OPEN CALL FOR TENDERS

*concludes with **a single Framework service contract***

Tender Documentation

External Cloud based Training Platform Access and Support Services

F-CBU-22-T34

Part 1 **Introduction to ENISA**

Part 2 **Terms of Reference**

Part 3 **Tender Specifications**

Annex I	Legal Entity & Financial ID Forms
Annex II	Simplified Financial Statement form
Annex III	Declaration on honour on exclusion criteria and selection criteria
Annex IV	Financial Offer form
Annex V	Draft Framework Service contract
Annex VI	Power of Attorney for Consortium Forms
Annex VII	Sub-Contractors Form
Annex VIII	Administrative ID and Declaration form

e-Submission

*Offers via e-Submission portal **ONLY***

CONTENTS

PART 1 ABOUT ENISA 4

PART 2 TERMS OF REFERENCE 6

I. SCOPE OF THIS TENDER 6

1. GENERAL DESCRIPTION OF THE REQUIRED SERVICES 7

2. DESCRIPTION OF SERVICES TO BE PROVIDED 8

2.1 summary of services 8

2.2 Detailed description of the services 9

2.4 Requirements of the service provision 16

3 SPECIFIC REQUIREMENTS 16

3.1 Provision of services - Contract Manager 16

3.2 Expected Skills 17

3.2 Experts profiles 18

3.2.1 Junior Expert profile 18

3.2.2 Senior Expert profile 18

4. PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATION 18

5. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER 19

5.1 GENERAL REQUIREMENTS 19

6. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER 20

7. TENDER RESULT AND ESTIMATED CONTRACT VALUES 21

8. DATA PROTECTION AND TRANSPARENCY 21

9. MARKING OF SUBMITTED DOCUMENTS 23

10. PRICE 23

11. PRICE REVISION 23

12. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER 23

13. PERIOD OF VALIDITY OF THE TENDER 23

14. PROTOCOL ON PRIVILEGES & IMMUNITIES OF THE EUROPEAN UNION 24

15. PAYMENT ARRANGEMENTS 24

16. CONTRACTUAL DETAILS 24

PART 3 TENDER SPECIFICATIONS 25

1. INFORMATION ON TENDERING 25

2. STRUCTURE AND CONTENT OF THE TENDER 26

3. ASSESSMENT AND AWARD OF THE CONTRACT 30

3.1 EXCLUSION CRITERIA 30

3.2 SELECTION CRITERIA 31

3.3 AWARD CRITERIA 34

4. TENDER OPENING 35

5. OTHER CONDITIONS 36

5.1 Validity 36

5.2 Lots 36

5.3 Additional Provisions 36

5.4 No obligation to award the contract 36

6. SPECIFIC INFORMATION 37

6.1 Timetable 37

PART 1 ABOUT ENISA

1.1 INTRODUCTION

The European Union Agency for Cybersecurity (ENISA) was established by the European Parliament and the Council Regulation (EU) No 2019/881 of 17 April 2019 (OJ L 151/15, 07.06.2019). ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.

1.2 SCOPE

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

The permanent mandate and enhanced role of the Agency established by the 2019 EU Cybersecurity Act (CSA) and ENISA's new strategy are two milestones that mark an unprecedented and exciting period in the 17 years of the Agency´s life.

1.3 OBJECTIVES

The Agency's objectives are as follows:

- ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.
- ENISA shall assist the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity.
- ENISA shall support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.
- ENISA shall promote cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies, and relevant private and public stakeholders on matters related to cybersecurity.
- ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents.
- ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.

- ENISA shall promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses.

2. ADDITIONAL INFORMATION

Further information about ENISA can be obtained on its website: www.enisa.europa.eu/.

PART 2 TERMS OF REFERENCE

I. SCOPE OF THIS TENDER

The purpose of this Call for Tenders is the purchase of access licenses to a cloud-based Training Platform populated with a pre-existing portfolio of courses and additional associated Services for ENISA Trainings & Exercises (TREX) Strategies. These services provided by ENISA, are intended to complement efforts by European Union Member States and those at Union level to further improve their readiness and capability to respond to large-scale cybersecurity incidents or crises.

By means of this Call for Tenders ENISA seeks to conclude a single framework contract with a qualified economic operator capable of providing the external cloud-based Training Platform and associated Support Services as stipulated in the Technical Specifications outlined below.

