NCIA Request for Information (RFI)

GOVERNANCE, RISK, AND COMPLIANCE TOOL
RFI-07119-GRC

NCIA/ACQ/2026/07119
Thursday, 07 May 2026

NCIA Request for Information (RFI)

To: Industry Partners

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify qualified vendors and gather input on potential solutions to support the upcoming acquisition for a Commercial-Off-The-Shelf (COTS) Governance, Risk, and Compliance (GRC) tool. To that end, we are issuing the attached Request for Information (RFI) 07119 to solicit feedback from capable and interested industry partners.

2. This RFI is issued for planning purposes only and is not a request for bids. It is part of NCIA's effort to ensure it has a clear understanding of the marketplace, available capabilities, and potential acquisition strategies.

3. We value your insight and invite you to:
   a. Share relevant corporate capabilities and experience;
   b. Review and comment on our draft requirements (Annexes A and B) with a view in providing recommendations for improving performance outcomes, competition, and efficiency; and identifying any risks or concerns that should be considered during planning.

4. Submission instructions and additional details can be found in the enclosure to this RFI.

5. Only companies from a NATO member country can participate in or respond to this RFI (https://www.nato.int/cps/en/natohq/nato_countries.htm).

6. Should you have any questions or need clarification, please contact **Esteban DIAZ** at **Esteban.Diaz@ncia.nato.int**.

7. We thank you in advance for your time and input, and we look forward to engaging with you as we shape this potential acquisition.

For the Chief of Acquisition:

Mihaela Zoicas
Digitally signed by Mihaela Zoicas
Date: 2026.05.07 16:22:42 +02'00'

On behalf of:
Esteban DIAZ
Senior Contracting Assistant

Enclosure:

- Request for Information with Annex A
- Distribution List

Distribution List

1. NATO Delegation (Attn: Infrastructure Adviser)

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

2. All NATEXs

Table of Contents

REQUEST FOR INFORMATION

A. Introduction

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify potential sources and gather information regarding industry capabilities to support a Commercial-Off-The-Shelf (COTS) solution to meet the requirements provided in this document for a Governance, Risk and Compliance tool. This Request for Information (RFI) is issued solely for informational purposes and does not constitute a Request for Proposal (RFP), Request for Quotation (RFQ), or invitation for bid.

B. Purpose

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

C. Background

1. NCIA is seeking an automated solution to synchronize the risk management and regulatory compliance processes that is adaptable based on the definition of security requirements coming from the NATO Policies and Directives. This includes providing the unified view of the enterprise IT related risks with flexible risk calculation, data visualization reporting, and dashboard capabilities.
2. The NCIA provide, maintain and defend the NATO enterprise-wide information technology infrastructure to enable Allies to consult together and, when required, stand together in the face of attack. The environment in which we operate is evolving and the growing number of services across the enterprise requires more centralized solutions to aggregate all required data. The NCIA is looking for a system to efficiently and effectively calculate, manage, and track risk mitigations and compliance status, considering compliance challenges and risk-based assessment decisions. This must be done expeditiously before vulnerabilities can be exploited by an adversary.
3. The sought GRC tool should enable smooth transition from a "static" approach to a dynamic "real-time" model, Everything as a code (EaC) and RegOps methodology. RegOps (Regulatory Operations) is a philosophy and methodology that applies DevOps principles – like automation, continuous integration, and collaboration – to the field of regulatory compliance.

D. Submission Instructions

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

   a. Submit responses via the email address in section H no later than **12:00 hours Central European Time (CET)** on **29 May 2026**.

   b. Responses should be submitted in PDF or Word format and must not exceed **15 pages**, including:
      i. Responses to Annex A

      excluding:
      i. Cover page

ii. Company brochures or product literature (if included)
iii. Attachments such as past performance references

c. Use the following subject line for submission
  i. "Response to RFI [RFI-07119-GRC] – [Company Name]"

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

E. Industry Engagement

1. Industry day is not foreseen during this initial stage, however technical discussions via one-on-one virtual sessions may take place following the submission of responses, with the purpose of clarifying or further augmenting those responses where required.

F. Disclaimer

1. This RFI is for planning and informational purposes only and shall not be construed as a solicitation or obligation on the part of the NCIA. The NCIA does not intend to award a contract based on responses to this RFI. Respondents are solely responsible for all costs incurred in responding to this RFI. The NCIA will consider and analyse all information received from this RFI and may use these findings to develop a future solicitation. The NCIA will consider all responses as confidential commercial information and will protect it as such.

