

European Stability Mechanism 
Request for Proposal
Ref. No.: PRC0004226
Provision of Code Quality Tool

Contents

1	Introduction	4
1.1	The European Stability Mechanism	4
1.2	Overview of this RFP	4
1.3	Overview of the Procurement Requirement	4
2	RFP Content	5
3	The RFP Process	5
3.1.	Type of Procurement Procedure.....	5
3.2.	Eligibility, Exclusion, Selection and Award Criteria	6
3.3.	The ESM Contact Details	7
3.4.	Clarifications of the RFP	7
3.5.	Presentations	8
3.6.	Due Diligence Elements	8
3.7.	Negotiations.....	8
3.8.	Notification of the ESM’s decision	8
3.9.	Contract Terms and Conditions	9
4	Terms and Conditions of the RFP.....	9
4.1	Rights of the ESM	9
4.2	Cost of Participating in the Procurement Process	10
4.3	Materials and Documents.....	10
4.4	Validity of the Proposal.....	10
4.5	Compliance with Law	10
4.6	Trade Name, Logo and Marks	10
4.7	Confidentiality.....	10
4.8	Involvement of/Reliance on Third Parties	11
4.9	Transfer of Undertakings	12
4.10	Use of Artificial Intelligence (AI) in preparation of proposals.....	13
5	Structure of the Proposal.....	13
6	Submission of the Proposal.....	15
	Annex 1 Terms of Reference (Attached).....	16
	Annex 2 Eligibility, Exclusion Criteria, and other required information and documents	16
	Annex 3 Selection and Award criteria.....	17
1.	Selection Criteria.....	17
1)	Economic and financial standing	17
2)	Technical or professional ability	18
3)	Authorisation and suitability to carry out the relevant professional activity	18
2.	Award Criteria	19

Annex 4 Commercial Response Annex	20
Mandatory Technical Requirements:.....	21
Additional Technical and Service Requirements:	24
Service Requirements	30

1 Introduction

1.1 The European Stability Mechanism

The European Stability Mechanism (“**ESM**”) is a permanent crisis resolution mechanism established by the euro area Member States as an intergovernmental organisation under public international law. Its purpose is to ensure the financial stability of the euro area as a whole, and of its Member States experiencing severe financing problems, by providing financial assistance through a number of instruments.

More background information about the ESM may be found on the website: www.esm.europa.eu.

Neither Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 nor Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 (as amended) apply to the ESM. The ESM procures supplies, services and works on its own behalf and for its own account pursuant to the ESM Procurement Policy as published on the ESM website. Please refer to the ESM website for more information.

1.2 Overview of this RFP

This Request for Proposal (“**RFP**”) sets out the procurement requirement and procurement process of the ESM that parties are invited to respond to. The agreement to be awarded as a result of this procurement process (“**Agreement**” or “**Contract**”) will be awarded to the Candidate whose Proposal best meets the award criteria. The Agreement will include the requirements and obligations set out in the Terms of Reference, enclosed as Annex 1, and those set out in Annex 4 of this RFP as potentially adapted and agreed, if required, between the selected Candidate and the ESM during the course of this procurement procedure.

For the purposes of this RFP, candidates who wish to participate in this procurement process are referred to as “**Candidate**” or “**Candidates**” and their response is referred to as a “**Proposal**” or “**Proposals**”.

Unless otherwise defined in this RFP, all capitalised terms used in this RFP have the meanings ascribed to them in the ESM Procurement Policy.

1.3 Overview of the Procurement Requirement

The ESM intends to conclude a single Agreement for the provision of the services with a single service provider (“**Service Provider**”) to support the service needs of the ESM as further detailed in the Terms of Reference provided in Annex 1 of this RFP (“**Services**”).

The ESM’s official working language is English and the Services must be provided in English.

The Agreement will be awarded for a four (4) year term.

2 RFP Content

The RFP package consists of the following documents:

No.	Document Title	Comment
1.	Request for Proposal – Core Document	This document
Annexes		
2.	Annex 1 – Terms of Reference	Attached
3.	Annex 2 – Section 1: Declaration on the Eligibility / Non-Collusion Declaration, Annex 2 – Section 2: Section 3: Cover Certification Form / Consortium / Subcontractor letter	Attached
4.	Annex 3 – Selection and Award Criteria and response elements	Below
5.	Annex 4 – Commercial Response Annex	Attached

3 The RFP Process

3.1. Type of Procurement Procedure

This procurement process is carried out by the ESM under a Negotiated Procedure with Full Publication in accordance with Article 9.1 (3) and Article 3 (6) of Annex 4 of the ESM Procurement Policy and is referred to in this RFP as a procurement process or a procurement procedure. Procurement Process Steps and Timelines

The ESM plans to carry out the procurement process in accordance with the steps defined in the table below. The ESM reserves, at its sole discretion, the right to vary the steps and timelines.

No.	Procurement Process Steps	Timeline
1.	Publication of the Contract Notice and the RFP	10/09/2026
2.	Deadline for submission of clarifications/questions on the Contract Notice and the RFP (via the ESM Procurement tool)	28/09/2026 11:00 hrs (local Luxembourg time)
3.	Response to the clarifications/questions on the Contract Notice and the RFP (via the ESM Procurement tool)	Regularly

No.	Procurement Process Steps	Timeline
4.	Deadline for submission of Proposals (via the ESM Procurement tool)	05/10/2026 11:00 hrs (local Luxembourg time)
5.	Presentations	12/10/2026 to 23/10/2026
6.	Target notification date of the ESM's decision to advance/not advance the Candidate's Proposal	12/11/2026
7.	Negotiations completed (if applicable)	12/11/2026
8.	Target contract signature (start of the transition period)	15/12/2026
9.	Target contract start date_	01/02/2027

3.2. Eligibility, Exclusion, Selection and Award Criteria

In order to be eligible to participate in this procurement process, Candidates must be natural or legal persons and state that they are not subject to any of the exclusion situations listed in the declarations included in Annex 2 Section 1. If such circumstances arise in the course of the procurement process, the Candidate concerned must inform the ESM without undue delay.

Candidates may submit, and if requested by the ESM will submit, evidence to demonstrate their eligibility despite the existence of grounds for exclusion. The ESM may, in its sole discretion, decide whether such evidence is satisfactory.

Candidates must comply with all eligibility and exclusion criteria to be assessed further.

ELIGIBILITY AND EXCLUSION CRITERIA – elements of the evaluation		
Eligibility and Exclusion Criteria	Duly executed declarations as requested in Annex 2 Section 1	Pass / Fail

In order to assess a Candidate's capacity to perform the contract the ESM will apply the following selection criteria (full information can be found in Annex 3 Section 1).

In the event that the Candidate submits a Proposal together with a third party/-ies and/or with subcontractor(s), the combined capacities of the Candidate and all such third party/-ies and/or subcontractor(s) will be assessed for the purpose of meeting the selection criteria.

SELECTION CRITERIA – elements of the evaluation		
Selection Criteria	Economic and financial standing	Pass / Fail
	Technical or professional ability	Pass / Fail
	Authorisation and suitability to carry out the relevant professional activity	Pass / Fail

Candidates must achieve "pass" for all "pass/fail" criteria and must comply with all eligibility, exclusion and selection criteria to be assessed further.

