or classified information.

b. Answers will be posted on the HQ SACT P&C website at: www.act.nato.int/contracting.

c. HQ SACT reserves the right to seek clarification on any submission.

4.6 **Intent/Objectives.** The intent of this RFI is to involve Nations and Industry, through collaboration, in final development of the ETEE FS CRs and Capability Architecture. The objective is to identify potential solutions for the ETEE FS Capability.

4.7 **Expected Benefits to Respondents.** National and Industry participants will have the chance to reveal state-of-the-art systems, products and services in the area of ETEE FS to NATO.

4.8 **Expected Benefits to NATO.** The expected benefits include collaboration with

Nations and industry in the finalisation of the ETEE FS CRs and Capability Architecture, and the identification potential state-of-the-art solutions for the ETEE FS Capability.

4.9 **Classified Information.** NATO information that is CLASSIFIED is not included herein but can be passed to authorized industry recipients with appropriate clearances and control measures.

4.10 **Proprietary information.** Proprietary information, if any, should be minimized and clearly marked as such. HQ SACT will treat proprietary information with the same due care as the command treats its own proprietary information, and will exercise due caution to prevent its unauthorized disclosure. Please be advised that all submissions become HQ SACT property and will not be returned.

5 NON-DISCLOSURE PRINCIPLES AND/OR NON-DISCLOSURE AGREEMENT WITH THIRD PARTY COMPANY

5.1 Please be informed that HQ SACT may contract a company to conduct the AoA investigation in support of this project. HQ SACT will follow nondisclosure principles and possibly conclude a Non-Disclosure Agreement (NDA) with that company to protect submitted information from further disclosure. As the third party beneficiary of this nondisclosure, this RFI serves to inform you of how HQ SACT plans to proceed and of HQ SACT's intent to protect information from unauthorized disclosure, requiring the third party company to protect the disclosed information using the highest degree of care that the company utilizes to protect its own Proprietary Information of a similar nature, and no less than reasonable care. This includes the following responsibilities and obligations:

a. The third party company receiving the information shall not, without explicit, written consent of HQ SACT:

- Discuss, disclose, publish or disseminate any Proprietary Information received or accessed under nondisclosure principles and subject to an NDA, if an NDA is concluded;

- Use disclosed Proprietary Information in any way except for the purpose for which it was disclosed in furtherance of the goals of the instant project, collaboration, activity or contract; or

- Mention the other Party or disclose the relationship including, without limitation, in marketing materials, presentations, press releases or interviews

b. Exceptions to Obligations. The third party company receiving the information may disclose, publish, disseminate, and use Proprietary Information:

- To its employees, officers, directors, contractors, and affiliates of the recipient who have a need to know and who have an organizational code of

conduct or written agreement with the recipient requiring them to treat the disclosed Proprietary Information in accordance with nondisclosure principles and the NDA (if executed);

- To the extent required by law; however, the company receiving the information will give HQ SACT prompt notice to allow HQ SACT a reasonable opportunity to obtain a protective order or otherwise protect the disclosed information through legal process; or

- That is demonstrated in written record to have been developed independently or already in the possession of the company receiving the information without obligation of confidentiality prior to the date of receipt from HQ SACT; that is disclosed or used with prior written approval from HQ SACT; obtained from a source other than HQ SACT without obligation of confidentiality; or publicly available when received.

c. Any response to this RFI is considered to establish consent to this process. A copy of the NDA, if or when concluded, can be provided on request.

6 EXCEPTIONS TO OBLIGATIONS

6.1 The third party company receiving the information may disclose, publish, disseminate, and use Proprietary Information:

a. To its employees, officers, directors, contractors, and affiliates of the recipient who have a need to know and who have an organizational code of conduct or written agreement with the recipient requiring them to treat the disclosed Proprietary Information in accordance with nondisclosure principles and the NDA (if executed);

b. To the extent required by law; however, the company receiving the information will give HQ SACT prompt notice to allow HQ SACT a reasonable opportunity to obtain a protective order or otherwise protect the disclosed information through legal process; or

c. That is demonstrated in written record to have been developed independently or already in the possession of the company receiving the information without obligation of confidentiality prior to the date of receipt from HQ SACT; that is disclosed or used with prior written approval from HQ SACT; obtained from a source other than HQ SACT without obligation of confidentiality; or publicly available when received.

6.2 Any response to this RFI is considered to establish consent to this process. A copy of the NDA, if or when concluded, can be provided on request.

7 ORGANIZATIONAL CONFLICTS OF INTEREST

7.1 As Procurement/Contracting involves the expenditure of funds allocated by the member nations, we must always strive to maintain trust in and preserve the integrity of this Headquarters' procurement procedures. It is essential that our procedures facilitate transparent and robust competition from industry. Contractor and subcontractor personnel performing work under an HQ SACT contract may receive, have access to, or participate in the development of sensitive information relating to source selection methodology, cost or pricing information, budget information, and future specifications, requirements or Statements of Work or perform evaluation services that may create a current or subsequent Organizational Conflict of Interests (OCI). Similarly, companies responding to an HQ SACT RFI may create a subsequent OCI determination when pursuing future NATO contracts generated from that RFI. Each individual contracting situation will of course be examined on the basis of its particular facts and the nature of any proposed contract. The exercise of common sense, good judgment, and sound discretion is required in both the decision on whether a significant potential conflict exists and, if it does, the development of an appropriate means for resolving it. In anticipation of a future OCI determination, any company either awarded an HQ SACT contract or responding to an HQ SACT RFI while also anticipating bidding on future NATO contracts relating to this work, should consider having a mitigation plan in place to address or mitigate any OCI concerns now or in the future.

8 FOLLOW-ON

8.1 Any and all information provided as part of the submission in response to this RFI may be considered in developing any future HQ SACT requirements.

8.2 The data collected in response to this RFI will be used to develop a report to inform the ETEE FS CPP. The report will provide an assessment to support a decision as to whether NATO should pursue an ABC approach to meet ETEE FS requirements.

8.3 In the event that there is a competitive bidding process later as part of NATO Common Funded Capability Development, the provision of data, or lack of, will not prejudice any respondent.

9 SUMMARY

9.1 The purpose of this RFI is to involve Nations and Industry, through collaboration, in final development of the ETEE FS Capability CRs and Capability Architecture, and to identify potential solutions for the ETEE FS Capability. HQ SACT has not made a commitment to procure any of the systems, products or services described herein, and release of this RFI shall not be construed as such a commitment, nor as authorization to incur cost for which reimbursement will be required or sought. **It is emphasised that this is an RFI only, and not an RFP of any kind.** Thank you in advance for your time and submission to this RFI.

Education, Training, Exercises and Evaluations (ETEE)
Functional Services (FS)

Capability Architecture

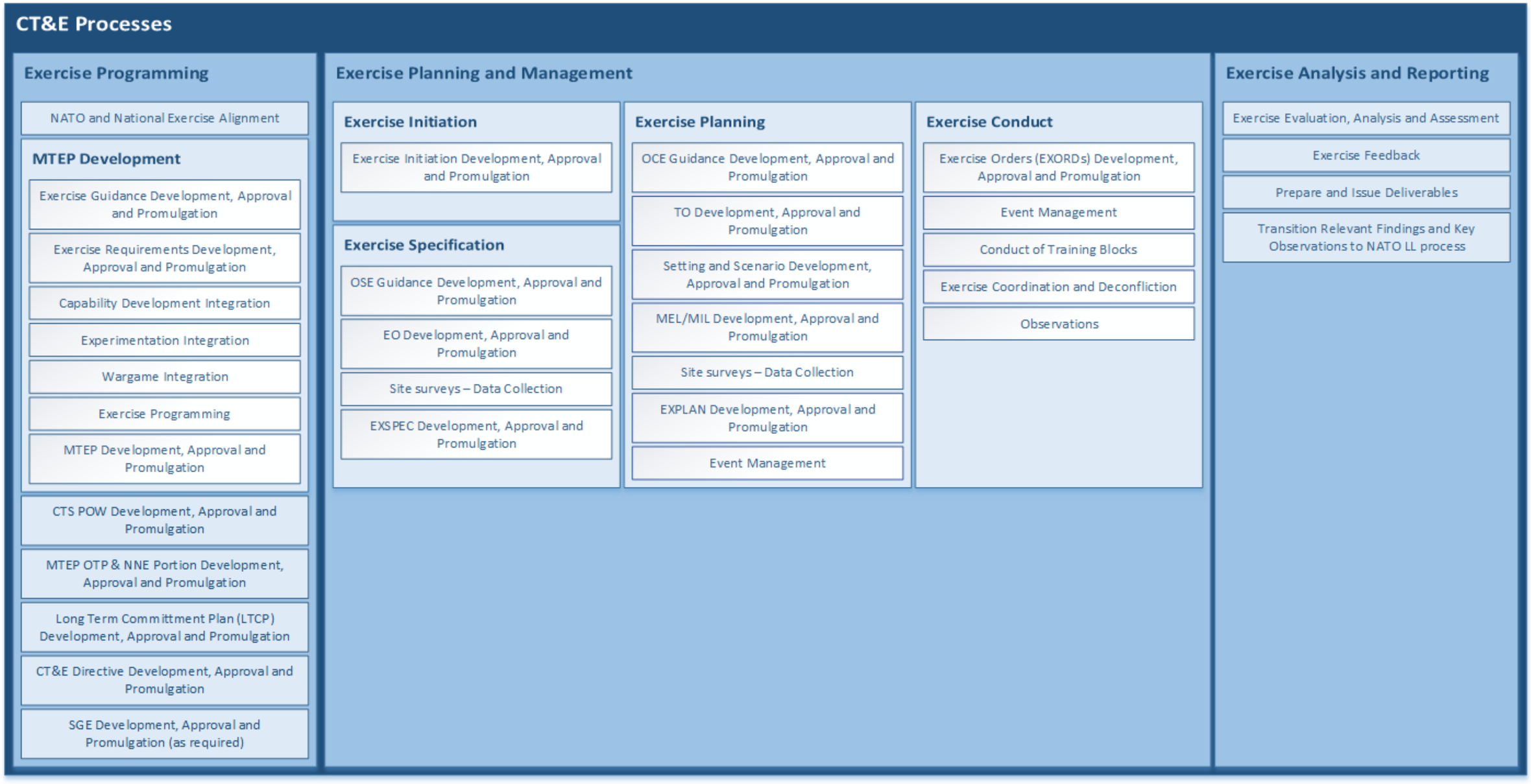
Version 3.0

Products are in DRAFT form and have yet to be fully vetted and peer-reviewed.

Contents

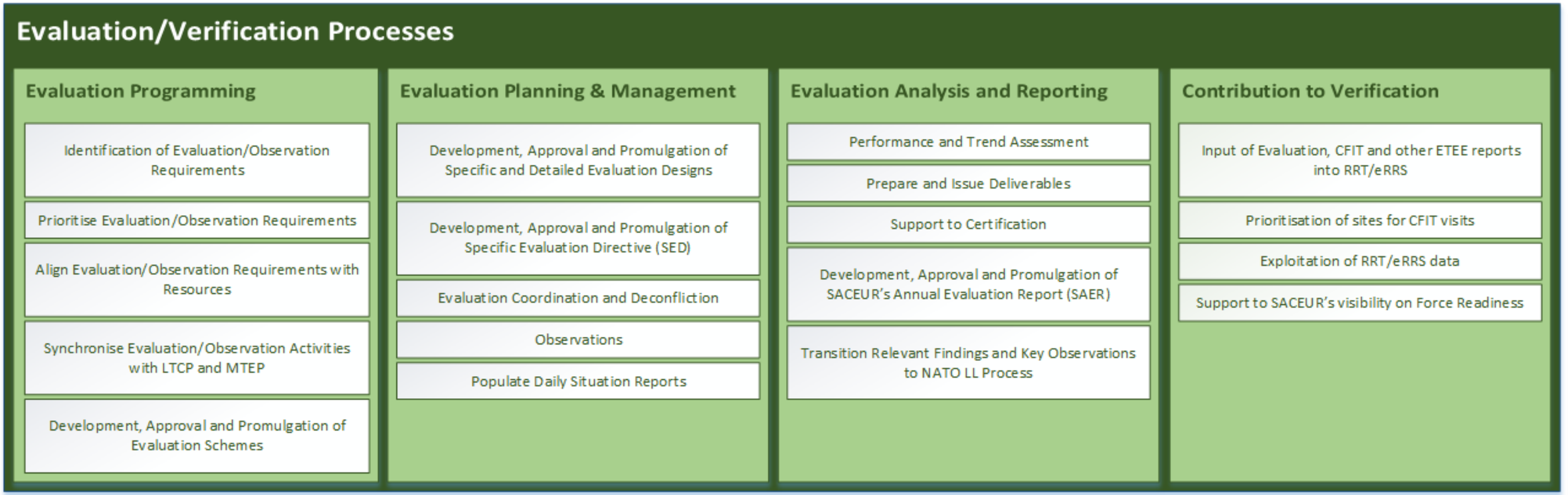
C4 – Standard Processes (CT&E)	NAFv3: NCV-6

The C4 Viewpoint is concerned with identification of enduring tasks and standard activities relevant for the architecture. The following model describes the recurring Collective Training and Exercises (CT&E) stakeholder processes that ETEE FS will support.