Subject of the tender	Maximum budget
External Cloud based Training Platform Access and Support Services	A maximum budget of **€ 4 000 000 (four million) Euro** over the maximum possible period of **4 years**
Last date for dispatch of offers	**7th November 2022 until 18:00 CET**

PLEASE NOTE:

a). *In the case where unforeseen circumstances result in this contract being consumed faster than originally planned, the Agency reserves the right to consider conducting a 'Negotiated procedure without prior publication of a contract notice' with the existing contractor in order to increase the maximum amount stated above by up to 50%. This procedure being fully in accordance with Article 164(4) and Annex I - point 11.1(e) of the EU Financial Regulation (FR)).*

b). *This tender procedure is limited to tenderers which are legally incorporated or which have an incorporated subsidiary in a Member State of the European Union/EEA as well as SAA countries[1] . The Agreement on Government Procurement (GPA) does not apply to EU Regulatory Agencies and as such, ENISA cannot accept offers from legal entities based in 'third countries".*

IMPORTANT: For entities outside the EU (including UK based entities):

The United Kingdom is now considered a 'third country by the European Union'. ENISA cannot therefore accept submissions from legal entities based in the UK, nor can a UK legal entity be nominated as part of a consortium. Subcontracting of UK (and other third country) entities is allowed. In these cases, any transfer of personal data to third countries shall only take place after prior authorisation of ENISA and shall fully comply with the requirements laid down in Chapter V of Regulation (EU)2018/1725.

Method of submitting tenders: 	***e-Submission portal***	***YES***
	Courier or postal service	*NO*
	By hand	*NO*
	By email	*NO*

[1] Under the Stabilisation and Association Agreements (SAA) economic operators established in FYROM, Albania, Montenegro, Serbia, Bosnia and Herzegovina and Kosovo have been granted access to procurement procedures of the Union institutions, agencies and bodies.

1. GENERAL DESCRIPTION OF THE REQUIRED SERVICES

ENISA aims to reinforce its capacity and capabilities, in line with its Strategies for Trainings & Exercises, by purchasing access licenses to a cloud-based Training Platform populated with a pre-existing portfolio of courses and additional associated Services from specialised service providers in the cybersecurity (training) domain. The ENISA Trainings & Exercises (TREX) Strategies are based on an approach that aims to build a portfolio that utilises as much as possible self-paced e-learning style material for basic-level knowledge building purposes. A wide range of relevant and up-to-date topics have to be covered and upscaling of the number of trainees should be feasible. In the next level of activities, shift of the goals towards deeper knowledge building and adds of either more hands-on participation and/or in person training activities will take place. The last level is either more exercise oriented, offering the opportunity to test whether acquired skills can also be applied in real-life like situations, or it aims to train more specialised skills by means of invoking a high degree of active participation from the trainees.

For the first level of Capacity Building activities described in the above paragraph (but not limited to that only), ENISA is looking to purchase access licenses to a cloud-based Training Platform populated with a pre-existing portfolio of courses and additional associated Services. By choosing to go for an “as-a-service” model, ENISA can immediately offer to its stakeholders a wide range of trainings and exercises on various topics.

The available content should be up-to-date and in line with current cybersecurity trends and it should be easily accessible from any computer with internet connectivity and a recent browser installed, and this for all popular operating systems (Windows based, OS-X based, Linux based).

The additional services would allow ENISA to request the creation of content that is purely tweaked towards its stakeholders and it should be made available exclusively to them. Other potential additional services of interest are more situated in the area of skills-validating exercises and they can potentially include gamification elements.

Providing access to trainees to specific courses in the platform can be done in an ex-ante and ex-post context.

Ex-ante services are defined as cyber security services which will contribute to increased preparedness and resilience of the Union’s essential and important entities (as defined in the proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union[2]) against potential imminent threats.

Ex-post services are defined as cyber security services which either help entities to respond to an actual incident but also can be invoked to remediate specific skill gaps that were identified during the analysis of specific real incidents.

[2] https://digital-strategy.ec.europa.eu/fr/node/433

2. DESCRIPTION OF SERVICES TO BE PROVIDED

2.1 SUMMARY OF SERVICES

The table below provides an overview of the services that ENISA may request from the prospective contractor under this framework contract. A detailed description of each service is provided in section 2.2 of this Tender Document.