The Proposals submitted by the Candidates will be evaluated, in accordance with the following award Criteria using both the written proposals and the presentation.

AWARD CRITERIA			
QUALITY	60%	PRICE	40%
Criteria 1: Security Analysis	30%		
Criteria 2: Access Management	10%		
Criteria 3: Artificial Intelligence	10%		
Criteria 4: Performance	10%		
Total Score 100%			

Technical proposals of those Candidates who received less than 50% of the maximum available score for each Quality (60%) award criteria will be deemed of insufficient quality and eliminated from further evaluation.

The Candidates' Commercial response will be evaluated according to the following formula:

$$\text{Candidate's Commercial Score} = \frac{\text{Lowest offered Estimated total cost}}{\text{Candidate's Proposed Estimated total cost}} \times \text{Maximum Price score (i.e. 40)}$$

To determine the final score, the Candidates' score for quality will be combined with their respective score for their Commercial Response and the Contract will be awarded to the Candidate whose Proposal best meets the quality/price ratio.

3.3. The ESM Contact Details

All communications must be done via the [ESM Procurement tool](#). Only in case **the ESM Procurement tool** does not work, candidates will be allowed to contact ESM directly via the following email address: procurement@esm.europa.eu
Attention: Mr Ampeglio Amore

The ESM will not be bound by and the Candidate agrees not to rely upon any written or verbal statements or representations of any other persons, whether employed by the ESM or not.

3.4. Clarifications of the RFP

The process for clarifications pertaining to this RFP will be as follows:

- Queries can be raised via the [ESM Procurement tool](#).
- Queries can be raised on any matter in this RFP, including the Annexes. However, the ESM reserves the right not to answer any particular query.

- c) The ESM will endeavour to respond to all queries and issue responses in a timely and professional manner. The ESM reserves the right not to answer any queries received after the deadline for submission of the queries has passed.
- d) Subject to point e) below, responses to the queries will be published on the [ESM Procurement tool](#) if they are of relevance to all of Candidates.
- e) If the ESM receives a query from a Candidate which, in the sole discretion of the ESM, constitutes a query relevant to that Candidate only, the ESM will provide response to that Candidate only.

3.5. Presentations

The ESM will coordinate the schedule of presentations promptly after the release of the RFP. These will likely occur in person at the ESM offices however if this is not feasible, presentations via video conference will also be allowed. The Candidates should ensure that qualified personnel are available during this period to present the case study and to answer questions from the ESM. Presentations are anticipated to take place over one hour.

Scope of the presentation is to assess the proposed tool in accordance with the technical award criteria listed in this RFP.

Note that no pricing information can be disclosed or discussed during the presentations.

3.6. Due Diligence Elements

In order to further ascertain the viability and acceptability of the proposal and of the Candidate, the ESM, in its sole discretion acting reasonably, reserves the right to request the preferred Candidate, and in responding to this RFP the Candidates agree to provide, make available, or facilitate verification of any information certified by the Candidate and any information the ESM deems necessary to assess any potential risks related to data protection, data location, IT security, information security and legal and regulatory matters. The ESM will review this information and assess its correctness and level of risk. In case the ESM deems, in its sole discretion acting reasonably, the level of risk as too high, the Candidate will be excluded from the procurement procedure.

3.7. Negotiations

The ESM conducts negotiations in accordance with the ESM Procurement Policy, ensuring equal treatment of all Candidates invited to participate in the negotiations.

By submitting a written proposal to this Request for Proposal, the Candidates commit themselves to respond in a timely manner to any negotiation request made by the ESM, ensure any new Proposal submitted during negotiations is more beneficial to the ESM than the previous one and acknowledge that any new Proposal submitted is legally binding for the Candidate the same as the original Proposal submitted in response to this Request for Proposal. At a minimum, for all Candidates advancing to the final evaluation stage, the ESM will request a best and final Commercial Response before determining the Candidate whose Proposal has the best price-quality ratio.

3.8. Notification of the ESM's decision

The ESM will notify in writing via the [ESM Procurement tool](#) its decision to advance or not advance the Candidate's Proposal. The notification is sent by electronic means at least fifteen (15) business days prior to the signing of the Agreement by the ESM. The Candidates whose Proposal did not advance can request, in accordance with the ESM Procurement Policy and timelines set within and in

the ESM notification, a de-brief addressing the reasons for not advancing their Proposal. The de-brief will be limited to the reasons related to the unsuccessful Candidate's Proposal and will not cover any information about other Candidates' Proposals.

3.9. Contract Terms and Conditions

The ESM is willing to enter into an agreement based on the contractual terms proposed by the preferred Candidate (the "**Candidate Terms**"). The proposed Candidate Terms must be submitted as part of the Proposal by the deadline for the submission of Proposals. The ESM expects the Candidate Terms to be fair and balanced and acceptable to the ESM. The ESM will review the Candidate Terms and request any changes required from the ESM's perspective. To the extent the Candidate does not agree with the ESM's change requests, the Candidate must provide, for each rejected change request, a clear explanation why the change request is not acceptable from the Candidate's perspective and a counter-proposal where possible. Both parties will endeavour to find an amicable agreement. In case the ESM deems, in its sole discretion acting reasonably, that the Candidate Terms are not acceptable and the contract negotiations have failed, the Candidate will be excluded from the procurement procedure.

4 Terms and Conditions of the RFP

4.1 Rights of the ESM

By submitting a Proposal, Candidates confirm that they have taken note and accepted all terms and conditions of this RFP.

The ESM reserves the right, at its sole discretion and in exceptional circumstances, to accept Proposals received after the deadline for submission of Proposals.

After the ESM opens Proposals, it may request Candidates to submit, supplement, clarify or complete information or documentation which is or appears missing, incomplete, inconsistent or erroneous within an appropriate time limit. The ESM reserves the right at its sole discretion to reject from further consideration any such Proposal.

The ESM reserves the right to request that Candidates provide documentary evidence in support of the statements made in their Proposal.

Any effort by the Candidate to influence the ESM in the process of examination, evaluation and comparison of Proposals may result in the rejection of the Candidate's Proposal.

The ESM may decide, at its sole discretion while respecting the general principles set forth in the ESM Procurement Policy, to cancel this procurement process in whole or in part at any time before the Agreement is signed. The cancellation does not give rise to any form of compensation for Candidates.

The ESM will ensure that the information provided by Candidates is treated and stored in accordance with the principles of confidentiality and integrity.

The ESM reserves the right at its sole discretion to disclose the contents of Proposals to its third party advisors (if applicable) who are bound by the same confidentiality and integrity obligations as the ESM.

If the ESM discovers, before the expiry of the deadline for submissions of Proposals, a lack of precision, an omission or any other type of error in this RFP, it will rectify the error and inform all Candidates in writing via the [ESM Procurement tool](#).