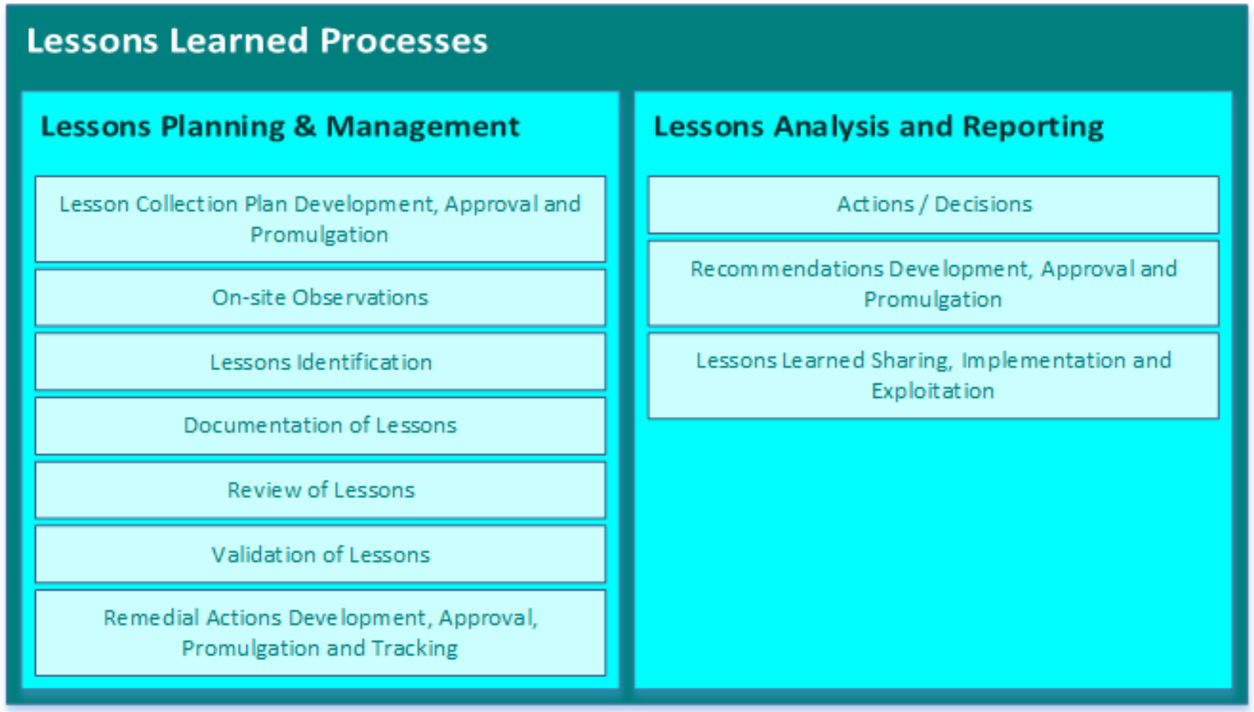


C4 – Standard Processes (Evaluations)	**NAFv3: NCV-6**

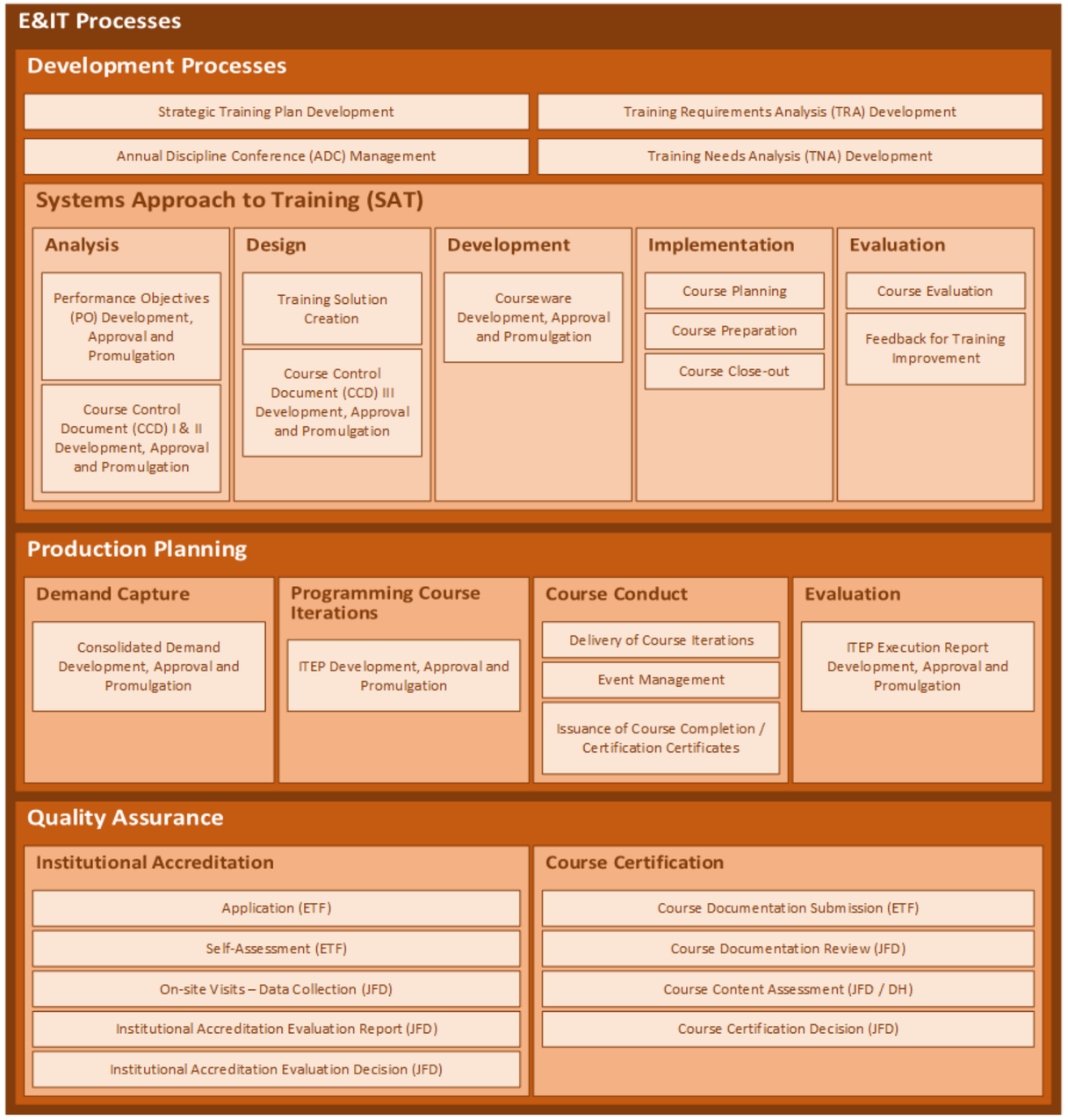
The C4 Viewpoint is concerned with identification of enduring tasks and standard activities relevant for the architecture. The following model describe the recurring Evaluation/Verification stakeholder processes that ETEE FS will support.



C4 – Standard Processes (Lessons Learned)	NAFv3: NCV-6
The C4 Viewpoint is concerned with identification of enduring tasks and standard activities relevant for the architecture. The following model describe the recurring Lessons Learned stakeholder processes that ETEE FS will support.	



C4 – Standard Processes (E&IT)	NAFv3: NCV-6
The C4 Viewpoint is concerned with identification of enduring tasks and standard activities relevant for the architecture. The following model describe the recurring Education and Individual Training (E&IT) stakeholder processes that ETEE FS will support.	



S4 – Service Functions (CR 1.0)	NAFv3: NSOV-3

The S4 Viewpoint is concerned with the definition of the behaviour of a service in terms of the functions it is expected to perform. The following table lists the required service functionalities, in the form of capability requirements (CRs), for the programming (i.e., scheduling) of NATO ETEE events and activities.

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
1.0					ETEE FS shall facilitate programming of NATO ETEE events and activities within different security domains without provider support.	Must
	1.1				ETEE FS shall facilitate NATO Collective Training and Exercises (CT&E) and Evaluations/Verifications programming within different security domains without provider support.	Must
		1.1.1			ETEE FS shall facilitate programming of NATO Exercises.	Must
			1.1.1.1		ETEE FS shall facilitate the collection of NATO and National exercise plans.	Must
			1.1.1.2		ETEE FS shall facilitate the collection of NATO CT&E requirements.	Must
			1.1.1.3		ETEE FS shall facilitate the management of NATO Exercise programme plans as defined in CR 4.5.	Must
				1.1.1.3.1	EETE FS shall be capable of identifying scheduling conflicts automatically in NATO Exercise programme plans.	Must
				1.1.1.3.2	EETE FS shall be able to provide visualizations of NATO Exercise plans in user-defined formats.	Must
			1.1.1.4		ETEE FS shall facilitate the management of NATO Collective Training Support requirements as defined in CR 4.5.	Must
			1.1.1.5		ETEE FS shall facilitate the management of the Open to Partners and Non-NATO Entities (OTP & NNE) portion of the MTEP as defined in CR 4.5.	Must
		1.1.2			ETEE FS shall facilitate the programming of NATO Evaluations/Verifications.	Must
			1.1.2.1		ETEE FS shall support the collection of Evaluation/Verification requirements.	Must
			1.1.2.2		ETEE FS shall facilitate the management of NATO Evaluation/Verification programme plans as defined in CR 4.5.	Must
				1.1.2.2.1	EETE FS should be capable of automatically identifying scheduling conflicts in NATO Evaluation/Verification programme plans.	Should
				1.1.2.2.2	EETE FS should be capable of providing visualizations of NATO Evaluation/Verification programme plans in user-defined formats.	Should
	1.2				ETEE FS shall facilitate NATO Education and Individual Training (E&IT) programming within different security domains without provider support.	Must
		1.2.1			ETEE FS shall facilitate the identification of NATO E&IT training requirements.	Must
			1.2.1.1		ETEE FS shall facilitate the collection of training requirements.	Must
			1.2.1.2		ETEE FS shall facilitate the alignment of training requirements with available training opportunities.	Must
			1.2.1.3		ETEE FS shall facilitate the management of Training Requirements Analysis (TRA) reports as defined in CR 4.5.	Must
		1.2.2			ETEE FS shall facilitate the analysis of training requirements.	Must
			1.2.2.1		ETEE FS shall facilitate the management of training analysis products as defined in CR 4.5.	Must
		1.2.3			ETEE FS shall facilitate the design of training solutions.	Must
			1.2.3.1		ETEE FS shall facilitate the management of training design products as defined in CR 4.5.	Must
		1.2.4			ETEE FS shall facilitate the management of training solutions.	Must
			1.2.4.1		ETEE FS shall facilitate the management of training support products and materials as defined in CR 4.5.	Must
			1.2.4.2		ETEE FS shall facilitate the programming of training solutions.	Must

S4 – Service Functions (CR 2.0)	NAFv3: NSOV-3

The S4 Viewpoint is concerned with the definition of the behaviour of a service in terms of the functions it is expected to perform. The following table lists the required service functionalities, in the form of capability requirements (CRs), for the management, execution analysis and reporting of NATO ETEE events and activities.