2. NCIA reserves the right, at any time, to cancel this informal market survey, partially or in its entirety. No legal liability on the part of NCIA for payment of any sort shall arise and in no event will a cause of action lie with any prospective participant for the recovery of any costs incurred in connection with the preparation of documentation or participation in response hereto. All effort initiated or undertaken by prospective informal market survey participants shall be done considering and accepting this fact.

G. Use of Information Provided through Responses

1. Confidentiality of Responses

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

a. Mark the title page with the following legend:

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

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

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

H. RFI Point of Contact

1. Esteban DIAZ
2. Esteban.Diaz@ncia.nato.int

.

Annex A – Requested Information

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

   a. **Company Information**
      i. Legal Business Name
      ii. Address
      iii. Website
      iv. Primary Point of Contact
      v. Email address

   b. **Technical Capability**
      i. Summary of relevant capabilities and past performance

   c. **Feedback and Recommendations**
      i. Responses to the RFI Questions listed on the next pages
      ii. Innovations or alternatives
      iii. Rough Order Magnitude (ROM), including any assumptions upon which they are based

   d. **Questions or Concerns**
      i. Risks, concerns, or barriers
      ii. Suggestions for risk mitigation or enhancing competition

RFI Questions

Part I: General RFI questions

Crt. No.	Domain	Subdomain	Question	Details
1	**Approval by NATO nations**		Was the tool approved/certified by any NATO Nation?	
2	**Commercial Aspects**		Can you provide references to public sector customers, preferably in the defence or government sector, currently using your COTS solution?	
3	**Procurement, Licensing and Cost**		Please describe the procurement & licensing model. Address topics such as perpetual vs. subscription licenses, floating vs. user licensing, the commitment term and initial ramp-up periods, restrictions on the number of assets, number of users, how is that technically controlled. Does the product allow licensing scaling, increase/decrease use (depending on the license model)?	
4			Assuming a number of 500 nominal users and 200 concurrent users, and 1M assets, please provide a Rough Order of Magnitude of the licensing cost for your solution for the next 5 years.	
5			Please provide a Rough Order of Magnitude of the initial costs for installation, integration, services, support, etc., and O&M costs for the next 5 years.	
6			Please provide a Rough Order of Magnitude for the costs related to updates, upgrades and lifecycle replacement, tool migration to a new OS/platform.	
7			Licence activation - confirm that the product does not require Internet access for License activation.	

8			What is the customer support cost? (considering working hours (time zone?), 24/7, tech support access)	
9	**Technical Capability**	**Installation**	**Is it possible to install and use the product on premises, without an active Internet connection, such as:**	
10			• Completely standalone installation in an air-gapped environment? E.g. On the local network (including, for example, local License server, as long as there is no connection to the Internet or company's server directly)?	
11			• Patches and updates are not pushed automatically (but only applied after testing by our organization), and without an active Internet connection?	
			Does the solution allow the installation of two instances, in two different environments, and one-way synchronization between the instances?	The synchronization is required from the instance connected to Internet to the one installed on-prem/in the air-gapped environment.
12			If AI is used in the product, is it handled on-prem/no Internet connection required?	
13		**Dynamic Data Inputs:**	**Does the product support automated data ingestion for the following:**	i.e. Inputs are collected via API or connectors from external data sources, and dynamically updated within the tool, rather than requiring manual entry/definition.
14			• Assets Definition and Asset criticality/valuation (example: from CMDB/BMC Hellix)	
15			• Threats information	
16			• Vulnerabilities information	

17			• Implementation of safeguards	
18			• Third-party or customer APIs	
19			Does the tool provide any customizable APIs for data collections?	
20			Does the product ingest flat files, e.g. *.csv*?	
21		**Security Frameworks and Policy Compliance**	Does the product integrate compliance checks against the following security frameworks:	
22			• NIST CSF/NIST 800-53 ?	
23			• ISO 27001 ?	
24			• Other Security Frameworks?	
25			Is it possible to add additional regulatory security framework requirements, and use those as the safeguards? (via connection to a data source - or defined manually?)	
26			Are requirements/security controls from the following NATO security directives already integrated in the product? (e.g.: AC/322-D/0048-REV3, AC/322-D/0030-REV6, AC/322-D(2021)0032 REV1, AC/322-D(2019)0038 (INV))	
			Does the tool have the ability to dynamically update the policy compliance assessment, based on the provided inputs? (i.e. “live” policy compliance assessment)	
27		**Risk Calculation**	Is the risk value updated dynamically / “real-time” on the basis of the provided inputs?	
28			Does the risk calculation algorithm include asset dependencies, and is the risk dynamically updated on the basis of these dependencies? (e.g. Kubernetes compromised affecting Dockers or IaaS compromised affecting SaaS that runs on it)	