4.2 Cost of Participating in the Procurement Process

All costs relating to the participation in this procurement process, including in particular any costs in relation to the attendance at Presentations and of any other documents requested by the ESM and any subsequent follow-up will be borne exclusively by Candidates.

4.3 Materials and Documents

All materials and documents provided by the ESM during this procurement process will remain the ESM's property. Nothing in this RFP or in any other document issued by the ESM in connection therewith will be construed as to grant Candidates any right or license to use these documents for any purpose, except the right to use them in as much as necessary to prepare their Proposals.

All materials and documents prepared by the Candidate, once submitted to the ESM in response to this procurement process, will become the property of the ESM and, irrespective of the outcome of the procurement process, may be retained by the ESM, and, in any case, the ESM will have the right to use any concept or ideas contained therein without incurring any costs or expenses or any liability whatsoever.

4.4 Validity of the Proposal

By submitting a Proposal, Candidates acknowledge and agree that their Proposal will remain valid and legally binding for a period of 180 calendar days from the deadline for submission of Proposals.

4.5 Compliance with Law

Candidates are invited, but not bound to participate in this procurement process. Yet, the participation in this procurement process following the receipt of the RFP from the ESM implies the acceptance of the terms and conditions of the RFP and any other provisions of the RFP and any breach of these will be subject to appropriate remedies under the applicable law.

Before the Agreement enters into force, the successful Candidate undertakes to comply with all applicable laws and regulations and to obtain all relevant authorisations, permits and certificates required to provide the services described in this RFP.

Nothing in this RFP will be construed as implying a waiver, renunciation or modification by the ESM of any rights, privileges, immunities or exemptions from which ESM may benefit under the Treaty establishing the ESM or any applicable laws.

4.6 Trade Name, Logo and Marks

The ESM logo, covers, page headers, custom graphics, icons, other design elements and other words or symbols used to identify the description of the procurement requirement described are either trademarks, trade names or service marks of the ESM and its licensors, or are the property of their respective owners. These marks may not be copied, imitated or used, in whole or in part, without the explicit prior written consent of the ESM.

4.7 Confidentiality

All documents and information provided by the ESM in connection with this RFP constitute Confidential Information within the meaning of this section.

If the Candidate considers that any part of its Proposal or other documents/information submitted to the ESM include Confidential Information within the meaning of this section it must clearly mark such parts of Proposal or other documents/information as 'confidential'.

Candidates are advised that their participation in this procurement process constitutes Confidential Information except for the announcement by the ESM of the successful Candidate on the ESM website in accordance with Article 9.17 (3) of the Procurement Policy.

Except if required in a judicial or administrative proceeding, or if it is otherwise required to be disclosed by any law or regulation, or where information is already in the public domain, the ESM or the Candidate will (a) not disclose the Confidential Information, (b) take all reasonable measures to preserve the confidentiality and avoid disclosure, dissemination or unauthorised use of Confidential Information, and (c) not use such Confidential Information for any purpose other than as is necessary in connection with this RFP. Confidential Information does not include information which (a) was known to the ESM or the Candidate prior to receiving the information from the Candidate or the ESM; (b) becomes rightfully known to the ESM or the Candidate from a third-party source not known to the ESM or the Candidate (after diligent inquiry) to be under an obligation to the Candidate or the ESM to maintain confidentiality; (c) is or becomes publicly available through no fault of or failure to act by the ESM or the Candidate; or (d) has been developed independently by the ESM or the Candidate or authorised to be disclosed by the Candidate or the ESM. Confidential Information may only be shared with third parties (e.g. contractors) that have a need to know the Confidential Information in relation to this procurement process and provided that such third parties comply with the confidentiality obligations provided in this section.

In addition, if the Candidate has signed an ESM confidentiality undertaking the Candidate agrees to comply with all obligations set forth in such confidentiality undertaking. If there is a conflict between such confidentiality undertaking and this RFP, the confidentiality undertaking will prevail.

4.8 Involvement of/Reliance on Third Parties

If the Candidate intends to involve a third party in the supply of the services offered to the ESM the Candidate has to ensure that any such third party is bound by the requirements set forth in this RFP.

If a Candidate submits its Proposal as part of a consortium with a third party/third parties, such Candidate must provide as part of its Proposal:

- a) a clear description of the proposed consortium, its organisational hierarchy and structure, the names of all consortium members and the roles, activities and responsibilities of the consortium leader and each consortium member;
- b) a document authorising the consortium leader to act on behalf of the consortium member(s) (consortium declaration);
- c) a written undertaking from the consortium member(s) confirming that it/they will place, at the consortium leader's disposal, the resources necessary for the performance of the Contract. The written undertaking must be signed by an authorised representative of each such consortium member; and
- d) information on whether the consortium will form a legal entity and if yes, details of the actual or proposed percentage shareholding within such legal entity and other official documents confirming existence of such legal entity. If not, full details of the proposed consortium arrangement including submission of an executed consortium agreement.

If a Contract is awarded to a consortium, all consortium members will be jointly and severally liable towards the ESM for all obligations arising of or resulting from the Contract.

If a Candidate considers any changes in the consortium structure it must immediately notify the ESM in writing via the [ESM Procurement tool](#). The composition of a consortium (including the roles, activities and responsibilities of the consortium leader and each consortium member) cannot be modified or members of the consortium cannot be exchanged, whether during the course of this procurement process or during the term of the Contract, without the prior written consent of the ESM.

If a Candidate intends to subcontract some of the services offered to the ESM to a third party, the Candidate must provide as part of its Proposal:

- a) a clear description of the proposed subcontracting arrangement, in particular which tasks the Candidate intends to subcontract and their volume or proportion, the name(s) of the proposed subcontractor(s) and its/their roles, activities and responsibilities; and
- b) a document signed by a subcontractor stating its intention to collaborate with the Candidate should the Candidate be awarded a Contract.

If a Candidate subcontracts some of the services under the Contract to subcontractors, it will nevertheless remain fully liable towards the ESM for the performance of such services and responsible for the Contract as a whole. The ESM will have no direct legal commitments with the subcontractor(s).

Where the information provided to the ESM indicates that subcontractor(s) is/are to play a significant role in delivering the services offered to the ESM, any changes to the proposed subcontractors must be notified immediately to the ESM. Candidates cannot exchange or replace the subcontractors or modify the nature of the subcontracting arrangement (including the subcontracted tasks, their volume or proportion), whether during the course of this procurement procedure or during the term of the Contract, without the prior written consent of the ESM.

Moreover, any additional subcontractor(s) which was/were not assessed by the ESM during this procurement procedure may only be appointed if the ESM's has given its prior written consent.

4.9 Transfer of Undertakings

The Candidates acknowledge and accept the possibility that if they are awarded the Contract, the Contract may in some cases trigger the application of the relevant provisions of Luxembourg law or of a collective labour agreement regarding transfers of undertakings, in particular, but not limited to, Articles L.127- 1 to L.127-6 of the Luxembourg Labour Code as amended from time to time (collectively the "Regulations"). Consequently, the Candidates acknowledge and accept the possibility that if they are awarded a Contract the staff employed by the existing service provider performing the services to the ESM (the "Employees") may, if necessary, be taken over and/or transferred automatically, by the virtue of the Regulations.