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
2.0					ETEE FS shall facilitate management and execution of NATO ETEE events and activities within different security domains without provider support.	Must
	2.1				ETEE FS shall facilitate the management and execution of NATO Exercises within different security domains without provider support.	Must
		2.1.1			ETEE FS shall facilitate the management of CT&E planning products as defined in CR 4.5.	Must
			2.1.1.1		ETEE FS shall be capable of exchanging exercise design data with external tools and services.	Must
		2.1.2			ETEE FS shall facilitate the management of setting data as defined in CR 4.5.	Must
			2.1.2.1		ETEE FS shall allow authorised users to create setting data in in a single source system.	Must
			2.1.2.2		ETEE FS shall allow initialisation of a specific scenario based on a setting.	Must
			2.1.2.3		ETEE FS shall allow visualisation of setting data in user-defined formats.	Must
		2.1.3			ETEE FS shall facilitate the management of scenario data as defined in CR 4.5.	Must
			2.1.3.1		ETEE FS shall allow authorised users to create scenario data in in a single source system.	Must
			2.1.3.2		ETEE FS shall allow visualisation of scenario data in user-defined formats.	Must
		2.1.4			ETEE FS shall facilitate the management of CT&E objectives as defined in CR 4.5.	Must
			2.1.4.1		ETEE FS shall allow authorised users to track CT&E objective implementation during exercise design and scripting.	Must
			2.1.4.2		ETEE FS should allow authorised users to view real-time CT&E objective implementation data in configurable dashboards.	Should
		2.1.5			ETEE FS shall facilitate the management of Exercise content as defined in CR 4.5.	Must
			2.1.5.1		ETEE FS shall be capable of exchanging exercise design data with external tools and services.	Must
		2.1.6			ETEE FS shall facilitate the execution of NATO Exercises.	Must
			2.1.6.1		ETEE FS shall facilitate the dynamic management of Exercise events.	Must
			2.1.6.2		ETEE FS shall be able to provide a real-time customisable Exercise Control (EXCON) Common Operational Picture (COP).	Must
				2.1.6.2.1	ETEE FS shall be able to display the current exercise picture.	Must
				2.1.6.2.2	ETEE FS should be able to display pending exercise events in accordance with user-defined criteria.	Should
				2.1.6.2.3	ETEE FS should be able to provide geographical overlays for displays in accordance with Open Geospatial Consortium (OGC) standards.	Should
			2.1.6.3		ETEE FS shall allow authorised users to track real-time objective achievement during exercise execution.	Must
				2.1.6.3.1	ETEE FS should allow authorised users to view real-time CT&E objective achievement results in configurable dashboards.	Should
			2.1.6.4		ETEE FS shall allow real-time collection of observations in user-defined formats.	Must
				2.1.6.4.1	ETEE FS shall facilitate the identification of lessons and best practices from observations.	Must
				2.1.6.4.2	ETEE FS shall support the documentation of lessons and best practices in user-defined formats.	Must
				2.1.6.4.3	ETEE FS shall allow authorised users to manage lessons and best practices as defined in CR 4.5.	Must
				2.1.6.4.4	ETEE FS shall allow authorised users to track the validation, approval and implementation of lessons and best practices.	Must
				2.1.6.4.5	ETEE FS shall be capable of exchanging observation data with external tools and services.	Must
		2.1.7			ETEE FS shall facilitate the exploitation of CT&E data as defined in CR 4.4.	Must
	2.2				ETEE FS shall facilitate the management and execution of NATO Evaluations and Observations within different security domains without provider support.	Must
		2.2.1			ETEE FS shall facilitate the management of Evaluation design.	Must

ANNEX A to RFI-ACT-SACT-23-42

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
			2.2.1.1		ETEE FS shall facilitate the management of Evaluation design requirements as defined in CR 4.5.	Must
			2.2.1.2		ETEE FS shall facilitate the management of Evaluation Objectives as defined in CR 4.5.	Must
				2.2.1.2.1	ETEE FS shall allow authorised users to track Evaluation Objective implementation during exercise design and scripting.	Must
				2.2.1.2.2	ETEE FS should allow authorised users to view real-time Evaluation Objective implementation data in configurable dashboards.	Should
			2.2.1.3		ETEE FS shall facilitate the management of Evaluation content as defined in CR 4.5.	Must
		2.2.2			ETEE FS shall facilitate the execution of NATO Evaluations.	Must
			2.2.2.1		ETEE FS shall facilitate the dynamic management of NATO Evaluations.	Must
			2.2.2.2		ETEE FS shall allow authorised users to track Evaluation Objective achievement during exercise execution.	Must
				2.2.2.2.1	ETEE FS should allow authorised users to view real-time Evaluation Objective achievement results in configurable dashboards.	Should
			2.2.2.3		ETEE FS shall allow real-time collection of evaluation data in user-defined formats.	Must
				2.2.2.3.1	ETEE FS shall be capable of exchanging evaluation data with external tools and services.	Must
		2.2.3			ETEE FS shall facilitate the exploitation of Evaluation data as defined in CR 4.4.	Must
	2.3				ETEE FS shall facilitate management, execution and implementation of NATO Lessons Learned from NATO operations, missions and activities, as defined in the NATO Lessons Learned Policy, within different security domains without provider support.	Must
		2.3.1			ETEE FS shall facilitate the management of Lessons Collection Plan as defined in CR 4.5.	Must
		2.3.2			ETEE FS shall allow real-time collection of observations in user-defined formats.	Must
			2.3.2.1		ETEE FS shall allow users to submit observations anonymously in accordance with user-defined authorisation policies.	Must
			2.3.2.2		ETEE FS shall allow authorised users to manage observations as defined in CR 4.5.	Must
		2.3.3			ETEE FS shall facilitate the identification and documentation of lessons.	Must
			2.3.3.1		ETEE FS shall allow authorised users to manage lessons as defined in CR 4.5.	Must
		2.3.4			ETEE FS shall allow authorised users to plan remedial actions.	Must
			2.3.4.1		ETEE FS shall allow authorised users to manage remedial actions as defined in CR 4.5.	Must
			2.3.4.2		ETEE FS shall allow authorised users track the implementation of remedial actions.	Must
		2.3.5			ETEE FS shall facilitate the exploitation of Lessons data as defined in CR 4.4.	Must
		2.3.6			ETEE FS shall facilitate the dissemination of Lessons Learned products as defined in CR 4.5.	Must
	2.4				ETEE FS shall facilitate the management and execution of NATO Education and Individual Training (E&IT) within different security domains without provider support.	Must
		2.4.1			ETEE FS shall facilitate training management.	Must
			2.4.1.1		ETEE FS shall allow authorised users to schedule training solutions.	Must
			2.4.1.2		ETEE FS shall allow authorised users to manage Individual Training Plans (ITPs) based on user-defined criteria.	Must
			2.4.1.3		ETEE FS shall allow authorised users to manage learning paths without provider support.	Must
			2.4.1.4		ETEE FS shall allow authorised users to track student progress.	Must
			2.4.1.5		ETEE FS shall allow authorised users to manage testing and assessment material without provider support.	Must
		2.4.2			ETEE FS shall provide a repository of course and course iteration information.	Must
			2.4.2.1		ETEE FS shall allow users to access the repository based on user-defined permissions.	Must
			2.4.2.2		ETEE FS shall allow authorised users to manage templates within the course repository.	Must
			2.4.2.3		ETEE FS shall allow authorised users to manage information within the course repository.	Must

ANNEX A to RFI-ACT-SACT-23-42

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
			2.4.2.4		ETEE FS shall allow users to search and filter repository data as defined in CR 4.5.4.5.	Must
			2.4.2.5		ETEE FS shall allow authorised users to customise the repository user interface without provider support.	Must
			2.4.2.6		ETEE FS shall be able to send notifications of changes or updates to course information or status automatically based on user-defined criteria.	Must
			2.4.2.7		ETEE FS shall allow authorised users to send manual notifications of changes or updates to course information or status.	Must
			2.4.2.8		ETEE FS shall be able to validate course repository inputs automatically based on user-defined criteria.	Must
		2.4.3			ETEE FS shall facilitate the exploitation of individual training execution data as defined in CR 4.4.	Must
	2.5				ETEE FS shall facilitate NATO Quality Assurance management within different security domains without provider support.	Must
		2.5.1			ETEE FS shall facilitate NATO Institutional Accreditation management.	Must
			2.5.1.1		ETEE FS shall allow authorised users to manage Institutional Accreditation requirements without provider support.	Must
			2.5.1.2		ETEE FS shall allow institutions to submit accreditation requirements electronically, to include supporting documentation.	Must
			2.5.1.3		ETEE FS shall facilitate the exploitation of institutional accreditation data as defined in CR 4.4.	Must
			2.5.1.4		ETEE FS should be able to notify institutions automatically of changes in accreditation status in accordance with user-defined criteria.	Should
			2.5.1.5		ETEE FS should be able to notify institutions automatically of pending accreditation status requirements in accordance with user-defined criteria.	Should
		2.5.2			ETEE FS shall facilitate NATO Course Certification (NCC) management.	Must
			2.5.2.1		ETEE FS shall allow authorised users to manage course certification requirements without provider support.	Must
			2.5.2.2		ETEE FS shall allow institutions to submit course certification requests electronically, to include required supporting documentation.	Must
			2.5.2.3		ETEE FS shall allow authorised users to adjudicate course certifications requests.	Must
			2.5.2.4		ETEE FS should be able to notify institutions automatically of changes in certification status in accordance with user-defined criteria.	Should
	2.6				ETEE FS shall facilitate management of internal business processes within different security domains without provider support.	Must
		2.6.1			ETEE FS shall allow authorised users to define process requirements without provider support.	Must
		2.6.2			ETEE FS shall allow authorised users to manage processes without provider support.	Must
		2.6.3			ETEE FS shall allow authorised users to implement processes without provider support.	Must
		2.6.4			ETEE FS shall allow authorised users to automate and digitize processes without provider support.	Must
	2.7				ETEE FS should facilitate event coordination and management within different security domains without provider support.	Should
		2.7.1			ETEE FS should facilitate event scheduling.	Should
			2.7.1.1		ETEE FS should allow authorised users to duplicate past events, to include all information and supporting files.	Should
			2.7.1.2		ETEE FS should allow authorised users to manage event requirements.	Should
				2.7.1.2.1	ETEE FS should be able to identify event requirements automatically based on user-defined criteria.	Should
			2.7.1.3		ETEE FS should be able to identify scheduling conflicts automatically.	Should
			2.7.1.4		ETEE FS should allow authorised users to manage event calendars.	Should
			2.7.1.5		ETEE FS should allow authorised users to manage event specific landing/web site.	Should
		2.7.2			ETEE FS should facilitate event management.	Should
			2.7.2.1		ETEE FS should provide dynamic and customisable online registration options.	Should
			2.7.2.2		ETEE FS should allow authorised users to manage attendee accounts as defined in CR 4.1.2.	Should
			2.7.2.3		ETEE FS should allow event attendees to manage their accounts as defined in CR 4.1.3.	Should
			2.7.2.4		ETEE FS should allow authorised users to manage specific aspects of an event.	Should
				2.7.2.4.1	ETEE FS should allow authorised users to manage tasks associated with an event.	Should

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
				2.7.2.4.2	ETEE FS should allow authorised users to manage financial aspects of an event.	Should
				2.7.2.4.3	ETEE FS should allow authorised users to manage resource allocation for an event.	Should
				2.7.2.4.4	ETEE FS should allow authorised users to manage the security aspects of an event.	Should
				2.7.2.4.5	ETEE FS should allow authorised users to manage support requirements for an event.	Should
				2.7.2.4.6	ETEE FS should allow authorised users to manage contributors/speakers for an event	Should
				2.7.2.4.7	ETEE FS should allow authorised users to manage the marketing aspects of an event.	Should
				2.7.2.4.8	ETEE FS should be able to identify conflicts in event plans and schedules automatically in accordance with user-defined criteria.	Should
				2.7.2.4.9	ETEE FS should allow authorised users to manage event completion requirements, to include completion certificate submission and attendee accreditation/certification, as appropriate.	Should
			2.7.2.5		ETEE FS should provide dynamic and customisable event survey options.	Should
			2.7.2.6		ETEE FS should facilitate the exploitation of event data as defined in CR 4.4.	Should

S4 – Service Functions (CR 3.0)	NAFv3: NSOV-3

The S4 Viewpoint is concerned with the definition of the behaviour of a service in terms of the functions it is expected to perform. The following table lists the required service provision aspects, in the form of capability requirements (CRs), related to user manuals and guides for the ETEE FS Capability.