29			How is the security risk calculated and weighted?	
30			Is the risk calculation formula editable/possible to adjust/weighted?	
31			If AI is implemented in the tool, can it be disabled?	
32			Can third-party risks be added as part of the Risk Calculation and tracked individually?	
33			Does the tool map specific threat TTPs against current security controls to calculate residual risk?	i.e. Does the tool calculate risk based on specific threats and their TTPs against the customer's pre-defined security controls and monitoring, to get a more accurate picture of risk?
34			Does the tool drive decision making to focus on the highest risk items? Are the criteria driving decision making customizable?	
35			Can risk be comprehensively understood and meaningfully assessed through two fundamental components: the asset value, determined by the impact on the Enterprise in case of a complete loss of the asset, and the residual cyber risk, which remains after the implementation of effective mitigation measures?	The determination of asset value involves a mix of criteria such as the classification level of the information, the number of users affected, the potential reputational damage, the timeline of the supported mission, system criticality for the Enterprise, and the asset's interconnectedness with other systems. The assessment of the residual cyber risk, overall or specific to a scenario, is based on the evaluation's degree of the

				mitigation measures' implementation after employing protective strategies.
36			Is there a third-party risk scoring system for the suppliers integrated in the tool? If yes, how does it work, to ensure supply chain security?	
37		**AAA and Access Control**	How is Access Control implemented? (e.g. RBAC?)	
38			How is authentication, authorization and accounting (AAA) implemented?	
39			Does the tool allow Single Sign On (SSO) with one or more Identity Providers (IdP)?	
40			Does the solution allow integration with other technologies and systems, enabling cross-system information gathering and consolidation?	
41			Is the tool Multi Factor Authentication (MFA) capable?	
42		**Customization**	Does the solution allow tailoring of the collected information, e.g. define additional fields for collected asset valuation?	
43			Are all assets visible and manageable from within the application and allow tailoring of assets model, e.g.: define "essential" asset types, and build asset dependencies between essential assets and supporting assets?	
44			Does it support mapping to both public Cloud and on-prem environments, allowing the definition of assets model, threats information and implementation of safeguards for the specifics of each of these environments?	
45			Does it allow to model risk of the interconnections between the IT systems (the risk value shall be available	

			for both the interconnecting CISs and the interconnection, and specific security controls and threats shall be considered for the interconnection)?	
46			Is the system's risk analysis based upon a specific risk management framework/method/process (e.g., MAGERIT methodology, NIST Risk Management Framework (NIST RMF), COSO Enterprise Risk Management Framework (ERM), FAIR (Factor Analysis of Information Risk), or NIST Artificial Intelligence Risk Management Framework (AI RMF),)?	
47			Does the solution have the capability to enforce and maintain the confidentiality labelling of all NATO information objects in conformance with STANAG/ADatP 4774 and 4778? This needs to be maintained during the creation and modification of all information.	
48			Does the solution support spelling and grammar checks and rich text edition for the generated reports and outputs?	
49			How are outputs generated on basis of specific inputs, maintaining the data format (e.g. URLs)?	Please describe how the solution handles the documents and links to other objects in the database and external URLs
50			What are the current KPIs/KRIs used in the system, and are these customizable?	
51			Does the product provide monitoring on the basis of defined Key Performance Indicators (KPI) and Key Risk Indicators (KRI) and send automated alerts based on predefined thresholds? Is it possible to create customized alerts, for example 30 or 60 days prior to the expiration date?	

52			Within an on-prem solution with Internet access, what is data residency location? Does the tool library reside in the local installation or it is stored in the cloud/company datacentre etc.?	
53			How encompassing is the *Help/Guidance/Frequently Asked Questions* implementation within the tool, if present?	
54		**Predefined data building blocks, output, reporting and other templates**	Does the solution have the capability to define (reusable) templates for: Threat profiles, Asset groups, IT architectural building blocks and other data artefacts groups, etc.? Can pre-populated templates be saved and re-used?	
55			Does the solution have the capability to generate outputs/reports in different formats (Microsoft Word, Excel, PDF, etc.) including predefined headings/footers, etc.? Does the product allow both manual and automated reporting?	Manual reporting: generate report on demand; Automated reporting: generate report periodically or send alert when the risk level increases above a defined threshold;
56		**Workflow support for reporting and outputs**	Does the tool support document versioning and collaborative workflows for reports/outputs/documents, including threaded comments and responses to the respective reports/documents? Additionally, does it support formal sign-off/attestation of specific versions, confirming risk acceptance or authorization?	
57		**User Interface**	Does the solution provide a clientless web access option via web browser, allowing access from separated domains and requiring identity federation?	
58			Is the web interface dashboard configurable from the data and user access perspective?	
59			Is it possible to have multiple configurable dashboards?	
60			Is the dashboard updated in “real-time”?	