The Candidates are therefore invited, if deemed appropriate and if not already included in the procurement documents, to request the ESM to provide any necessary information regarding the Employees. The ESM reserves the right to answer questions at a later stage of the procurement procedure if deemed appropriate in the ESM's sole discretion.

Should the Regulations be applicable, the existing service provider and the successful Candidate will fully comply with all of their obligations under the Regulations and will take all necessary steps to facilitate the takeover and/or transfer of the Employees. Any discussions regarding potential takeover

and/or transfer of the Employees will be directly between the existing service provider and the successful Candidate. All the costs incurred by the successful Candidate in relation to the application of the Regulations will be borne solely by such Candidate and will not give rise to any financial compensation from the ESM and will not affect in any way the financial proposal submitted by the successful Candidate.

4.10 Use of Artificial Intelligence (AI)¹ in preparation of proposals

The Candidate may use AI, including Generative AI models², to assist in preparing its proposal, provided that the Candidate remains fully responsible for the proposal and ensures that it is accurate, complete and compliant with the procurement documents.

In case the Candidate is using AI, the Candidate must not input any ESM confidential information, any ESM personal data or any non-public procurement documents or information provided by the ESM into any AI tool unless this is lawful and expressly permitted by the ESM.

In case the Candidate used AI to materially assist in preparing its proposal, the Candidate must briefly identify the parts of the proposal for which AI was used and the general type of AI assistance (e.g. the Generative AI model used), without being required to disclose confidential know-how, prompts or proprietary internal working methods.

Where AI was used, the Candidate confirms by submitting its proposal that the proposal has been subject to human review and validation, and that the Candidate remains fully responsible for its content.

5 Structure of the Proposal

When preparing Proposals, Candidates should observe the following:

- All documents must be submitted in English.
- Any deviations from the specified requirements of this RFP that cannot be satisfied by the Candidate, should be clearly identified in the Proposal.
- In some cases, page/word limits may be specified. Any response exceeding the specified limits may be disregarded beyond that limit.
- Answers should be as concise as possible, complete and comprehensive.
- The ESM does not wish to receive any marketing or other promotional materials.
- All digital copies of the Proposal should be submitted in compliance with the following guidelines:
 - a) One file per section as described in the “Proposal Structure” table below.
 - b) Any supporting or additional files should be clearly named.
 - c) All files should be named clearly with a sequential number and relevant file name.
 - d) All files should be provided in a standard non-editable format, such as PDF.

¹ “Artificial Intelligence”, “Artificial Intelligence capability” or “AI” = a machine-based system that is designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions, that can influence physical or virtual environments.

² Generative AI models = Computer programs designed to create content that resembles human-made output (i.e., creating media/content, such as software code, text, images, videos, and music) based on a user prompt. The models work by learning patterns and structures from a large collection of data.

Proposal Structure			
#	Section	Template and instructions	Document format
1.	Cover Certification Form Upload in the ESM Procurement tool under: TECHNICAL ENVELOPE	Candidates are requested to provide completed, dated and signed by a duly authorised representative Annex 2 Section 2.1 – “Cover Certification Form”	Fully scanned copy with signature in PDF
2.	Declaration on the Candidate’s Exclusion Criteria, Economic, Financial and Operating Capacity and Absence of Conflict of Interest Upload in the ESM Procurement tool under: TECHNICAL ENVELOPE	Candidates are requested to submit completed, dated and signed declaration, signed by a duly authorised representative Annex 2 Section 1.1 – “Declaration on the Candidate’s Exclusion Criteria, Economic and Financial Capacity and Absence of Conflict of Interest”)	Fully scanned copy with signature in PDF
3.	Non-Collusion Declaration Upload in the ESM Procurement tool under: TECHNICAL ENVELOPE	Candidates are requested to submit completed, dated and signed by a duly authorised representative Annex 2 Section 1.2 – “Non-Collusion Declaration”	Fully scanned copy with signature in PDF
4.	Selection Criteria Upload in the ESM Procurement tool under: TECHNICAL ENVELOPE	Candidates are requested to address the requirements under the selection criteria listed in Annex 3 section 1	Fully scanned copy with signature in PDF
5.	Technical Proposal Upload in the ESM Procurement tool under: TECHNICAL ENVELOPE	Candidates are requested to address the requirements under the quality award criteria listed in Annex 3 section 2 in compliance with the Terms of Reference provided in Annex 1.	Fully scanned copy with signature in PDF

6.	Commercial Proposal Upload in the ESM Procurement tool under: FINANCIAL ENVELOPE	Candidates are requested to address the requirements under the price award criteria listed in Annex 4 in compliance with the Terms of Reference provided in Annex 1.	Fully scanned copy with signature in PDF and an writable Excel version
----	--	--	--

Forms to fill in	Candidate (including Consortium Lead)	Consortium members	Key Subcontractors
Declaration on Eligibility Annex 2 1.1	To be completed	To be completed	N/A
Declaration of Non-Collusion Annex 2 1.2	To be completed	To be completed	N/A
Cover Certification form Annex 2 2.1	To be completed	N/A	N/A
Consortium declaration Annex 2 2.2	To be completed	To be completed	N/A
Subcontractor commitment letter Annex 2 2.3	N/A	N/A	To be completed

These forms must be uploaded in the **ESM Procurement tool** under the **TECHNICAL ENVELOPE**.

6 Submission of the Proposal

Proposals must be submitted in the **ESM Procurement tool** no later than by the “**Deadline for submission of Proposals**” specified at point No. 4 of the **Procurement Process Steps and Timelines** table in Section 3.2 of this RFP.

Only Proposals received through these means will be accepted.

Annex 1 Terms of Reference (Attached)

Annex 2 Eligibility, Exclusion Criteria, and other required information and documents

1. Eligibility and Exclusion Criteria

- 1.1 Declaration on eligibility
- 1.2 Non-Collusion Declaration

Note: See the separate document with the above declarations

2. Other Required Information and Documents

- 2.1 Cover certification form
- 2.2 Consortium declaration
- 2.3 Subcontractor commitment letter

Note: See the separate document with the above declarations

Annex 3 Selection and Award criteria

1. Selection Criteria

As part of their Proposal, Candidates are requested to address each item/question below and supply the requested evidence in the correspondingly named and numbered way.

The selection criteria apply to the Candidate as a whole, i.e. a consolidated assessment of the combined capacities of all involved entities will be carried out.

Please note that for the purpose of the evaluation of the Proposals, the ESM will assess the responses provided to the items set out below in this Section 2.

1) Economic and financial standing

Candidates must comply with the following selection criteria in order to prove that they have the necessary economic and financial capacity to perform the Contract.

Selection Criteria	Requirements	Evidence
The Candidate must demonstrate sufficient relevant annual revenue.	The Candidate must have generated annual global revenue of at least EUR 250,000 in each of the last two completed financial years from the provision of services similar to those set out in Annex 1 to this RFP.	The Candidate must complete Appendix 1 to the Terms of Reference and submit it as part of its Proposal.
The Candidate must have a current Dun & Bradstreet Risk Indicator of 1 or 2 (the “D&B Requirement”).	The ESM will obtain a Dun & Bradstreet report and bear the cost of that report.	No evidence is required from the Candidate.