CR ID					*Requirement Statement*	*Priority*
Tier 1	*Tier 2*	*Tier 3*	*Tier 4*	*Tier 5*		
3.0					ETEE FS provision shall include necessary electronic manuals and guides for each service and application, by version.	Must
	3.1				ETEE FS provision shall include electronic User manuals and guides for each service and application, by version.	Must
	3.2				ETEE FS provision shall include electronic Technical Administrator manuals and guides for each service and application, by version.	Must
	3.3				ETEE FS provision shall include electronic Functional Administrator manuals and guides for each service and application, by version.	Must
	3.4				ETEE FS provision shall allow for customer review and assessment of training manuals and guides prior to acceptance.	Must
	3.5				ETEE FS should include a help function for each service and application.	Should
	3.6				ETEE FS should include a training mode for each service and application.	Should

S4 – Service Functions (CR 4.0)	NAFv3: NSOV-3

The S4 Viewpoint is concerned with the definition of the behaviour of a service in terms of the functions it is expected to perform. The following table lists the required service functionalities, in the form of capability requirements (CRs), for the collaboration among ETEE stakeholders.

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
4.0					ETEE FS shall facilitate seamless collaboration among ETEE Stakeholders regardless of security domain, device or location (static or deployed).	Must
	4.1				ETEE FS shall be accessible by ETEE Stakeholders regardless of security domain, device or location (static or deployed) in accordance with NATO security policies.	Must
		4.1.1			ETEE FS shall have a means to reliably identify and authenticate persons with authorised access.	Must
			4.1.1.1		ETEE FS shall be capable of identifying duplicate user accounts automatically.	Must
		4.1.2			ETEE FS shall allow authorised users to manage user accounts without provider support.	Must
			4.1.2.1		ETEE FS shall allow authorised users to manage user account information requirements without provider support.	Must
			4.1.2.2		ETEE FS shall allow authorised users to manage user roles, groups and permissions without provider support.	Must
				4.1.2.2.1	ETEE FS shall allow authorised users to create authorization policies without provider support.	Must
			4.1.2.3		ETEE FS shall allow authorised users to manage password requirements in accordance with NATO policy without provider support.	Must
			4.1.2.4		ETEE FS shall allow authorised users to limit concurrent sessions by a single user.	Must
			4.1.2.5		ETEE FS shall allow authorised users to monitor sessions by specific users.	Must
			4.1.2.6		ETEE FS shall allow authorised users to track user accounts and disable when no longer required.	Must
		4.1.3			ETEE FS shall allow users able to manage information associated with their account in accordance with user-defined requirements.	Must
	4.2				ETEE FS shall facilitate synchronous and asynchronous collaboration among ETEE Stakeholders by security domain, regardless of device or location (static or deployed) in accordance NATO security policies.	Must
		4.2.1			ETEE FS shall be capable of real-time session sharing with text, audio and video.	Must
		4.2.2			ETEE FS shall be capable of recording sessions with text, audio and video.	Must
		4.2.3			ETEE FS shall facilitate communication among ETEE Stakeholders regardless of security domain or location (static or deployed) within the scope of existing NATO security policies.	Must
		4.2.4			ETEE FS shall allow authorised users to manage collaboration areas without provider support.	Must
			4.2.4.1		ETEE FS shall allow authorised users to manage access requirements to collaboration areas without provider support.	Must
			4.2.4.2		ETEE FS shall allow authorised users to assign collaboration area access rights to specific roles and groups without provider support.	Must
	4.3				ETEE FS shall facilitate the creation of configurable / customizable displays (dashboards).	Must
		4.3.1			ETEE FS application displays shall be optimised for the device in use (e.g., phone, tablet, laptop, desktop, etc.).	Must
		4.3.2			ETEE FS applications shall provide the same displays regardless of security domain.	Must
		4.3.3			ETEE FS applications shall provide Barrier Free Access in accordance with relevant international standards.	Must
		4.3.4			ETEE FS applications shall support inclusion of external links in user displays.	Must
			4.3.4.1		ETEE FS shall allow authorised users to manage external links in application displays without provider support.	Must
		4.3.5			ETEE FS applications may be capable of supporting NATO approved languages other than English (UK) for user displays.	Could
	4.4				ETEE FS shall facilitate data exploitation in accordance with the NATO Data Exploitation Framework Policy.	Must
		4.4.1			ETEE FS shall be capable of extracting data from data repositories.	Must
			4.4.1.1		ETEE FS shall be capable of extracting data from repositories automatically.	Must

ANNEX A to RFI-ACT-SACT-23-42

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
			4.4.1.2		ETEE FS shall allow authorised users to extract data from repositories manually.	Must
			4.4.1.3		ETEE FS shall be capable of automatically integrating and consuming data extracted from repositories.	Must
			4.4.1.4		ETEE FS shall be able to automatically determine and assess the authority of the source and integrity of data.	Must
		4.4.2			ETEE FS shall be capable of automatically integrating data from external tools and services.	Must
		4.4.3			ETEE FS shall allow authorised users to collect real-time, on-site data in user-defined formats.	Must
		4.4.4			ETEE FS shall enable real-time exploitation of data.	Must
		4.4.5			ETEE FS shall facilitate data analysis.	Must
			4.4.5.1		ETEE FS shall be capable of automated data analysis in accordance with user-defined criteria.	Must
			4.4.5.2		ETEE FS shall allow authorised users to perform data analysis manually.	Must
			4.4.5.3		ETEE FS shall be capable of analysing data using Artificial Intelligence (AI) in accordance with extant NATO AI Policy.	Must
			4.4.5.4		ETEE FS shall be capable of analysing structured data.	Must
			4.4.5.5		ETEE FS shall be capable of analysing unstructured data.	Must
			4.4.5.6		ETEE FS shall allow authorised users to define custom models to analyse data.	Must
			4.4.5.7		ETEE FS shall allow authorised users to store and reuse analyses.	Must
		4.4.6			ETEE FS shall provide dynamic, customizable reporting tools.	Must
			4.4.6.1		ETEE FS shall allow authorised users to create specific analysis reports based on customer requirements, as defined in CR 4.5.	Must
			4.4.6.2		ETEE FS should allow authorised users to view analysis results in configurable dashboards.	Should
	4.5				ETEE FS shall facilitate the management of ETEE data and information in accordance with NATO security, information management and data retention policies and STANAGs.	Must
		4.5.1			ETEE FS shall facilitate the management of data.	Must
			4.5.1.1		ETEE FS shall allow authorised users to create data.	Must
				4.5.1.1.1	ETEE FS shall be able to identify duplicate data automatically in accordance with user-defined criteria.	Must
				4.5.1.1.2	ETEE FS shall allow authorised users to manage ownership of data.	Must
				4.5.1.1.3	ETEE FS shall allow authorised users to manage custodianship of data.	Must
				4.5.1.1.4	ETEE FS shall allow authorised users to manage classification of data.	Must
			4.5.1.2		ETEE FS shall allow authorised users to review data.	Must
			4.5.1.3		ETEE FS shall allow authorised users to modify data.	Must
				4.5.1.3.1	ETEE FS shall allow multiple users to edit data simultaneously.	Must
				4.5.1.3.2	ETEE FS shall be capable of logging modifications made to data by specific users.	Must
				4.5.1.3.3	ETEE FS shall be capable of identifying conflicts in modifications made to data.	Must
				4.5.1.3.4	ETEE FS shall allow authorised users to audit modifications made to data by specific users.	Must
			4.5.1.4		ETEE FS shall allow authorised users to dispose of data.	Must
				4.5.1.4.1	ETEE FS shall allow authorised users to delete data.	Must
				4.5.1.4.2	ETEE FS shall support transferring data to the NATO Archives in accordance with NATO information management and data retention policies.	Must
				4.5.1.4.3	ETEE FS shall allow authorised users to recover previously stored versions of data.	Must
		4.5.2			ETEE FS shall facilitate the management of metadata in accordance with NATO policies, directives and STANAGs.	Must
			4.5.2.1		ETEE FS shall allow authorised users to manage metadata requirements without provider support.	Must

ANNEX A to RFI-ACT-SACT-23-42

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
			4.5.2.2		ETEE FS shall allow authorised users to manage metadata sources without provider support.	Must
			4.5.2.3		ETEE FS shall be able to populate specified metadata fields automatically in accordance with user-defined criteria.	Must
			4.5.2.4		ETEE FS shall allow authorised users to manage metadata in bulk in accordance with user-defined criteria.	Must
			4.5.2.5		ETEE FS shall be able to retain metadata values upon import and export of objects.	Must
		4.5.3			ETEE FS shall facilitate the dissemination of data across security domains in accordance with NATO security, information and data management policies.	Must
			4.5.3.1		ETEE FS shall be capable of automatically disseminating data in accordance with user-defined criteria and NATO security policies.	Must
			4.5.3.2		ETEE FS shall allow authorised users to disseminate information and data manually in accordance with NATO security policies.	Must
			4.5.3.3		ETEE FS should allow authorised users to redact and partially disclose data.	Should
		4.5.4			ETEE FS shall facilitate data storage in accordance with NATO information management and data security policies and STANAGs.	Must
			4.5.4.1		ETEE FS repositories shall have a scalable capacity.	Must
			4.5.4.2		ETEE FS repositories should be cloud based.	Should
			4.5.4.3		ETEE FS shall allow users to store classified and unclassified data based on user specified data formats.	Must
				4.5.4.3.1	ETEE FS shall allow authorised users to migrate data from existing repositories.	Must
				4.5.4.3.2	ETEE FS repositories shall be able to synchronize data across security domains in accordance with NATO security policies.	Must
			4.5.4.4		ETEE FS shall allow authorised users to create logically separated information environments within the repositories without provider support.	Must
			4.5.4.5		ETEE FS shall allow users to search and filter repository data.	Must
				4.5.4.5.1	ETEE FS shall allow users to perform searches based on free text (key word search).	Must
				4.5.4.5.2	ETEE FS shall allow users to perform searches based on structured Metadata.	Must
				4.5.4.5.3	ETEE FS shall allow users to perform searches based on Semantic Search.	Must
				4.5.4.5.4	ETEE FS shall allow users to order search results based on user-selected criteria.	Must
				4.5.4.5.5	ETEE FS shall allow users to filter search results based on multiple user-selected criteria.	Must
				4.5.4.5.6	ETEE FS shall allow users to refine searches according to multiple user-selected criteria.	Must
				4.5.4.5.7	ETEE FS shall allow users to make use of predicted search terms.	Must
				4.5.4.5.8	ETEE FS shall allow authorised users to limit search results based on user roles and permissions.	Must
			4.5.4.6		ETEE FS shall allow users to retrieve data in accordance with user roles and permissions, and NATO security and information management policies.	Must

S4 – Service Functions (CR 5.0)	NAFv3: NSOV-3

The S4 Viewpoint is concerned with the definition of the behaviour of a service in terms of the functions it is expected to perform. The following table lists the required service provision aspects, in the form of capability requirements (CRs), related to the lifecycle management of the ETEE FS Capability.