Service	Description
Online Training Platform as a Service, including pre-existing training portfolio	• Secure online Training Platform for self-paced Trainings, accessible using the most common browsers on an, as wide as possible, range of operating systems. • The browser and an internet connection (HTTPS) should be the only technical requirements for the participants. • The included pre-existing Training content should cover a broad range of actual and relevant topics in the broad area of cybersecurity. • Training modules should be well structured, grouping the trainings into relevant topic-based categories or tracks. • Can be provided ex-ante (preparedness) or ex-post (improving weaknesses, remediating skill gaps). • Access to individual users granted by means of a “license” model.
Setup of Training Platform according to ENISA specifications	• Enrolment to the training courses should be via a “low threshold” process and ENISA should have the final “gatekeeper” role. • Only data necessary for the identification of the users and the correct functioning should be stored and processed compliant with the GDPR and in line with EDPS requirements for ENISA. • Setting up an environment that meets the above requirements and provides a smooth experience for all enlisted users. • Displaying the ENISA name and logo inside the platform.
Training Module Development Services	• Allowing for the development of new bespoke training modules or complete tracks according to ENISA specifications. • With the option of making them only available to ENISA users. • For theory-based modules, technical modules, hands-on modules and video-based modules or any combination of them.
Platform Development Services	• Allowing ENISA to request support on or development of specific (technical) features of the platform.
Optional Skill Validation Event Services[3]	• Services that allow the creation and conduction of hands-on events that aim to test acquired skills of the participants, either individually or as a team. • Ideally, these skills can be acquired by following specific courses that are featured in the Training Platform. • Additionally, after the conclusion of such an event, specific training modules can be suggested in order to improve certain skills. • This is very relevant in the area of SOC-related skills.

[3] Optional services will not be evaluated although they could be included in the list of services to be contracted

2.2 DETAILED DESCRIPTION OF THE SERVICES

In this section the first paragraph under each sub-section covers the minimum requirements and the second paragraph the requirements that are considered as being advantageous and they can lead to bonus points being awarded to the score of the quality of the technical offer (award criteria).

2.2.1 ONLINE TRAINING PLATFORM AS A SERVICE, INCLUDING PRE-EXISTING TRAINING PORTFOLIO

Minimum requirements:

- ENISA expects the training portfolio to cover a broad range of actual and relevant topics, concepts, tools and techniques.
- The offered training portfolio should be well structured, grouping the trainings into relevant topic-based categories or tracks, offering some kind of “learning paths” for people that are new to the domain or that can guide students towards acquiring the necessary skills expected for certain roles or job profiles.
- Based on specific needs of our stakeholders, ENISA should have the option to suggest such learning paths to these stakeholders, based on their requirements.
- The available topics should be relevant for students with diverse levels of pre-knowledge and for different target audiences (e.g.: not aimed only at incident responders or any other job role-profile).
- ENISA should receive a well-structured overview of the portfolio so we can use it in our own communications to our key stakeholders or place it on our current and future websites.
- Any important updates or changes to this portfolio should be communicated in advance to ENISA.
- Access to the platform will be granted by means of a license model: a single license should grant access to a user and the user should get access to the full portfolio.
- Any processing of personal data in the context of the contract shall comply with Regulation (EU) 2018/1725 (EDPR)[4], and in accordance with the provisions of Section 8 (DATA PROTECTION AND TRANSPARENCY) of these tender specifications. Location of the processing shall be only within EU/EEA. The service provider shall only process personal data under the instructions of ENISA and shall not engage in any further processing of personal data (of the users of the platform) for its own purposes.

Potentially Advantageous Requirements:

- If the portfolio of trainings offered by the tenderers can be aligned with Service Frameworks like NICE[5], the FIRST Services Framework[6] or similar initiatives[7], this can be considered as an advantage.
- It can be considered as an advantage if ENISA has the ability to also provide access to the platform for accounts with a “supervisory” role. This type of accounts should have the

[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

[5] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

[6] https://www.firslorg/standards/frameworks/

[7] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

possibility to monitor the progress of groups of students (all grouped under a same stakeholder) along the suggested “learning paths” that were provided to them.
- The ability to provide elements like gamification, badges, trophies, “certificates” and similar items that can be presented to encourage students can be considered as an advantage.