2) Technical or professional ability

Candidates must comply with the following selection criteria in order to prove that they have the necessary technical or professional ability to perform the Contract.

Selection Criteria	Requirements	Evidence
The Candidate must prove experience necessary for performance of the Contract.	At least 3 years of relevant experience in the provision of services similar to the services set out in Annex 1 to this RfP.	The Candidate must complete Appendix 1 to the Terms of Reference and submit it as part of its Proposal.
The Candidate must have technical capacity to perform the Contract	The Candidate must comply with all requirements set out in Articles 2.1.2 and 2.1.3 of the Terms of Reference.	The Candidate must complete Appendix 1 to the Terms of Reference and submit it as part of its Proposal.

3) Authorisation and suitability to carry out the relevant professional activity

Candidates must comply with the following selection criteria in order to prove that they have the necessary authorisation and suitability to perform the Contract.

Selection Criteria	Evidence
The Candidate must prove that they have legal capacity to perform the Contract.	Copy of a proof of enrolment in a relevant trade or professional register.

2. Award Criteria

In their technical responses, Candidates should refer to the quality award criteria and instruction numbers before providing their answers.

The Candidates' technical response should then be sent to the ESM as a separate PDF attachment along with the other documents requested (see Section 5 'Structure of the Proposal').

In responding to the Award Criteria, Candidates should explain clearly how they can fulfil ESM's requirements and whether they can even add some value.

- **Technical Award Criteria**

Quality	60%
Criteria 1: Code Quality & Security Analysis	30%
Each Candidate must provide a description of the proposed Code Quality & Security Analysis functionality and explain how it addresses the following assessment aspects: Triage workflow: The extent to which the proposed triage workflow enables efficient, controlled and auditable human review of findings (including but not limited to code quality, duplication, vulnerabilities, test coverage, open source licensing), including the completeness of the recorded reviewer, decision, justification and timestamp information. Customization: Who and how custom rules can be authored Finding identity and lifecycle metadata: The robustness of the mechanism used to maintain stable finding identities across analyses and code refactoring, and the completeness and accessibility of lifecycle metadata, including through the API. Advanced security analysis: The breadth and depth of the proposed advanced security analysis, including coverage of logic-level vulnerabilities, supported languages and frameworks, accuracy of findings, and the clarity, completeness and auditability of the reasoning trace. Detection-quality benchmark: Each Candidate must take part in an ESM benchmark using the same sample code in Java, Python and TypeScript. The code will include known defects and unchanged control code. The ESM will assess how well the Platform finds real defects, avoids false positives, detects the seeded defects and presents clear, consistent findings	
Criteria 2: Access Management	10%
Each Candidate must provide a description of its proposed integration with EntraID and Microsoft Sentinel, especially addressing the latter's effectiveness, maturity and ease of implementation, including the range of security and administrative events covered, the timeliness of event transmission, the use of standard formats, and the level of configuration required by the ESM.	
Criteria 3: Artificial Intelligence	10%

Each Candidate must provide a description of the proposed Artificial Intelligence functionality and explain how it addresses the following assessment aspects: Protection of ESM data from model training: The adequacy, transparency and contractual enforceability of the measures ensuring that ESM source code, findings and Platform configuration are not used for model training or improvement, including controls applicable to subprocessors and processing locations. Automatic remediation fixes: The breadth, quality and reliability of automatically generated remediation fixes, including supported languages and finding categories, proportion of eligible findings, technical correctness and practical usefulness of the proposed code changes. Delivery of generated fixes: The range, maturity and usability of the supported methods for delivering generated fixes, including integration with Azure DevOps or GitHub, developer integrated development environments, and APIs for ESM automation. Third-party AI transparency: The completeness and transparency of the information provided regarding third-party or hosted AI models, including model providers, models used, geographical processing locations, data-retention arrangements and enforceable safeguards against using ESM data for training	
Criteria 4: Performance	10%
Each Candidate must provide a description about the quality and robustness of the proposed availability commitment, including the guaranteed monthly availability, measurement methodology, exclusions, monitoring and reporting arrangements, incident response and service credits.	

- **Commercial Award Criteria**

The Candidate must submit its Commercial Response using the template provided in Annex 4.

Annex 4 Commercial Response Annex

Appendix 1 (Response template)

	Description	Candidate's response (Yes/No): The Candidate shall confirm whether it complies with the requirement by selecting "Yes" or "No."
Economic and financial standing	The Candidate must have generated annual global revenue of at least EUR 250,000 in each of the last two completed financial years from the provision of services similar to those set out in Annex 1 to this RFP.	Yes/No

Technical and professional capacity	At least 3 years of relevant experience in the provision of services similar to the services set out in Annex 1 to this RFP.	Yes/No
--	--	--------

Authorisation and suitability to carry out the relevant professional activity	The Candidate must prove that they have legal capacity to perform the Contract.	Provide a Copy of a proof of enrolment in a relevant trade or professional register.
--	---	--

Mandatory Technical Requirements:

The Candidate must comply with all mandatory requirements. If the Candidate fails to comply with any mandatory requirement, its Proposal will be deemed non-compliant, rejected and not considered for further evaluation.

Applicable to	Area	Description	Candidate's response (Yes/No): The Candidate shall confirm whether it complies with the requirement by selecting "Yes" or "No."
Platform	Languages	The platform will support all of the following languages / technologies:	Yes/No

		• Java • Python • Typescript • Javascript • HTML • CSS • XML • PowerShell	
Platform	Functionality	The Platform will permit ESM to exclude specified paths, files or generated code from analysis and from metric calculation, configurable per repository.	Yes/No
Platform	Functionality	The Platform will perform static analysis without executing the code and without requiring the application to be deployed or running.	Yes/No
Platform	Functionality	The Platform will detect and report, as distinct categories: • reliability defects (code that is or may be functionally wrong) • duplicated code • security weaknesses.	Yes/No
Platform	Functionality	Every finding will identify the file, line, and where applicable the code path , and will carry a human-readable explanation of why it is a defect and how to remediate it.	Yes/No
Platform	Functionality	The Platform will ingest externally produced test coverage reports in at least one widely used open format per mandatory language (where applicable), and attribute coverage per file and per line .	Yes/No
Platform	Functionality	The Platform will support multi-module and monorepo structures , aggregating multiple build modules within one repository into a single reported result while retaining per-module detail.	Yes/No
Platform	Functionality	Analysis will be deterministic : the same commit analysed with the same configuration and rule set version will produce the same findings.	Yes/No
Platform	Functionality	The Platform will support suppression of individual findings with mandatory justification, attribution to the suppressing user, and an audit trail .	Yes/No
Platform	Security Analysis	The Platform will perform static application security testing (SAST) covering the OWASP Top 10 and CWE Top 25 for the following executable languages: • Java • Python • TypeScript • JavaScript	Yes/No
Platform	Security Analysis	Each security finding will be mapped to a CWE identifier , and to the relevant OWASP category where applicable.	Yes/No
Platform	Security Analysis	The Platform will detect secrets and credentials committed to source code: • API keys • Tokens • connection strings • private keys in the current checkout of every analyzed branch.	Yes/No
Platform	Security Analysis	The Platform will perform software composition analysis (SCA) of third-party dependencies, including	Yes/No