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
5.0					ETEE FS provision shall include lifecycle management of applications and services.	Must
	5.1				ETEE FS provision shall include change management processes.	Must
		5.1.1			ETEE FS shall be able to respond to changing resource demands with no effect on the end user.	Must
			5.1.1.1		Reconfiguration of ETEE FS applications shall be within an agreed period as defined in the Service Level Agreement (SLA).	Must
			5.1.1.2		Requests for additional ETEE FS capacity shall be able to be fulfilled directly or within an agreed period, as defined in the Service Level Agreement (SLA), without extensive redesign or reconfiguration.	Must
			5.1.1.3		Provisioning and de-provisioning of ETEE FS resources shall be completed within an agreed period as defined in the Service Level Agreement (SLA).	Must
		5.1.2			ETEE FS shall be able to respond to new business requirements with no effect on the end user.	Must
			5.1.2.1		New ETEE FS applications shall be able to be implemented without affecting the rest of the operating environment.	Must
			5.1.2.2		Individual ETEE FS applications shall be able to be adapted or upgraded without affecting the rest of the operating environment.	Must
			5.1.2.3		Individual ETEE FS applications shall be able to be removed without affecting the rest of the operating environment.	Must
		5.1.3			ETEE FS shall allow authorized users to manage change requests without provider support.	Must
			5.1.3.1		ETEE FS shall allow users to submit change request proposals to NATO change management authorities.	Must
			5.1.3.2		ETEE FS shall allow NATO change management authorities to submit change request proposals to the provider.	Must
			5.1.3.3		Responses to ETEE FS change requests shall be provided within an agreed period as defined in the Service Level Agreement (SLA).	Must
			5.1.3.4		Status updates for ETEE FS change requests shall be provided at agreed intervals as defined in the Service Level Agreement (SLA).	Must
			5.1.3.5		Implementation of approved changes shall be in accordance within agreed periods, based on the extent of the change(s), as defined in the Service Level Agreement (SLA).	Must
		5.1.4			User acceptance testing of new or updated ETEE FS applications shall be conducted prior to implementation.	Must
		5.1.5			Security testing of new or updated ETEE FS applications shall be conducted prior to implementation.	Must
	5.2				ETEE FS provision shall include incident management processes.	Must
		5.2.1			ETEE FS shall be capable of automatic issue notification.	Must
		5.2.2			ETEE FS shall allow users to submit issue notifications (trouble tickets) in accordance with service provider processes.	Must
		5.2.3			ETEE FS shall be capable of automatically issuing incident status notifications in accordance with service provider processes.	Must

S8 – Service Policy (CR 5.0)	NAFv3: NSOV-4C

The S8 Viewpoint is concerned with the identification and description of constraints that apply to service implementations. The following table lists, in the form of Capability Requirements (CRs), the resource constraints relative to Key Performance Indicators (KPIs) and NATO regulatory requirements that are relevant to the ETEE FS Capability.

CR ID					Requirement Statement	Priority
Tier 1	Tier 2	Tier 3	Tier 4	Tier 5		
5.0					ETEE FS provision shall include lifecycle management of applications and services.	Must
	5.3				ETEE FS service performance shall be in accordance with Key Performance Indicators as defined in the Service Level Agreement (SLA).	Must
					The SLA will identify the roles and responsibilities in delivering the intended service, as well as the quality, timing and overall performance indicators (effectiveness) of all operational and security characteristics of the service. It will address the planned availability, quality, and capacity levels indicated as a measure of the ability to deliver the required performance in accordance with legal, statutory, and regulatory compliance obligations.	
	5.4				ETEE FS shall comply with the principles of provision, use and control of services provided within NATO, outlined in the Alliance Consultation, Command and Control (C3) Policy (C-M(2015)0041-REV2), as applicable.	Must
		5.4.1			ETEE FS shall be provided as a modular service.	Must
		5.4.2			ETEE FS shall employ agreed standards and profiles, defined in the NATO Interoperability Standards and Profiles (NISP), to control the exchange of information, and to ensure interoperability, with identified tools and services.	Must
		5.4.3			ETEE FS provision shall include accreditation, or a plan to achieve accreditation, in accordance with NATO security policies.	Must
		5.4.4			ETEE FS shall reside on NATO CIS infrastructure.	Must
		5.4.5			ETEE FS shall be able to be hosted within the NATO Enterprise's shared cloud-computing infrastructure in accordance with the NATO Cloud Computing Policy.	Must
		5.4.6			ETEE FS provision shall employ green standards and industry best practices for ICT applications and services.	Must
		5.4.7			ETEE FS shall allow for the establishment and management of privileged user accounts in accordance with NATO policy without provider support.	Must

ANNEX A to RFI-ACT-SACT-23-42

S8 – Service Policy (Regulatory Compliance)	NAFv3: NSOV-4C

The S8 Viewpoint is concerned with the identification and description of constraints that apply to service implementations. The following table lists the regulatory requirements, traced to applicable CRs, which are relevant to the ETEE FS Capability.

Policy	Title	Location in Document	Policy Text	CR ID
AC/322-D(2017)0027	NATO Information and Knowledge Management Policy	Para. 10	Information is a corporate resource and shall be managed and preserved as such to support NATO's missions, consultation, decision-making processes, and operational requirements by organising and controlling information throughout its life cycle regardless of the medium and format in which information is held.	4.5 4.5.1
AC/322-D(2017)0027	NATO Information and Knowledge Management Policy	Para. 11	Information shall have an originator, and clearly defined ownership and custodianship assigned throughout its life cycle.	4.5.1.1.2 4.5.1.1.3
AC/322-D(2017)0027	NATO Information and Knowledge Management Policy	Para. 13	Information shall be managed with an emphasis on the 'responsibility-to-share' balanced by the security principle of 'need-to-know', and managed to facilitate access, optimise information sharing and re-use, and reduce duplication, all in accordance with security, legal and privacy obligations.	4.1.1 4.5
AC/322-D(2017)0027	NATO Information and Knowledge Management Policy	Para. 14	Information shall have standardised structures and consistent representations to enable interoperability, cooperation and more effective and efficient processes.	4.5.2 4.5.3 4.5.4.3
AC/322-D(2017)0027	NATO Information and Knowledge Management Policy	Para. 15	Information shall be protected by applying the principle of Information Assurance, which is described as the set of measures to achieve a given level of confidence in the protection of information, communication, and other electronic and non-electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, non-repudiation and authentication.	4.1 4.1.1 4.2 4.5
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 10	Specific processes shall be put in place for accessing, using, sharing and protecting data as a corporate asset. Its value is increased through the widespread and appropriate use of high quality data. Its value is diminished through misuse, misinterpretation or unnecessary access restrictions.	4.1.1 4.5.2 4.5.3 4.5.4.3
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 11	Organisations shall ensure that data is advertised and can be discovered by users and applications, and that duplication of existing data is minimized.	4.5.4.5
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 12	Data shall be accessible in a shared networked environment to users and applications, unless policies, regulations, or other security means prohibit such access. Data repositories shall be managed, provisioned and administered across the data life-cycle in accordance with NATO policies [To include policies and directives related to the appraisal, retention and long-term preservation, currently available in C-M(2002)49, C-M(2002)60, C-M(2011)0043; C-M(2009)0021 and AC/324-D(2014)0008], standards and best practices.	4.1 4.5.4.3
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 13	Data of permanent value shall be retained and archived, whilst data of temporary value shall be destroyed when no longer needed - in accordance with NATO policies, standards and best practices.	4.5.1.4 4.5.4.5 4.5.4.6

ANNEX A to RFI-ACT-SACT-23-42

Policy	Title	Location in Document	Policy Text	CR ID
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 14	Organisations shall allow users and applications to exchange, understand and interpret data, both structurally and semantically and to determine how it may be used for their specific needs. XML shall be used as a syntax for data exchange.	4.4
				4.4.1.3
				4.5.2
				4.5.3
				4.5.4.3.1
				4.5.4.3.2
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 15	Organisations shall ensure proper authentication, authorization, integrity, access, auditing and handling of data. Users and applications shall have the ability to determine and assess the authority of the source and integrity of the data.	4.1.1
				4.4.1.4
				4.5
				4.5.1
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 16	Users and applications shall have the ability to measure, assess, and ensure data to be fit for purpose and fit for use.	4.4.1.4
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 19	Critical data shall be consistently defined, stored and managed to provide a single point of reference across the NATO Enterprise.	4.5.1.4
				4.5.4
				4.5.4.6
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 21	Metadata shall be defined to allow discoverability of data and information, to enable the description of the structure and the content of data and information, to provide sufficient details for authenticity, pedigree, protection, security classification, and access control, to facilitate the identification of ownership and custodianship, to facilitate retention and disposition and long-term preservation, and to support system interoperability and information exchange.	4.4.1.4
				4.5.1.1.2
				4.5.1.1.3
				4.5.1.1.4
				4.5.2
				4.5.3
				4.5.3.1
				4.5.3.2
				4.5.4
				4.5.4.5.2
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 22	Any data and information exchanged on NATO systems shall be accompanied with an approved core set of metadata [Implementation directive(s)/guidance shall provide details for a core set of metadata (currently the NATO Core Metadata Specification - NCMS).].	4.5.2
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 23	Various communities of interest shall use metadata schemas that are aligned with the NATO core metadata. Metadata schemas shall be registered and permanently updated in a common repository [Implementation directive(s)/guidance shall provide details for a metadata repository (currently the NATO Metadata Registry and Repository – NMRR).].	4.5.2
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 24	In principle, metadata and its metadata schema should be unclassified, visible to, accessible and exchangeable by all authorised users and systems. As a consequence, metadata may have a different classification level from the data or information that it is associated with.	4.5.2

ANNEX A to RFI-ACT-SACT-23-42

Policy	Title	Location in Document	Policy Text	CR ID
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 25	Metadata shall evolve and be persistently associated with the data and information throughout their life-cycle. Metadata of records shall be maintained for long-term preservation beyond the destruction of the record itself.	4.5.2
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 26	Metadata shall support a coherent and standardised approach to marking, labelling and binding of metadata to data and information.	4.5.2
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 27	The capture of metadata shall be automated where possible. To ensure both human-readable and machine-readable metadata, XML shall be used as the primary language to structure metadata.	4.5.2
AC/322-D(2017)0028-REV1	NATO Data Management Policy	Para. 28	Data management principles related to visibility, accessibility, interoperability, quality, assurance and security shall apply to metadata management.	4.5.2
AC/322-D(2019)0038 (INV)	CIS Security Technical and Implementation Directive for the Security of Web Applications	Para. 12	The identified set of security requirements shall be accounted for in the design, implementation, and future enhancements of the web application solution, given the specific technology chosen.	5.4.3
AC/322-D(2019)0038 (INV)	CIS Security Technical and Implementation Directive for the Security of Web Applications	Para. 13	Security testing, validation and accreditation shall be conducted in accordance with References G and H, and shall consider the guidance of References I, J, and K.	5.4.3
AC/322-D(2019)0038 (INV)	CIS Security Technical and Implementation Directive for the Security of Web Applications	Para. 14	The CISP shall operate the web application and supporting infrastructure as per References A, G, and H to ensure security is upheld.	5.4.3
AC/322-D(2019)0038 (INV)	CIS Security Technical and Implementation Directive for the Security of Web Applications	Para. 7	The CISP, in coordination with the CISOA and subject to approval by the SAA, shall conduct an assessment to determine the web application security level requirements for each web application and any additional security measures.	5.4.3
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID CM3-2	New or modified versions of software are checked for integrity and for malware before being introduced to the CIS.	5.1.5
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID EA3-1	Comprehensive CIS Security role focused education is provided to privileged users and CIS Security personnel.	3.2 3.3
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM10-1	Administrator responsibilities are divided into three Tiers as per AC/322-D(2015)0029.	5.4.7
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM10-4	Administration is not allowed from standard user accounts.	5.4.7
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM10-5	A privileged user working on several Tier have an account dedicated to each Tier and are only administrator of their administration computer when needed, not by default.	5.4.7
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM10-7	Privileged user's privileges are defined and current status can be determined.	5.4.7
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM10-8	Privileges for privileged users are reviewed periodically and when an administrator changes roles.	5.4.7
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM10-9	Administrator privileges are managed to ensure least privilege.	5.4.7
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM10-10	The number of administrator privilege accounts is limited to the absolute minimum required.	5.4.7
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM11-1	Session lock is implemented after a certain period of inactivity as agreed by the SAA	5.3
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM11-2	Concurrent sessions to a service by a single user are limited and monitored to prevent masquerading.	4.1.2.4 4.1.2.5
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM12-1	Editors or administrators of publicly accessible websites or portals use multi-factor authentication, if available. If multi-factor authentication is not available, the passwords used are at least 16 characters long while using a minimum of 4 types of keyboard characters.	4.1.2.3