61		**Scalability and Speed**	What computing power is required, and can it scale easily considering average number of assets to model risk in the range of 1-5 million(s) and the compliance Security Controls in the range of 1-5 thousand(s)?	
62	**Training and Technical Support**	**Training and Documentation**	Does the company provide manuals and supporting documentation for installation, customization, administration and use of the product?	
63			Does the company provide training on the installation, customization, administration and use of the product? Requested: initial in person training for the installation and customization, prerecorded training for administration and use of the product	
64		**Support**	Is technical support provided during working hours (Europe) or 24/7?	
65			How does the company ensure that only personnel from NATO nations provide technical support?	
66			Does the company have personnel that are NATO Security Cleared? Up to what level?	**Note:** The personnel supporting the solution will need to be NATO security cleared to be able to support the instances installed in the NATO environment. If no personnel with security clearance is available at this time, this will be required before the contract is awarded.
67	**Additional features**		Are there any other important features of the tool that were not addressed in the requirements above?	
68	**Feedback and Recommendations**			
69	**Questions or Concerns**			

Part II: Additional questions/requirements, specific to Cloud environments:

The following are additional requirements aimed for security risk management and compliance of public-cloud solutions:

Crt. No.	Category	Domain	Subdomain	Questions	
1.1	Governance	Standards	NIST OSCAL Framework Portability	Does the platform natively support NIST OSCAL support for all catalogue and profile exports?	
1.2		Governance	Digital TPRM	Can the tool ingest a vendor OSCAL component definition?	
1.3		Governance	Policy Sync	Does the tool support “GitOps” workflows for policies?	
1.4		Governance	Identity Mapping	Does the platform support automated RBAC synced with Entra ID?	
1.5		Standards	CSA CCM	Does the tool support Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)?	
2.1	Risk	Risk	Continuous Monitoring	Can the tool update Risk Scores via live vulnerability telemetry?	
2.2		Risk	Impact Analysis	Does the tool provide graph-based control inheritance?	
2.3		Risk	AI/ML Assessment	Does the platform use AI/ML for risk suggestions? If so, can it use local/private LLM deployment within our perimeter?	
2.4		Risk	Threat Model Link	Can the tool ingest threat models via API?	
2.5		Supply Chain	Software Bill of Materials (SBOM)	Can the tool ingest Software Bill of Materials (SBOM) to track supply chain risk?	
3.1	Compliance	Compliance	API-First Evidence	Is every control check satisfied via API-driven evidence upload?	

3.2		Compliance	CLI for Engineers	Does the vendor offer a CLI for developers?	
3.3		Compliance	Digital SSP	Does the system generate a real-time System Security Plan?	
3.4		Compliance	Auto-Remediation	Can the platform trigger fixes via webhooks when drift is detected?	
3.5		Enforcement	OPA/Rego	Can the platform ingest and display the results of Open Policy Agent (OPA) “Rego” policy checks?	
3.6		Interoperability	Multi-framework mapping	Can the tool automatically “cross-walk” a single piece of evidence to multiple frameworks (NIST, ISO, SOC2)?	
4.1	Deployment & Architecture	Deployment	Self-Hosting / PaaS	Does the solution support deployment via Helm/Containers on internal Kubernetes? (AKS/EKS)	
4.2		Deployment	Air-Gap Capability	Can the system function entirely without outbound internet connection to the vendor?	
4.3		Architecture	Database Ownership	Do we maintain full ownership and direct access to underlying database?	
4.4		Architecture	High Availability	Does the architecture support active-active clustering support?	
5.1	Licensing & Cost	Commercial	Unit of Measure	Is licensing Asset-based vs. User-based?	
5.2		Commercial	API Usage Fees	Are there additional costs or rate limits for API calls or data ingestion?	
5.3		Commercial	Price Protection	Does the contract include an annual price “cap”?	
5.4		Commercial	Exit Strategy	Data portability clause included?	

6.1	Training & Technical Support	Support	Developer Support	Access to Engineering-level resources?	
6.2		Training	Certification Path	Certification track for OSCAL Architects or Platform admins?	
6.3		Support	SLA for Self-Hosted	SLA for cloud connectivity bug fixes?	
6.4		Training	Training Library	Is there a searchable « Documentation-as-Code » portal available?	