		transitive dependencies, for the ecosystems corresponding to ESM's mandatory languages: • Maven (Java), • npm (TypeScript/JavaScript) and • PyPI (Python).	
Platform	Security Analysis	Dependency vulnerability data will be drawn from a maintained vulnerability database updated at least daily . The Candidate will name its data sources.	Yes/No
Platform	Security Analysis	Findings will carry a severity assigned per a documented and published scheme, and a CVSS score where one applies.	Yes/No
Platform	Management	The Platform will support a centrally defined quality policy applied by default across all repositories, editable only by explicitly authorized administrators and not overridable by individual project teams .	Yes/No
Platform	Management	The quality policy will support, at minimum, conditions on the metrics listed #4, with ESM-configurable thresholds and comparison operators .	Yes/No
Platform	Management	The Platform will support incremental analysis : evaluating the policy against only code added or changed since a configurable baseline . The baseline will be selectable as at least the merge base with the target branch .	Yes/No
Platform	Management	The policy result will be exposed as an unambiguous binary pass/fail suitable for automated enforcement.	Yes/No
Platform	Integration	The Platform will provide native integration with Azure DevOps Services (cloud) and Github , including repository discovery and binding.	Yes/No
Platform	Integration	The Platform will annotate Azure DevOps AND Github pull requests , posting a summary and inline comments on the specific changed lines to which findings relate.	Yes/No
Platform	Integration	The Platform will operate correctly where the Azure DevOps / Github organization is federated to Microsoft Entra ID for single sign-on (OAuth application, Microsoft Entra ID service principal, workload identity federation, managed identity, or personal access token) not depending on interactive end-user OAuth consent , which a federated organization may be unable to grant.	Yes/No
Platform	Integration	The Platform will publish a pull request status check to Azure DevOps / Github that ESM can configure as a required branch policy blocking pull request completion .	Yes/No
Platform	Integration	The Platform will provide ready-to-use Azure Pipelines tasks (via the Visual Studio Marketplace) or a documented command-line interface usable within a container-based pipeline job.	Yes/No
Platform	Integration	Analysis will be invocable from ESM-hosted and Microsoft-managed Azure Pipelines agents requiring outbound HTTPS connectivity only , with no inbound connectivity to ESM networks .	Yes/No
Platform	Access Management	The Platform will support single sign-on interoperable with Microsoft Entra ID as the sole interactive authentication path for ESM users. ESM is protocol-agnostic : SAML 2.0, OpenID Connect, OAuth 2.0, or a native Microsoft Entra ID integration are all acceptable.	Yes/No

Platform	Access Management	The Platform will provide role-based access control that separates, at minimum, administration from contribution from read-only access , and permits quality policy administration to be restricted independently of general project administration.	Yes/No
Platform	Access Management	All ESM repositories and analysis results will be private by default .	Yes/No
Platform	Hosting	All ESM data — source code, analysis results, metadata, logs and backups — will be stored and processed exclusively within the EU/EEA in the normal operation of the Platform.	Yes/No
Platform	Hosting	Data will be encrypted in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent).	Yes/No
Platform	Hosting	ESM's data will be logically isolated from that of other customers.	Yes/No
Platform	Management	The Platform will expose a complete, documented, versioned administrative API sufficient to perform: (a) repository onboarding and per-repository settings; (b) quality policy definitions and their assignment to repositories; (c) rule set definitions and assignment; (d) user groups, roles and permission assignments; (e) integration bindings to Azure DevOps / Github	Yes/No
Service Provider	Hosting	The Service Provider will hold current ISO/IEC 27001 certification and/or SOC 2 Type II attestation covering the Platform.	Yes/No
Service Provider	Hosting	The Service Provider will provide a GDPR-aligned data processing agreement , a complete sub-processor list , and will commit to breach notification within a stated maximum period .	Yes/No
Service Provider	Hosting	On termination, the Service Provider will delete all ESM data within a stated period and provide written confirmation of deletion. Deletion obligations will extend to backups, caches, replicas, search indexes and log stores .	Yes/No
Service Provider	Maintenance	The Service Provider will maintain compatibility with Azure DevOps Services and Github as they evolve and will state its commitment and typical timescale for adapting to changes.	Yes/No

Additional Technical and Service Requirements:

Candidates are expected to comply with the requirements below listed. However, failure to comply with one or more mandatory requirements will not automatically result in the rejection of the Proposal.

Applicable to	Area	Description	Candidate's response (Yes/No): The Candidate shall confirm whether it complies with the requirement by selecting "Yes" or "No."
Platform	Functionality	The Platform will support the following test coverage formats: JaCoCo XML, Cobertura, LCOV, coverage.py, and Istanbul.	Yes/No
Platform	Functionality	The Platform will report a measure of duplicated code across.	yes/no
Platform	Functionality	The Platform must enable the ESM to create custom rules in addition to the rules supplied with the Platform and to distribute and manage those custom rules centrally across the ESM organisation.	yes/no
Platform	Functionality	The Platform must enable the ESM to suppress findings by adding annotations directly to the source code, ensuring that each suppression decision remains associated with the relevant code under version control.	yes/no
Platform	Functionality	The Platform must enable the ESM to restrict suppression permissions by role and to require that the suppression of security findings above an ESM-defined severity threshold be approved by an authorised user other than the code author.	yes/no
Platform	Security Analysis	The Platform will detect security-relevant weakness in the configuration and markup languages XML, YAML, HTML and Terraform/HCL — to the extent meaningful for each (for example insecure deserialization settings, exposed secrets in configuration, unsafe template constructs, permissive infrastructure rules).	yes/no
Platform	Security Analysis	The Platform must detect secrets in the reachable Git history, in addition to the current checkout, ensuring that credentials or other secrets that were committed and subsequently removed remain detectable.	yes/no
Platform	Security Analysis	The Platform will additionally perform SCA for NuGet and PowerShell Gallery .	yes/no
Platform	Security Analysis	The Platform will support reachability or exploitability analysis to distinguish dependency vulnerabilities that are actually invoked by ESM code from those that are not.	yes/no
Platform	Security Analysis	The Platform will detect the open-source licenses of dependencies and allow ESM to define permitted and prohibited license lists.	yes/no
Platform	Security Analysis	Regardless of the scope granted, the Platform will never modify existing source code on a protected branch , will never force-push, and will never delete branches it did not create.	yes/no
Platform	Security Analysis	The Platform will support remediation deadlines derived from finding severity — a target date computed and tracked per finding — and will report findings breaching their deadline.	yes/no
Platform	Security Analysis	The platform will provide a maintained emergency response process for actively exploited	yes/no