2.2.2 TECHNICAL REQUIREMENTS

Minimum Requirements:

- Users should be able to access the trainings from the most common browsers on an as wide as possible range of operating systems. The browser and an internet connection (HTTPS) should be the only technical requirements for the students.
- The potential users will be operating Windows, Apple and Linux operating systems. Typical examples of popular browsers are Firefox, Chrome, Edge and Safari.
- Another advantage of the browser and HTTPS only approach is that administrators do not have to open special ports on corporate firewalls to allow participants to connect to the training services from the corporate network.
- Any potential changes to the requirements for browsers should be communicated in advance to ENISA.
- Ability for single sign - on (SSO) using existing Microsoft Azure Active Directory.

Potentially Advantageous Requirements:

- Possibility of (future) integration of other single sign on technologies such as SAML, OpenID or single sign on with the European Commission Authentication Service (ECAS) will also be considered as an advantage.

2.2.3 SECURITY REQUIREMENTS

Since ENISA is the EU Cybersecurity Agency and the potential users of this service consist for a large part of members of the EU CSIRT Network[8] ,particular attention has to be paid on how the prospective contractor covers the "Prevent", "Detect" and "Respond & Recover" aspects of (cyber) incidents.

Minimum Requirements:

The tenderer should provide ENISA with information whether the following measures have been implemented and if possible, how they have been implemented.

Prevent:

- An inventory of components that make up the system(s) (incl. dependencies) is known and documented.
- Network Redundancy is in place (at least dual internet links are present).
- System components inventories are updated in line with changes.
- Network Diagram in place.
- Data Flow Diagram in Place.

[8] https://csirtsnetwork.eu/

- All components are fully supported by their vendors.
- The system is subject to Change control.
- Patching (at least Critical and Security issues) occurs Monthly.
- O/S are hardened in line with recognised standards (CIS, NIST).
- Server Software such as DBs / Web Servers are hardened in line with recognised standards (CIS, NIST).
- Generic admin accounts are either removed, renamed or disabled.
- Default credentials have been changed.
- Admin access is provisioned in line with least privilege (i.e. developers do not have access to Prod).
- Admin access is reviewed regularly and unrequired access removed
- Information is encrypted at rest.
- Anti-Virus is up to date and active response is enabled.
- Secure HTTPS configuration is in place for web facing apps.
- Internet facing components reside in a DMZ.
- Static firewall is in place.
- Firewall rules are implemented in line with least privilege.
- Network IPS is enabled (and blocking) on the Firewall.
- Network IPS is enabled between the DMZ and internal networks.
- Host based IPS is running on servers.
- A Web Application Firewall is in place and all traffic is inspected and malicious traffic blocked (HTTPS is decrypted).
- Anti-DDoS facility is in place in the event of an attack.
- On retirement, systems are securely destroyed.

Detect:

- System configurations scans are done vs an agreed benchmark such as CIS.
- The system is vulnerability Scanned [Monthly/Quarterly].
- Anti-Malware Scans occur weekly.
- Security Events are Logged and Monitored in Real Time.
- Pen Tests Occur at least annually by a third party.
- Certificates are monitored for expiry and configuration changes.
- Alerts are generated for newly opened server ports.

Respond & Recover:

- Systems are highly available.
- A DR plan exists.
- The DR Plan is Tested Annually.
- System back-ups are in place and tested for adequacy.
- Backups are stored or performed in an alternate location, separated from the primary location.
- Up-to-date IT Configuration Management Records are available for IT Assets, including configuration records and associated system documents to enable recovery.
- Business have agreed on Recovery Time Objective.
- Business have agreed on Recovery Point Objective.

- The tenderer should provide ENISA an overview of their incident response procedures. This should provide insight in the key actors of the incident response (IR) process: the prospective contractor, ENISA (Information Security Officer, Head of Sector for Trainings and Exercises, DPO), platform users enrolled by ENISA and any other key players like: CSIRTs, Member State Data Protection Authorities, etc.
- The tenderer should also propose how any incident related information (e.g. reports) can be exchanged with ENISA in a secure manner.
- The tenderer should provide insight in how they will provide "documentation" related to a security incident: report, follow-up, remediation & recovery.