ANNEX A to RFI-ACT-SACT-23-42

Policy	Title	Location in Document	Policy Text	CR ID
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM12-2	Editors are designated, authorized and trained to publish publicly accessible information.	3.2
				3.3
				4.1.2.2
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM12-3	Passwords for users of publicly accessible websites, if used, meet the requirements of section IAM4, Password based Authentication.	4.1.2.3
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM12-4	The requirements for passwords of publicly accessible websites, when used in conjunction with another authentication factor, will be agreed by the SAA	4.1.2.3
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM4-1	The password composition policy requires users to choose a password at least 12 characters long while using a minimum of 3 of the 4 types of keyboard characters.	4.1.2.3
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM4-2	Commonly used passwords and substrings (e.g. “1234” or keyboard patterns) are banned by using password blacklists.	4.1.2.3
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM4-6	Password reuse is prohibited for 10 generations (i.e. users cannot re-use their last 10 passwords on a system).	4.1.2.3
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM4-7	Users have the ability to change their passwords in compliance with the requirements of IAM4-6.	4.1.3
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM8-4	Inactive accounts are disabled within 90 days.	4.1.2.6
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM8-6	Service Accounts are tracked, disabled when no longer required and subject to the requirements of privilege user access controls.	4.1.2.6
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM9-3	Access profiles and their associated access rights are defined.	4.1.2.2
				4.1.2.2.1
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM9-4	The principle of Least Privilege applies: Users have the minimum set of permissions to accomplish their work tasks.	4.1.2.2
				4.1.2.2.1
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM9-5	Normal users do not have local admin privileges (Tier 2) on their workstations.	4.1.2.2
				4.1.2.2.1
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM9-6	User access permissions can be determined.	4.1.2.2
				4.1.2.2.1
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID IAM9-7	User access permissions are reviewed when a user changes roles.	4.1.2.2
				4.1.2.2.1
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID PSW2-1	The authenticity and integrity of software and firmware are verified before installation.	5.1.5
AC/322-D/0048-REV3 (INV)	Technical and Implementation Directive on CIS Security	Requirement ID PSW4-5	Application are security tested before the service is made available.	5.1.5
AC/322-D/0052-REV2	Primary Directive on INFOSEC	Para. 23	...system users shall only be given privileges and authorisations they require to perform their tasks and duties	4.1.2.2
				4.1.2.2.1
				5.4.2
AC/322-D/0052-REV2	Primary Directive on INFOSEC	Para. 42	Where access by non-NATO nationals to NATO communication and information systems (CIS) is authorised in support of NATO Operations, Training, Exercises, Transformation and Cooperation (OTETC) (Enclosure “B” to C-M(2002)49 refers), measures shall be applied to restrict access to the NATO classified information required to support the mission.	4.1.1

Policy	Title	Location in Document	Policy Text	CR ID
AC/35-D/2006	Directive for NATO on Security in Relation to Non-NATO Entities	Para. 70(e)	the CIS shall be security accredited with access by an NNE in scope, considering potential impact on other interconnected CIS	5.4.3
AC/35-D/2006	Directive for NATO on Security in Relation to Non-NATO Entities	Para. 70(f)	Measures shall be applied to restrict access to CIS by an NNE individual to only the NATO Classified Information required for the individual to support NATO.	4.1.1
AC/35-D/2006	Directive for NATO on Security in Relation to Non-NATO Entities	Para. 72	Interconnection of NATO CIS with an NNE CIS shall be security accredited in accordance with the C-M(2002)49-REV1 and supporting directives.	5.4.3
AdatP-5636 Ed. A Ver. 1	NATO Core Metadata Specification (NCMS)	Para. 1.3	All NATO information and any other information resource handled by information communication systems within the Alliance need to be accompanied by metadata to describe the resource and support its consistent and appropriate handling.	4.5.2
AdatP-5636 Ed. A Ver. 1	NATO Core Metadata Specification (NCMS)	Para. 2.2	Any newly developed COI metadata specifications shall extend the NCMS with the COI-defined metadata elements rather than overlapping or having no connection.	4.5.2 4.5.2.2
AdatP-5636 Ed. A Ver. 1	NATO Core Metadata Specification (NCMS)	Para. 2.4	COI metadata elements must be mapped to elements defined in the NCMS, and aligned with the roles defined in the NIMP and Primary Directive on Information Management (PDIM).	4.5.2 4.5.2.2
C-M(2002)49-REV1	Security within the North Atlantic Treaty Organization (NATO)	Enclosure E, Para. 2	Classified information shall be protected throughout its life cycle to a level commensurate with its security classification	4.1 4.1.1 4.2 4.5
C-M(2002)49-REV1	Security within the North Atlantic Treaty Organization (NATO)	Enclosure E, Para. 5	The physical and CIS security provided to the information in storage, transfer and transmission, its circulation, destruction and the Personnel Security Clearance (PSC) required for access shall be determined by the security classification assigned.	4.1.1
C-M(2002)60	The Management of Non-Classified NATO Information	Para. 5	All NATO information requires protection to ensure its integrity and availability.	4.1 4.1.1 4.2 4.5 5.3
C-M(2002)60	The Management of Non-Classified NATO Information	Para. 19	When non-classified NATO information is stored, processed or transmitted electromagnetically, security measures are required to ensure its integrity and availability and also, in the case of NATO UNCLASSIFIED information, its confidentiality.	4.1 4.1.1 4.2 4.5 5.3
C-M(2002)60	The Management of Non-Classified NATO Information	Para. 21	...there shall be a means to control the connection of systems handling NATO information.	5.4.2
C-M(2002)60	The Management of Non-Classified NATO Information	Para. 21(a)	The security measures for all systems handling NATO UNCLASSIFIED information shall include, where required by paragraph 19, a means to reliably identify and authenticate persons with authorised access to NATO UNCLASSIFIED information	4.1.1
C-M(2002)60	The Management of Non-Classified NATO Information	Para. 21(b)	The security measures for all systems handling NATO UNCLASSIFIED information shall include, where required by paragraph 19, a means to control authorised access to only those persons with a need-to-know.	4.1.1

ANNEX A to RFI-ACT-SACT-23-42

Policy	Title	Location in Document	Policy Text	CR ID
C-M(2007)0118	The NATO Information Management Policy	Para. 10	Information shall be protected by applying the principle of Information Assurance	4.1
				4.1.1
				4.2
				4.5
				5.3
C-M(2007)0118	The NATO Information Management Policy	Para. 5	Information is a corporate resource and shall be managed as such to support NATO's missions, consultation, decision-making processes, and operational requirements by organising and controlling information throughout its life cycle regardless of the medium and format in which the information is held.	4.5
				4.5.1
				4.5.4
C-M(2007)0118	The NATO Information Management Policy	Para. 6	Information shall have an originator, and clearly defined ownership and custodianship assigned throughout its life cycle.	4.5.1.1.2
				4.5.1.1.3
C-M(2007)0118	The NATO Information Management Policy	Para. 8	Information shall be managed with an emphasis on the 'responsibility-to-share' balanced by the security principle of 'need-to-know', and managed to facilitate access, optimise information sharing and re-use, and reduce duplication, all in accordance with security, legal and privacy obligations.	4.1.1
				4.5
				4.5.1
				4.5.3
				4.5.4
C-M(2007)0118	The NATO Information Management Policy	Para. 9	Information shall have standardised structures and consistent representations	4.5.2
				4.5.3
				4.5.4.3
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 13(a)	Information is a corporate resource and shall be managed as such to support NATO's missions, consultation, decision-making processes, and operational requirements by organising and controlling information throughout its life cycle regardless of the medium and format in which the information is held.	4.5
				4.5.1
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 13(b)	Information shall have an originator, and clearly defined ownership and custodianship assigned throughout its life-cycle	4.5.1.1.2
				4.5.1.1.3
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 13(d)	Information shall be managed with an emphasis on the 'responsibility-to-share' balanced by the security principle of 'need-to-know', and managed to facilitate access, optimise information sharing and re-use, and reduce duplication, all in accordance with security, legal and privacy obligations	4.1.1
				4.5
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 13(e)	Information shall have standardised structures and consistent representations to enable interoperability, cooperation and more effective and efficient processes	4.5.2
				4.5.3
				4.5.4.3
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 13(f)	Information shall be protected by applying the principle of Information Assurance	4.1
				4.1.1
				4.2
				4.5

ANNEX A to RFI-ACT-SACT-23-42

Policy	Title	Location in Document	Policy Text	CR ID
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 20	In order to use information effectively and efficiently, it must be organised in a standardised way that makes the information easily discoverable and accessible, and must be managed as a corporate resource.	4.1
				4.5.2
				4.5.3
				4.5.4.3
				4.5.4.5
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 21(a)	Metadata elements shall be in line with relevant NATO policies, directives and standards	4.5.2
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 21(a)(i)	Metadata elements shall, as a minimum, provide for the identification of ownership and custodianship	4.5.1.1.2
				4.5.1.1.3
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 21(a)(ii)	Metadata elements shall, as a minimum, provide sufficient details for protection and access control	4.1.1
				4.4.1.4
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 21(a)(iii)	Metadata elements shall, as a minimum, facilitate retention and disposition	4.5.1.4
				4.5.4
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 21(a)(iv)	Metadata elements shall, as a minimum, support re-usability and comprehensibility	4.4.1.4
				4.5.2
				4.5.2.5
				4.5.4.3.1
				4.5.4.3.2
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 21(a)(v)	Metadata elements shall, as a minimum, provide for the discoverability of information	4.5.4.5
				4.5.4.5.2
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 21(b)	NATO civil and military bodies shall define permissible values for the metadata elements in, inter alia, controlled vocabularies, taxonomies, ontologies or topic maps	4.5.2
				4.5.2.2
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 21(c)	NATO civil and military bodies shall describe and categorise their information assets by maintaining the required metadata elements using agreed permissible values	4.5.2
				4.5.2.2
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 21(d)	NATO civil and military bodies shall ensure publication of metadata	4.5.2
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 23(a)	In order to optimise information sharing and re-use, NATO civil and military bodies shall develop, maintain and use interoperable information holdings	4.5.4.3
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 23(b)	In order to optimise information sharing and re-use, NATO civil and military bodies shall develop and apply standards and mechanisms to control versions, expiration, supersession and dependencies of information.	4.5
				4.5.1
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 25(a)	The systems and services described in the architecture and implemented in the infrastructure shall ensure easy access to information respecting restrictions imposed for security or sensitivity reasons	4.1.1

ANNEX A to RFI-ACT-SACT-23-42

Policy	Title	Location in Document	Policy Text	CR ID
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 25(b)	The systems and services described in the architecture and implemented in the infrastructure shall ensure the timely availability and dissemination of accurate information to users, organisations and systems	4.5.3
				4.5.3
				4.5.3.1
				5.3
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 25(c)	The systems and services described in the architecture and implemented in the infrastructure shall enable use, re-use, fusion and exchange of information by both people and systems	4.4.1.3
				4.5.3
				4.5.4.3.1
				4.5.4.3.2
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 25(d)	The systems and services described in the architecture and implemented in the infrastructure shall allow for effective and efficient discoverability of relevant information	4.5.4.5
C-M(2008)0113 (INV)	The Primary Directive on Information Management	Para. 29(e)	NATO civil and military bodies shall comply with NATO retention and disposition policies, directives and guidelines [e.g., C-M(2009)0021 (INV), C-M(2011)0043, AC/35-D/2002-REV4, AC/324-D(2012)0003 and AC/324-D(2014)0008-REV1]	4.5.1.4
				4.5.4
				4.5.4.6
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 2, Para. 6	All NATO apportioned ICT capabilities shall be defined and provided as services	5.4.1
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 5, Para. 15	Service specifications shall define the detailed design characteristics of Core and COI services and shall include Service Interface Profiles (SIPs), to ensure the achievement of interoperability across services provided through NATO funded, multi-National and National programmes.	5.4.2
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 8, Para. 12	The chosen alternative must be tested and accredited or have a clear path to being tested and accredited by NATO	5.4.3
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 8, Para. 13	The solution shall be built in a modular fashion	5.4.1
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 10, Para. 14	All future ICT solutions within the NATO Enterprise should use the NATO Enterprise's cloud infrastructure rather than deploying distinct additional infrastructures	5.4.5
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 10, Para. 18.1	ICT solutions will be designed with the expectation that the infrastructure has already been designed and will be provisioned, when needed.	5.4.4
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 10, Para. 19	Application development shall use a shared cloud infrastructure and shall access that infrastructure through a service interface.	5.4.5
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 11, Para. 13	C3 Capabilities and ICT services shall be acquired and sustained by utilising green manufacturing standards and industry best-practices (e.g.: The US ENERGY STAR certification ; the EU Eco-design Directive (2009/125/EC)	5.4.6