Applicable to	Area	Description	Candidate's response (Yes/No): The Candidate shall confirm whether it complies with the requirement by selecting "Yes" or "No."
		vulnerabilities — for example a CISA KEV listing or a widely exploited zero-day in a common dependency — providing detection content and customer notification faster than the routine update cycle.	
Platform	Security Analysis	The Platform will consume and/or produce VEX (Vulnerability Exploitability eXchange) statements, so that ESM's assessment that a vulnerability is not exploitable in its context can be recorded and carried forward rather than re-triaged each cycle.	yes/no
Platform	Security Analysis	The Platform will flag malicious, typosquatted, protestware or hijacked packages in the dependency graph, distinctly from ordinary CVE findings.	yes/no
Platform	Security Analysis	The Platform must ensure that analyses are reproducible, such that the same commit analysed using the same configuration and Platform version produces materially equivalent findings. The Candidate must describe the factors governing reproducibility and any variance that the ESM may expect between runs.	yes/no
Platform	Security Analysis	The Platform must present these findings through the same queue, triage workflow and API used for all other findings, while clearly identifying their source, without requiring the ESM to use a separate console or parallel process.	yes/no
Platform	Security Analysis	The Platform must enable the ESM to scope and schedule the analysis independently for selected repositories, either on demand or according to a configurable schedule, without requiring the analysis to run for every pull request.	yes/no
Platform	Management	The Platform must enable the ESM to select the previously released version of the software as the baseline against which the analysis is performed.	yes/no
Platform	Management	The Platform will support multiple distinct policies , assignable per repository so that differing standards can apply to (for example) production services versus internal tooling.	yes/no
Platform	Management	All changes to policy definitions and rule sets will be versioned and audit-logged , recording actor, change and timestamp, and will be view- and exportable.	yes/no
Platform	Management	Policy and rule-set definitions will be exportable and importable as text , so they can be held under version control and promoted between environments. Policy held as code will reside in an ESM-controlled administrative repository ; the Platform will not honour policy overrides placed in the analyzed repositories themselves.	yes/no
Platform	Management	The Platform will allow ESM to defer or pin rule-set updates , so that a rule change delivered by the	yes/no

Applicable to	Area	Description	Candidate's response (Yes/No): The Candidate shall confirm whether it complies with the requirement by selecting "Yes" or "No."
		Service Provider does not cause previously passing repositories to fail without ESM's decision.	
Platform	Management	The Platform's own configuration will be manageable declaratively as code using HashiCorp Terraform , covering at minimum: (a) repository onboarding and per-repository settings; (b) quality policy definitions and their assignment to repositories; (c) rule set definitions and assignment; (d) user groups, roles and permission assignments; (e) integration bindings to Azure DevOps / Github.	yes/no
Platform	Management	Configuration applied as code will be idempotent and drift-detectable : re-applying an unchanged definition will produce no change, and configuration altered manually through the user interface will be detectable on subsequent reconciliation.	yes/no
Platform	Management	Administrative automation will not require long-lived administrative credentials to be stored in ESM's Terraform state or pipeline definitions.	yes/no
Platform	Integration	The Platform will support analysis of long-lived branches in addition to pull requests and the main branch.	yes/no
Platform	Integration	The Platform will support build-less analysis (analysis from a source checkout without a compilation step) for at least the interpreted and markup languages.	yes/no
Platform	Integration	The Platform will emit webhooks or equivalent event notifications on analysis completion and policy status change, to allow ESM to build downstream automation.	yes/no
Platform	Access Management	The Platform will allow ESM to disable all local and platform-native password authentication organization-wide , so that federated sign-on is the only interactive route in.	yes/no
Platform	Access Management	The Platform will map identity provider group membership to platform roles — via SAML attributes, OpenID Connect claims, Microsoft Entra ID group claims, or SCIM — so that access is governed by existing corporate group management rather than platform-local administration.	yes/no
Platform	Access Management	All interactive sign-in will be subject to ESM's Microsoft Entra ID Conditional Access policies , including device-compliance and location-based conditions. No interactive path will bypass them — including local accounts, legacy authentication endpoints, and long-lived tokens usable in place of interactive login. Non-interactive machine credentials under CQ-IAM-008 are outside this requirement and are governed instead by expiry and revocation.	yes/no

Applicable to	Area	Description	Candidate's response (Yes/No): The Candidate shall confirm whether it complies with the requirement by selecting "Yes" or "No."
Platform	Access Management	The Platform will support SCIM 2.0 automated user provisioning and, critically, automated de-provisioning , so that a leaver removed from Microsoft Entra ID loses platform access without manual action.	yes/no
Platform	Access Management	The Platform must provide sufficiently granular role-based access controls to distinguish, at a minimum, the following five roles: Organisation Administrator, Policy Administrator, Project Administrator, Contributor and Read-Only User.	yes/no
Platform	Access Management	The Platform will maintain an audit log of authentication events, permission changes, policy changes and administrative actions, retained for a stated period and exportable in machine-readable form .	yes/no
Platform	Access Management	The Platform will support Microsoft Entra ID managed identities or workload identity federation for service-to-service authentication, as an alternative to stored secrets.	yes/no
Platform	Access Management	The Platform will support periodic access review : producing, on demand or on schedule, a complete report of users, their roles, their group derivation and their last activity date, in a form suitable for attestation by a reviewer.	yes/no
Platform	Access Management	Exported events will carry a stable schema with a documented change policy , so that an ESM-built collector does not break silently when the Platform is updated.	yes/no
Platform	AI	The platform supports to opt-out of any usage telemetry (feature usage counts, performance data, error reports) that is used for platform or model improvement.	yes/no
Platform	AI	The Platform will provide a documented, versioned, authenticated REST API covering at minimum: retrieval of findings, policy status, and metrics; and modification of finding triage state.	yes/no
Platform	AI	The Platform will provide an interface consumable by AI coding agents — for example a Model Context Protocol (MCP) server or equivalent documented agent interface— permitting an agent to query findings and policy status within a development session. The Service provider will state whether this interface is maintained by the service provider or by the community .	yes/no
Platform	AI	The Platform will provide IDE integration for Visual Studio Code and JetBrains IDEs , surfacing findings before commit.	yes/no