2.2.4 OTHER REQUIREMENTS

Minimum Requirements:

- Enrolment to the training courses should be via a "low threshold" process and ENISA should have the final "gatekeeper" role.
- Reporting options should cover at least basic, aggregated reporting that allows ENISA to have a high-level overview of the usage of the provided services and should allow ENISA to report aggregated usage data back to stakeholders.
- The default license services should cover a full period of 12 months, starting from a date agreed upon by ENISA and the prospective contractor, decided upon during a kick-off meeting that takes place shortly after ENISA purchased a batch of licenses – with possibility to be renewed, based on renewal of the Framework Contract and for a maximum period of 48 months.
- Normally, this starting date cannot be set on a date earlier than the date upon which the setup of the platform according to ENISA specifications has been approved by the ENISA PM.
- ENISA TREX Sector staff involved in the project should get up to 10 free licenses that can be used for oversight, follow-up and demo purposes.
- ENISA enrolled users shall connect to a landing page with ENISA logo and then they will start the authentication process using ENISA Azure AD.
- Users should be able to get professional and high-quality support when using the Training Services.
- ENISA should be able to escalate urgent requests and issues to the Service Provider and this escalation service should be covered by a reasonable SLA.

Potentially Advantageous Requirements:

- Any options that make the enrolment process smoother for ENISA can be considered as an advantage.
- More detailed reporting options can be considered as an advantage. The final implementation should be discussed during the kick-off phase of the service, based on the options that the winning tenderer proposed in their tender while still being compliant with data protection regulations.
    - The final options should always be compliant with EDPR and GDPR, in accordance with Section 8 (DATA PROTECTION AND TRANSPARENCY) of these tender specifications.

- If ENISA would be able to receive reports on the number of support requests that our users have initiated and if these reports include important information like "open requests", this can be considered as an advantage.
- An enrolment mechanism that will allow ENISA to decentralise the enrolment will be considered as an advantage. For example, supporting a role of an 'enrolment manager' for a specific team who will be able to enrol team members respecting the total number of licenses assigned to the team.
- Offering ENISA the possibility to purchase licenses at a pro-rate price (and corresponding validity duration) can be considered as an advantage.

2.2.5 SETUP OF TRAINING PLATFORM ACCORDING TO ENISA SPECIFICATIONS

The tenderer should provide a fixed-price proposal for setting up the Training Platform and corresponding training portfolio according to the following requirements:

- The platform should be in accordance with the provisions of Section 8 (DATA PROTECTION AND TRANSPARENCY) and be fully located in the EU.
- The platform should be provisioned to be able to allow for a smooth operation when the number of concurrent users is equal to the purchased licenses by ENISA.
- ENISA enrolled users shall connect to a landing page with ENISA logo and then they will start the authentication process using ENISA Azure AD.
- ENISA might be requested to provide access to users who do not wish to provide their real email address (or any other personal data) to the platform's provider. In this case the user will have a user identifier assigned by ENISA's Azure AD (as a fictive example: user123@grainings.eu).
- As the user's email will not be provided to the platform provider, a platform administrator assigned by ENISA shall be able to enrol the user without using the user's email for validation.
- Once inside the Platform, the ENISA logo and where possible look and feel should be applied, displaying the ENISA logo is considered to be a minimum requirement and should be an integral part of the fixed-price proposal by the tenderer.
- All onboarding material and help functionality (help text, help buttons, etc.) should be in line with the ENISA scope.
- Once the user engages in deeper technical areas of trainings, more flexibility can be allowed with regards to look & feel specifications since it might require much bigger efforts to apply rebranding to large amounts of pre-existing material.
- In an initial kick-off meeting with the winning tenderer, more advanced customisation options that are out-of-scope and budget of the proposed fixed price minimum proposal by the tenderer can be discussed but ENISA cannot commit by default to such proposals.
- The final Setup Services agreed upon will be purchased by ENISA and it will be treated on a Project basis for follow-up and acceptance.
  - Regular follow-up meetings will have to be planned and held.
  - Testing will be done by ENISA TREX staff.
  - Final acceptance will have to be approved by the ENISA PM.
  - Payment can only be done when the provided Setup Services have been completed and accepted by ENISA.
- After the initial setup, any potential future ENISA requests in this area can be covered by the “Platform Development Services” offered by the prospective contractor.