ANNEX A to RFI-ACT-SACT-23-42

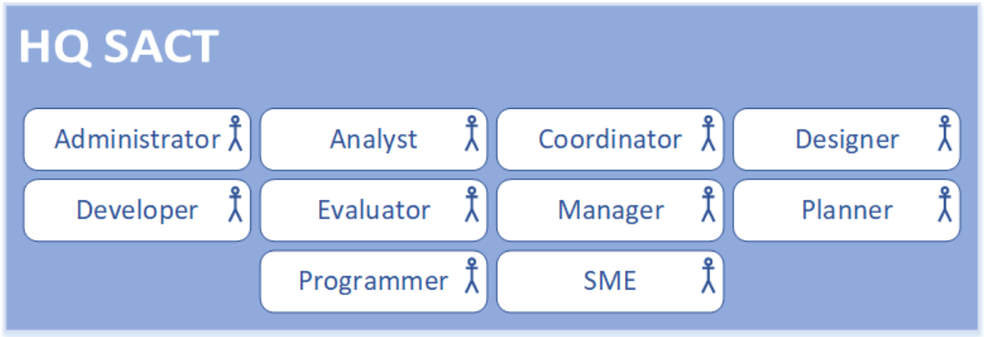
Policy	Title	Location in Document	Policy Text	CR ID
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 11, Para. 17	ICT Services shall be designed to achieve a paperless environment	2.1.4.2
				2.1.6.3.1
				2.2.1.2.2
				2.2.2.2.1
				2.5.1.2
				2.5.2.2
				4.3
				4.4.6.2
				4.4.6.2
				4.4.6.2
				4.4.6.2
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 11, Paras. 18 - 19	Collaboration tools and virtualisation are enhanced and exploited to the highest possible extent in order to reshape NATO business processes aiming at the reduction of resource-intensive activities (e.g. business travel for meetings)	1.1
				1.2
				2.1
				2.2
				2.3
				2.4
				2.5
				2.6
				4.1
				4.2
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 12, Paras. 9 - 12	New applications shall have both IPv4 and IPv6 software interfaces for data transfer and name-to-address resolution.	4.5.3
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Para. 10	Specific processes shall be put in place for accessing, using, sharing and protecting data.	4.1
				4.4
				4.5
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Para. 12	Data shall be accessible in a networked environment to users and applications.	4.5
				4.5.1
				4.5.3
				4.5.4
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Para. 14	XML shall be used as a syntax for data exchange	4.5.3
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Para. 15	Users and applications shall have the ability to determine and assess the authority of the source and integrity of the data.	4.4.1.4

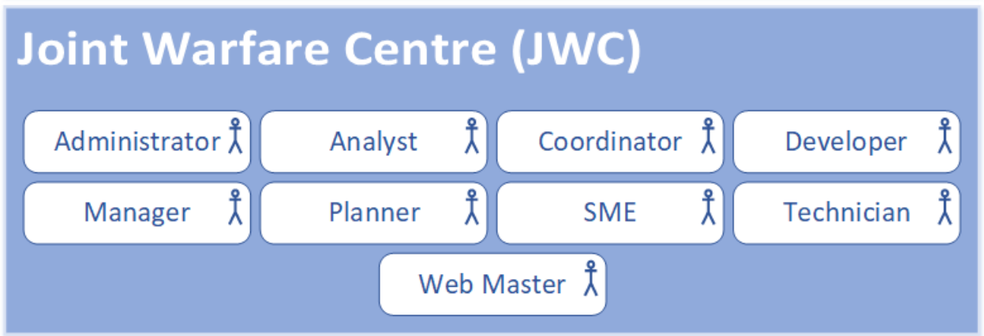
ANNEX A to RFI-ACT-SACT-23-42

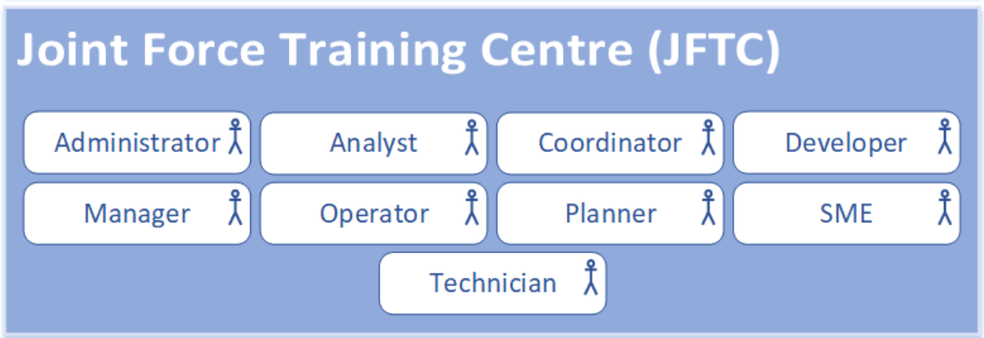
Policy	Title	Location in Document	Policy Text	CR ID
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Para. 21	Metadata shall be defined to allow discoverability of data and information, to enable the description of the structure and the content of data and information, to provide sufficient details for authenticity, pedigree, protection, security classification, and access control, to facilitate the identification of ownership and custodianship, to facilitate retention and disposition and long-term preservation, and to support system interoperability and information exchange	4.4.1.4
				4.5.1.1.2
				4.5.1.1.3
				4.5.1.1.4
				4.5.2
				4.5.3
				4.5.3.1
				4.5.3.2
				4.5.4
				4.5.4.5.2
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Para. 24	Metadata and its metadata schema should be unclassified, visible to, accessible and exchangeable by all authorised users and systems (Metadata may have a different classification level from the data or information that it is associated with)	4.5.2
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Para. 27	XML shall be used as the primary language to structure metadata	4.5.3
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Para. 28	Data management principles related to visibility, accessibility, interoperability, quality, assurance and security shall apply to metadata management.	4.5.2
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Paras. 11 - 16 - 18	Data shall be advertised, discoverable and assessable by users and applications. New programs shall search for existing data elements before creating new data elements	4.5.4.5
				4.5.4.6
C-M(2015)0041-REV2	Alliance Consultation, Command and Control Policy	Annex 13, Paras. 13 - 19	Data of permanent value shall be retained and archived, whilst data of temporary value shall be destroyed when no longer needed. Critical data shall be consistently defined, stored and managed to provide a single point of reference.	4.5.1.4
				4.5.4

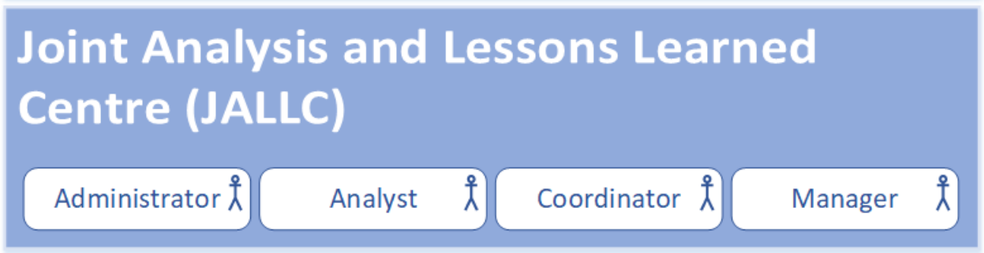
L1 – Node Types (ACT)	NAFv3: NAV-2

The L1 Viewpoint is concerned with the identification of nodes and their organization into specialization hierarchies (taxonomies). The following models identify the general ETEE FS users and roles for ACT.





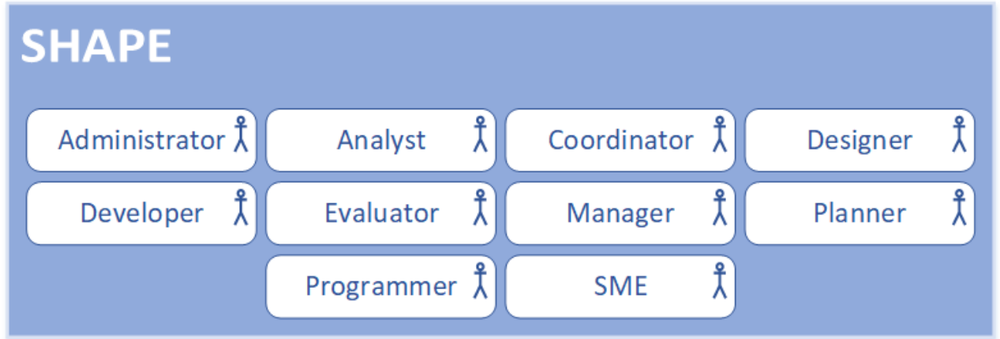


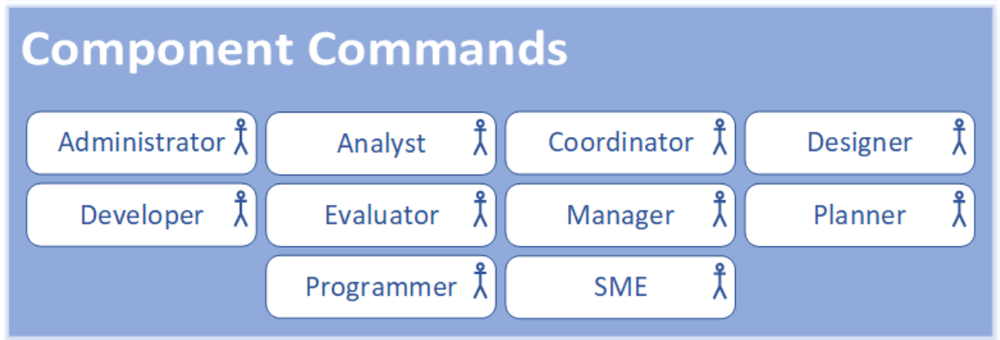


Role	Definition
Administrator (Local)	Oversees files, directories, services, and other resources on the local device. Manages local users, user groups, rights, and permissions.
Analyst	Conducts analyses on data, potentially in specific areas, associated with an event or activity.
Coordinator (Director)	Oversees the planning, organisation and execution of an event or activity, to include schedule, resource allocation, tasks, etc. May also be referred to as a Director.
Designer	Responsible for designing a specific aspect of an event or activity. Specific designers may vary by entity.
Developer	Responsible for developing or scripting a specific aspect of an event or activity. Specific developers may vary by entity.
Evaluator	1. Examines entities, activities, capabilities and/or performances against defined standards or criteria. 2. Collects qualitative and quantitative data to support decision-making processes.
Manager	Responsible for managing a specific aspect of an event or activity. Specific managers may vary by entity.
Operator	Manages the operation of a specific system or service.
Planner	Responsible for planning a specific aspect of an event or activity. Specific planners may vary by entity.
Programmer	Responsible for the programming of ETEE related events or activities.
Subject Matter Expert (SME)	Expert in a specific functional or operational area(s). Contributes to a specific aspect of an event or activity.
Technician	Responsible for installing, integrating, deploying and maintaining hardware and software components of an organization's IT infrastructure. May also be referred to as an Engineer or Integrator.
Web Master	Responsible for maintaining a specific website.

L1 – Node Types (ACO)	NAFv3: NAV-2

The L1 Viewpoint is concerned with the identification of nodes and their organization into specialization hierarchies (taxonomies). The following models describe the general ETEE FS users and roles for ACO.

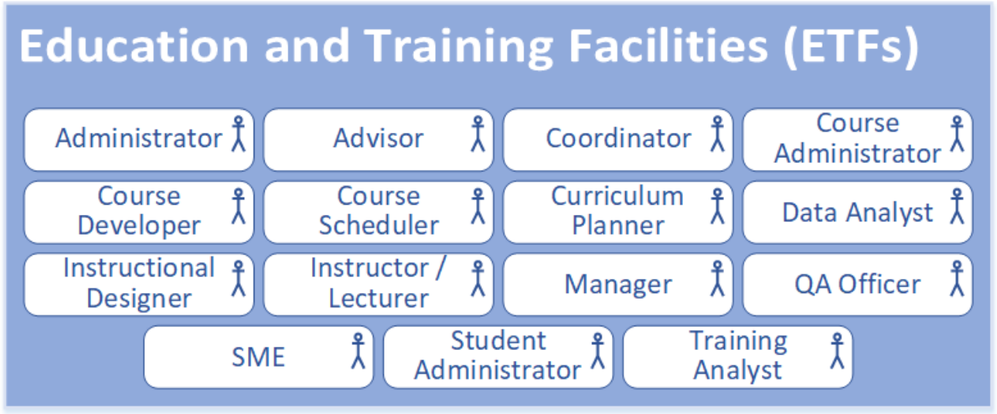




Role	Definition
Administrator (Local)	Oversees files, directories, services, and other resources on the local device. Manages local users, user groups, rights, and permissions.
Analyst	Responsible for conducting analyses on data, potentially in specific areas, associated with an event or activity.
Coordinator (Director)	Oversees the planning, organisation and execution of an event or activity, to include schedule, resource allocation, tasks, etc. May also be referred to as a Director.
Designer	Responsible for designing a specific aspect of an event or activity. Specific designers may vary by entity.
Developer	Responsible for developing or scripting a specific aspect of an event or activity. Specific developers may vary by entity.
Evaluator	1. Examines entities, activities, capabilities and/or performances against defined standards or criteria. 2. Collects qualitative and quantitative data to support decision-making processes.
Manager	Responsible for managing a specific aspect of an event or activity. Specific managers may vary by entity.
Planner	Responsible for planning a specific aspect of an event or activity. Specific planners may vary by entity.
Programmer	Responsible for the programming of ETEE related events or activities.
Subject Matter Expert (SME)	Expert in a specific functional or operational area(s). Contributes to a specific aspect of an event or activity.