Applicable to	Area	Description	Candidate's response (Yes/No): The Candidate shall confirm whether it complies with the requirement by selecting "Yes" or "No."
Platform	AI	IDE analysis will use the same rule set and rule set version as server-side analysis, centrally distributed, so that local and pipeline results agree.	yes/no
Platform	AI	Where the Platform generates fixes , those fixes will never be committed to a protected branch, nor merged, without explicit human review and approval . Any capability to merge automatically will be capable of being disabled by ESM.	yes/no
Platform	AI	The Platform must clearly identify any machine-generated fix delivered through a commit or pull request in the relevant metadata, enabling the ESM to identify AI-generated code retrospectively.	yes/no
Platform	AI	The Platform must re-analyse modified code after a generated fix is applied and confirm that the original finding has been resolved and that no new findings have been introduced.	yes/no
Platform	AI	The Platform must not present a generated fix to the ESM as ready for review unless it has successfully passed the repository's configured build, automated tests and the quality policy defined. The Platform must withhold any fix that fails such validation or clearly identify it as unvalidated.	yes/no
Platform	AI	The Platform must enable the ESM to configure automatic fix generation by repository, portfolio and finding category, allowing the ESM to conduct a limited pilot before wider deployment.	yes/no
Platform	AI	The Platform must clearly identify any machine-generated fix delivered through a commit or pull request in the relevant metadata, enabling the ESM to identify AI-generated code retrospectively.	yes/no
Platform	AI	The Platform can identify or attribute AI-generated code and apply differentiated policy to it.	yes/no
Platform	Reporting	The Platform will provide a portfolio-level view aggregating quality and security status across all repositories, with drill-down to portfolio, repository, file and finding.	yes/no
Platform	Reporting	The Platform will retain historical trend data for at least 24 months , permitting analysis of quality and security posture over time.	yes/no
Platform	Reporting	The Platform will provide bulk export of metrics via API , enabling ESM to build its own reporting, e.g., in Microsoft Power BI.	yes/no
Platform	Reporting	The Platform will provide exportable reports in PDF and/or CSV suitable for distribution to management.	yes/no
Platform	Reporting	The Platform will support user-defined dashboards combining metrics of ESM's choosing.	yes/no
Platform	Reporting	The Platform will report security findings in a form suitable for evidencing compliance activity , filterable by severity, CWE and remediation status.	yes/no

Applicable to	Area	Description	Candidate's response (Yes/No): The Candidate shall confirm whether it complies with the requirement by selecting "Yes" or "No."
Platform	Performance	The Platform will support at least 1000 repositories and at least 5,000,000 lines of code under continuous analysis without degradation.	yes/no
Platform	Performance	The Platform will scale to 10,000,000 lines of code without architectural change or migration to a different deployment model.	yes/no
Platform	Performance	The Platform will sustain at least 20 concurrent analyses , bursting to 30 , without queuing.	yes/no
Platform	Performance	Pull request analysis feedback will be returned within 10 minutes for a repository of up to 100,000 lines of code.	yes/no
Platform	Maintenance	Platform updates, rule set updates and vulnerability database updates will be delivered without requiring action by ESM , and will be included in the subscription price.	yes/no
Platform	Maintenance	The platform must enable the ESM to defer or pin rule set versions , so that a rule change delivered by the Service Provider does not cause previously compliant repositories to fail without ESM's decision. Where deferral is not supported, the Service Provider will state the advance notice given before behavior- changing rule updates.	yes/no
Platform	Maintenance	Planned maintenance will be notified at least 5 business days in advance and, where it causes service interruption, scheduled outside 07:00–19:00 CE(S)T on business days.	yes/no
Platform	Maintenance	The Platform will allow ESM to monitor its consumption against its entitlement , with warning before an overage threshold is reached.	yes/no
Platform	Migration	The platform must enable the ESM will be able to export all of its data — findings, triage decisions, metric history, policy definitions and configuration — on demand, in documented machine-readable formats, at no additional cost , throughout the contract term.	yes/no

Service Requirements

Candidates are expected to comply with the requirements below listed. However, failure to comply with one or more mandatory requirements will not automatically result in the rejection of the Proposal.

Applicable to	Area	Description	Candidate's response (Yes/No): The Candidate shall
---------------	------	-------------	--

			confirm whether it complies with the requirement by selecting “Yes” or “No.”
Service Provider	Security	The Service Provider will commission an independent penetration test of the Platform at least annually and make an executive summary available to ESM on request.	yes/no
Service Provider	Hosting	The Service Provider will state whether ESM source code is transmitted to and retained by the Platform , or whether only derived metadata is retained. If source code is retained, state for how long, for what purpose, and how it is deleted.	yes /no
Service Provider	Hosting	The Service Provider will confirm whether any support personnel outside the EU/EEA can access ESM data or systems, in what circumstances, from which jurisdictions, and under what controls.	yes/no
Service Provider	Hosting	Support and engineering access to ESM data from outside the EU/EEA will not occur. Where the Service Provider cannot meet this absolutely, it will describe the compensating controls it applies to any non-EU/EEA access: named and vetted individuals, prior ESM approval per access, time-boxed and least-privilege sessions, session recording, and full audit logging available to ESM.	yes/no
Service Provider	Hosting	The Service Provider will state its routine retention policy for ESM source code and analysis artifacts during the contract — how long transient copies persist after analysis completes, and whether ESM can configure a shorter retention.	yes/no
Service Provider	Performance	The Service Provider will state any hard limits on analyses per day or per month, lines of code analyzed, or API request rates, within the licensed scope.	yes/no
Service Provider	Performance	The Service Provider will operate a public status page and provide proactive notification of incidents affecting the Platform.	yes/no
Service Provider	Performance	The Service Provider will state its recovery time objective (RTO) and	yes/no

		recovery point objective (RPO) for the Platform.	
Service Provider	Maintenance	The Service Provider will publish release notes and a rule set changelog for every update affecting analysis behavior.	yes/no
Service Provider	Maintenance	The Service Provider will give advance notice of any breaking change to APIs, integrations, pipeline tasks or authentication mechanisms. ESM requires at least 90 days; the Service provider will state its committed notice period.	yes/no
Service Provider	Maintenance	Documentation is sufficient for ESM to operate and reconfigure the Platform without the Service Provider's assistance. Administrator enablement has covered the configuration-as-code workflow.	yes/no
Service Provider	Maintenance	The Service Provider will operate a published deprecation policy stating the minimum support period for a feature after deprecation is announced.	yes/no
Service Provider	Maintenance	The Service Provider will provide a product roadmap covering at least the next 12 months and will state how customers can influence it.	yes/no
Service Provider	Maintenance	The Service Provider will state its policy on version currency — whether ESM will always be on the current version, and whether ESM has any ability to defer platform upgrades.	yes/no
Service Provider	Migration	On termination, the Service Provider will provide read-only or export access for a stated period to allow ESM to retrieve its data.	yes/no
Service Provider	Migration	The Service Provider will deliver administrator enablement for ESM platform administrators, covering policy configuration, rule set management, access control, troubleshooting, and the declarative configuration-as-code workflow .	yes/no
Service Provider	User support	The Service Provider will provide technical support in English , available at minimum during business hours in Central European Time.	yes/no
Service Provider	User support	The Service Provider will operate a documented severity classification for support incidents and will commit to response and resolution targets per severity.	yes/no
Service Provider	User support	The Service Provider will provide at least two support channels , one of which will be a ticketing system	yes/no

		providing ESM with visibility of ticket status and history.	
Service Provider	User support	The Service Provider will provide a named escalation path with defined escalation triggers and named contacts at each level.	yes/no
Service Provider	User support	The Service Provider will state whether a named technical account manager or customer success contact is included, and at what service level.	yes/no
Service Provider	User support	The Service Provider will provide publicly accessible product documentation and a searchable knowledge base.	yes/no
Service Provider	User support	Support will be available to all ESM developers , not solely to a limited number of nominated administrators. Where a limit applies, the Service Provider will state it.	yes/no
Service Provider	User support	The Service Provider will report support performance against its committed targets at agreed intervals.	yes/no