2.2.6 TRAINING MODULE DEVELOPMENT SERVICES

- ENISA should have the option to request the development of specific training modules or courses that will be made available to ENISA enrolled users only.
- When such content is newly developed, it should be branded in full alignment with ENISA look & feel.
- ENISA would be the owner of the content and portability should be guaranteed.
  - This could be transfer of text files, media, scripts, Virtual Machines, etc to ENISA whenever ENISA requests it.
  - The content cannot be made available to other users without specific approval by ENISA.
- The tenderer should provide in their offer daily rates for experts involved in the development of new training modules.
  - Daily rates for Junior Profiles.
  - Daily rates for Senior Profiles.
- The training material should be adapted to self-paced learning and should allow inclusion of elements like hints, questions to be able to validate if the students grasped what was presented to them, badges, certificates, etc.
- Distinction can be made for different types of content:
  - Simple text-theory-foundation based content, allowing simple validation of student take-up and progress.
  - More technical content that might require more setup, screenshots, etc. while still allowing simple testing of student take-up and progress.
  - More complex content that requires a hands-on approach by students and typically involves deploying pre-configured environments and also potentially require more complex registration of student take-up and progress.
  - Content that includes the creation of media like videos.
- The tenderer should indicate in their offer the estimated indicative average prices for development of new content belonging to the above categories.
  - In the case of creation of media like video, the contractor is allowed to provide other indicative pricing mechanisms since this kind of formats are difficult to align with reliable day prices.
- If ENISA would request the creation of new training material, the prospective contractor is expected to provide to ENISA a fixed-price proposal whereby the proposal includes the indicated breakdown of the costs, based on the above points and provided daily rates.
- The final proposal agreed upon will be purchased by ENISA and it will be treated on a Project basis for follow-up and acceptance.
  - Regular follow-up meetings will have to be planned and held.
  - Testing will be done by ENISA TREX staff.
  - Final acceptance will have to be approved by the ENISA PM.
- Payment can only be done when the provided Services have been completed and accepted by ENISA.

2.2.7 PLATFORM DEVELOPMENT SERVICES

- ENISA should have the option to request the development of specific features related to the Platform.
- The results of these developments will potentially only be allowed to be deployed for ENISA enrolled users.
- They content cannot be made available to other users without specific approval by ENISA.
- The tenderer should provide in their offer daily rates for technical experts involved in the development of new training modules.
  - Daily rates for Junior Profiles.
  - Daily rates for Senior Profiles.
- If ENISA would request such services, the prospective contractor is expected to provide to ENISA a fixed-price proposal whereby the proposal includes the indicated breakdown of the costs, based on the provided daily rates and the description of tasks to be performed and their foreseen duration.
- The final proposal agreed upon will be purchased by ENISA and it will be treated on a Project basis for follow-up and acceptance.
  - Regular follow-up meetings will have to be planned and held.
  - Testing will be done by ENISA TREX staff.
  - Final acceptance will have to be approved by the ENISA PM.
- Payment can only be done when the provided Services have been completed and accepted by ENISA.

2.2.8 OPTIONAL SKILL VALIDATION EVENT SERVICES

Optional services will not be evaluated although they could be included in the list of services to be contracted

- The tenderer should specify the type of services they potentially offer and that allow preparing and organising hands-on style events that aim to test the proficiency of participating teams or individual participants in certain areas.
- The tested skills can either be acquired by the participants by completing (before the Event) certain training modules that are available in the Platform.
- After the completion of such an Event, an evaluation of the performance of the Team (or of the individuals) can be done and suggested training modules can be proposed in order to further perfect skills or to close potential skill-gaps.
- The tenderer should provide:
  - information related to the scope and goals of the proposed Services.
  - Pricing indication for organising such Events.
  - An indication of the number of participants (maximum, minimum, optimal).
  - Indicate if they propose these services for individuals or for teams (or both).
  - Indicate the duration of such an event and the time it takes to prepare for it, both as organiser or as participant.

2.4 REQUIREMENTS OF THE SERVICE PROVISION

The prospective contractor must be able to support ENISA capabilities for at least all the aforementioned (non – optional) services. Support of the services are to be delivered according to the highest standards, in an efficient, and timely manner. The prospective contractor must be able to support ENISA also in preparations for and management of such a service provision as well as during the consultations with Member States or any other ENISA key stakeholders concerning the response to a request, service team assembly and service provision.

The prospective contractor must be able to fit into the ENISA service provision procedure and support the ENISA service provision workflow as necessary. This service provision procedure will be made available to the contractor as and when required.

The prospective contractor must be able to comply with ENISA requirements and obligations of information classification and protection as well as liability and non-disclosure of information.