L1 – Node Types (ETFs)	NAFv3: NAV-2

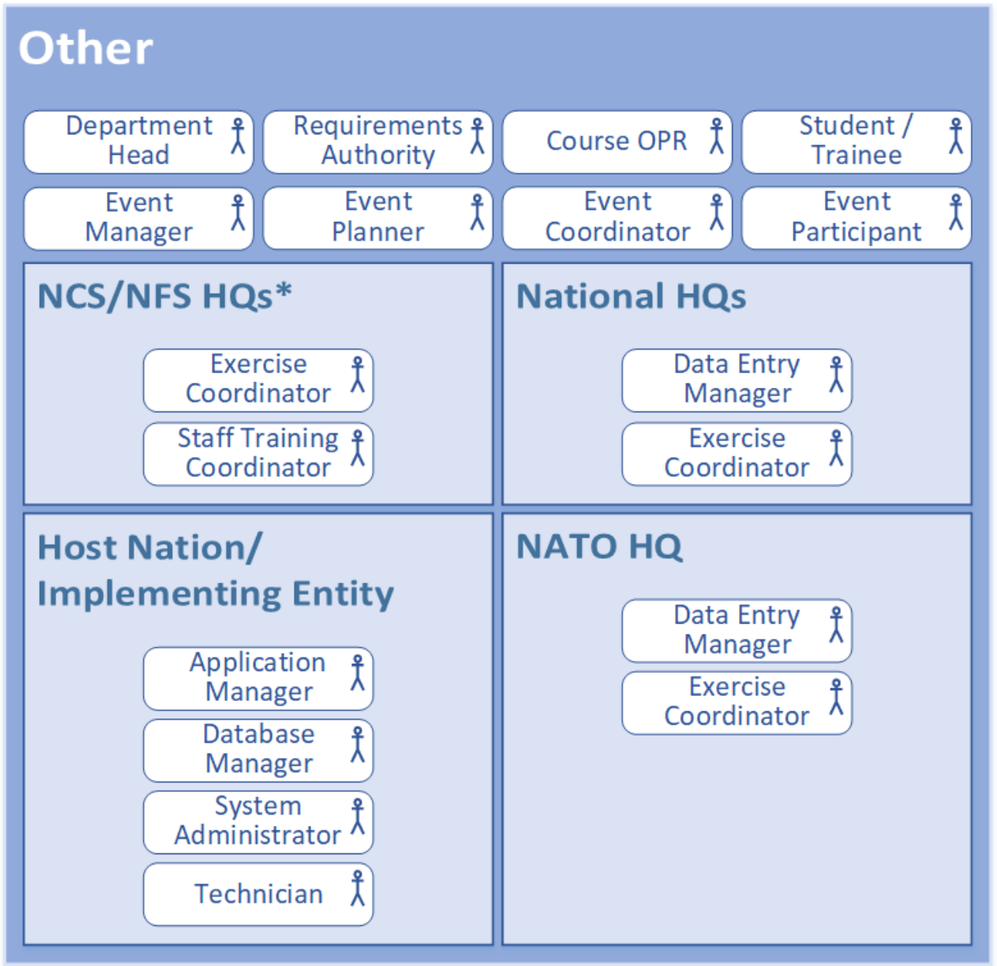
The L1 Viewpoint is concerned with the identification of nodes and their organization into specialization hierarchies (taxonomies). The following model describes the general ETEE FS users and roles for Education and Training Facilities (ETFs), such as, but not limited to, NATO School Oberammergau (NSO), NATO Defence College (NDC), NCIA Academy (NCI Ac), NATO accredited Centres of Excellence (COEs), NATO-recognised Partner Training and Education Centres (PTECs) and National/Multinational institutions from NATO and partner Nations and Non-NATO Entities (NNEs) in accordance with extent ETEE policy. Note that not all roles will be applicable to all ETFs.



Role	Definition
Administrator (Local)	Oversees files, directories, services, and other resources on the local device. Manages local users, user groups, rights, and permissions.
Advisor	1. Gives advice in a particular field. 2. Assists students in planning a course of study.
Coordinator (Director)	Oversees the planning, organisation and execution of a training event, to include schedule, resource allocation, tasks, etc. May also be referred to as a Director.
Course Administrator	Supports course set-up and delivery.
Course Developer	Develops a course in conjunction with the Course Coordinator/Director and the Instructional Designer.
Course Scheduler	Manages the annual course calendar.
Curriculum Planner	Plans and manages a set of related courses.
Data Analyst	Compiles training statistics.
Instructional Designer	Ensures quality and quantity control of training (i.e., development, management and provision of training solutions). May also be referred to as a Course Designer.
Instructor / Lecturer	Gives one or more lectures in a course iteration.
Manager	Responsible for managing a specific aspect of a training event. Specific managers may vary by entity.
Quality Assurance (QA) Officer	Ensures courses and instruction meet set standards.
Student Administrator	Manages student registrations and in processing.
Subject Matter Expert (SME)	Expert in a specific functional or operational area(s). Provides support in their area of expertise for the preparation and execution of a course iteration.
Training Analyst	Conducts needs assessments and develops measurement instruments for training.

L1 – Node Types (Other)	NAFv3: NAV-2

The L1 Viewpoint is concerned with the identification of nodes and their organization into specialization hierarchies (taxonomies). The following models describe additional ETEE FS users and roles for other ETEE stakeholders not previously defined.

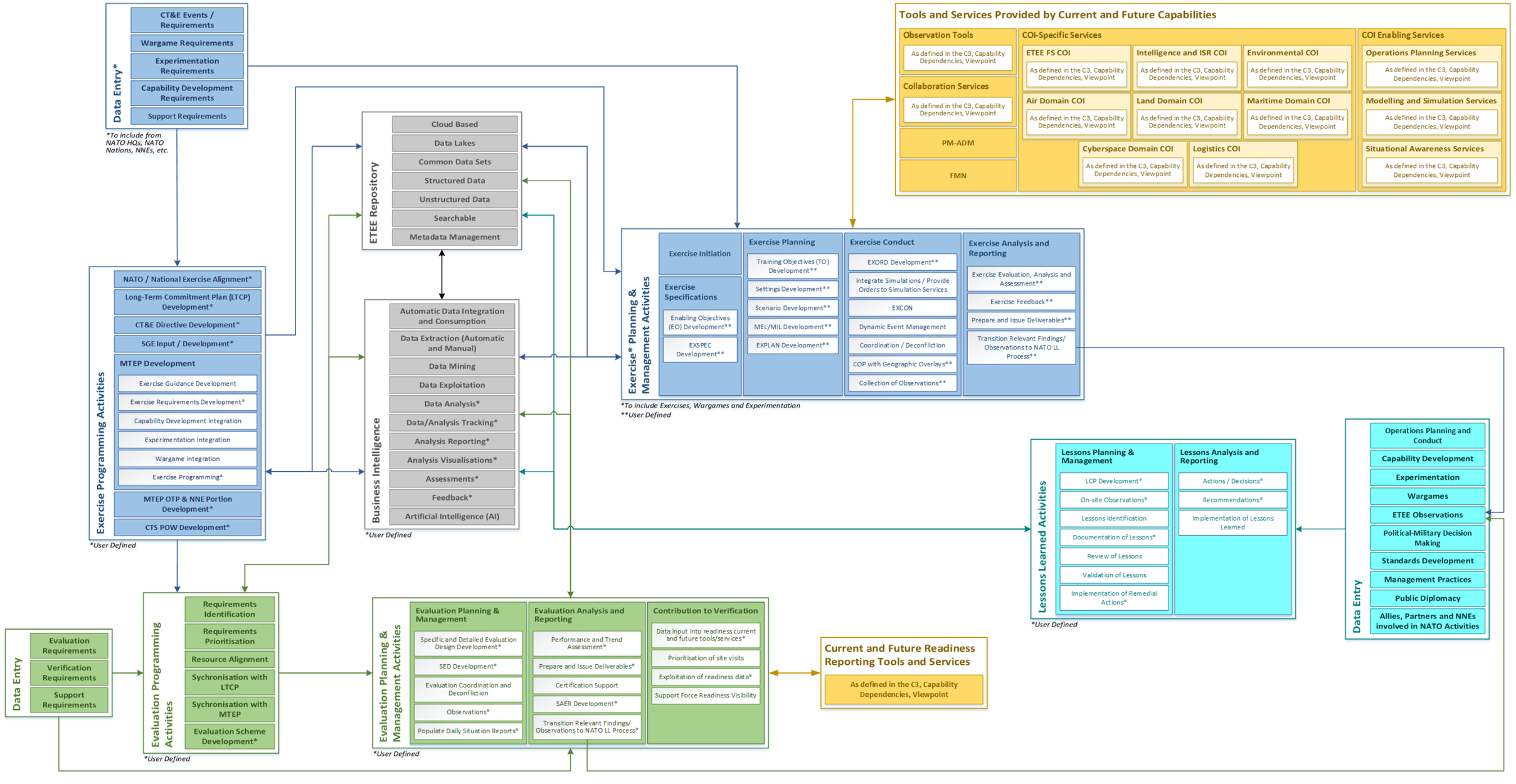


**Not previously defined in the architecture.*

Role	Definition
Application Manager	Responsible for managing the application lifecycle within the enterprise.
Course Officer of Primary Responsibility (OPR)	Role in accordance with Bi-SC Directive 075-007.
Data Entry Manager	Responsible for managing organisational information, to include inserting, updating and maintaining accurate data on relevant systems and in organisational archives.
Database Manager	Responsible for managing assigned databases.
Department Head	Role in accordance with Bi-SC Directive 075-002.
Event Coordinator	Oversees the planning, organisation and execution of an event, to include schedule, resource allocation, tasks, etc.
Event Manager	Responsible for managing a specific aspect of an event.
Event Participant	Participates in an event as an event sponsor, supporter, vendor or attendee.
Event Planner	Responsible for planning a specific aspect of an event.
Exercise Coordinator	Oversees the planning, organisation and execution of an exercise, to include schedule, resource allocation, tasks, etc.
Requirements Authority	Role in accordance with Bi-SC Directive 075-002.
Staff Training Coordinator	Oversees the planning, organisation and execution of a HQ's staff training requirements, to include schedule, resource allocation, etc.
Student / Trainee	Attends a course or training event.
System Administrator	Responsible for the upkeep, configuration and reliable operation of the ETEE FS system(s).
Technician	Responsible for installing, integrating, deploying and maintaining hardware and software components of an organization's IT infrastructure. May also be referred to as an Engineer or Integrator.

L4 – Logical Activities (CT&E, Evaluations and Lessons Learned)	NAFv3: NOV-5

The L4 Viewpoint is concerned with the identification of logical (i.e. implementation independent) activities, grouping and composition of these activities, and logical flows between the activities. The following model provides a composition of the standard CT&E, Evaluation and Lessons Learned activities, to include links to external supporting capabilities, which are relevant to the architecture.



L4 – Logical Activities (E&IT)	NAFv3: NOV-5

The L4 Viewpoint is concerned with the identification of logical (i.e. implementation independent) activities, grouping and composition of these activities, and logical flows between the activities. The following model provides a composition of the standard E&IT activities, to include links to external supporting capabilities, which are relevant to the architecture.