The tenderer shall also include a description of the working method and working arrangements in place. More specifically how they propose to implement the following:

- Regular follow-up meetings related to the Training Platform (usage, new features or trainings the Contractor will put in place, etc.).
- Specific meetings setup to on-board new (or existing) users.
- The process to on-board a new ENISA stakeholder, including a kick-off meeting with representatives from the stakeholder, the proposal of specific learning paths for the new users, creation of accounts for the stakeholder that allow the progress of users with the proposed paths and this for both ex-ante cases as ex-post (i.e. after an incident occurred).
- The process related to requesting non-Training Platform related services offered by the contractor.
- Escalation processes in case of issues with the Platform that are not resolved in a timely way by the Contractor via the normal support channels.

During the kick-off meeting after signature of the contract, fine-tuning of these procedures will take place and the final procedures will have to be agreed upon by both parties.

The prospective Contractor is expected to provide a proposal for a Service Level Agreement covering the availability of the Training Platform. This Service Level Agreement needs to be agreed upon and approved by ENISA.

The prospective contractor should be able to work together (with guidance from ENISA) with other relevant partners for specific request (including other contractors, MS entities, other ENISA stakeholders, etc.).

All communication with ENISA will be in English, being the working language of ENISA, and all deliverables must be provided in English unless specifically agreed otherwise.

3 SPECIFIC REQUIREMENTS

3.1 PROVISION OF SERVICES - CONTRACT MANAGER

ENISA will designate a contact point and a designated backup to run this contract and it expects the prospective contractor to designate one Contract Manager (and designated backup) to act as the (single) point of contact for all Agency needs.

The Contract Manager shall be responsible for the overall management and administration of the framework contract including the organisation of appointment schedules, requests from and communication with ENISA, i.e. invoicing, etc. The nominated Contract Manager shall be able to communicate fluently in the English language. The contractor shall provide their contact details (as minimum an e-mail address and phone number to which all communication shall be channelled). The Contractor should be able to make use of a ticketing system proposed by ENISA.

The prospective contractor shall ensure that sufficient provisions are made to ensure all holidays/absences of its staff are adequately covered, in order to ensure continuous provision of services.

The tenderer shall also include a description of the working method and working arrangements in place. More specifically how they propose to implement the following:

- Regular follow-up meetings related to the Training Platform (usage, new features or trainings the Contractor will put in place, etc.).
- Specific meetings setup to on-board new (or existing) users.
- The process to on-board a new ENISA stakeholder, including a kick-off meeting with representatives from the stakeholder, the proposal of specific learning paths for the new users, creation of accounts for the stakeholder that allow the progress of users with the proposed paths and this for both ex-ante cases as ex-post (i.e. after an incident occurred).
- The process related to requesting non-Training Platform related services offered by the contractor.
- Escalation processes in case of issues with the Platform that are not resolved in a timely way by the Contractor via the normal support channels.

All communication with ENISA will be in English, being the working language of ENISA, and all deliverables must be provided in English unless specifically agreed otherwise.

3.2 EXPECTED SKILLS

For the performance of the above-mentioned activities, the following skills and experience should be demonstrated by the tenderer in the submitted proposal:

- Relevant EU legislation knowledge and compliance.
- Experience with compliance with data protection requirements under EDPR and GDPR
- Relevant national legislation knowledge and compliance.
- Wide expertise in the field of cybersecurity.
- Being familiar with the tasks performed by CSIRTs and operational incident handling in particular.
- Extensive experience in the field of online training services and training principles in general.
- Experience in transforming concepts for trainings into a format that is ideally suited to self-paced e-learning courses.
- Excellent project management skills including quality assurance.
- Excellent support minded staff that can help users with issues and on boarding.
- Skilled technical staff that can keep the used infrastructure up and running, secure and is able to deal with technical requests.
- Skilled staff that can handle Incident Response in case of security incidents.

- Practical experience in provision of all the services listed in Section 2. DETAILED REQUIREMENTS FOR THE SERVICES described in the offer, at least at the level of detail mentioned in the individual sub-sections (2.2.1 to 2.2.7) describing the services in detail.

3.2 EXPERTS PROFILES

The tenderers shall provide CVs of experts describing their experience in similar projects and possible certifications if available. The team may comprise of a balance of both junior and senior experts. You are required to provide only the CVs of experts deemed relevant and experienced in the above-mentioned topics and as listed in Section 2 (DETAILED DESCRIPTION OF THE SERVICES).

3.2.1 JUNIOR EXPERT PROFILE

The **Junior Expert** shall have:

- At least one (1) year of professional experience and expertise relevant to the provision of the services listed in Section 2 (DETAILED DESCRIPTION OF THE SERVICES) and at least at the level of detail mentioned in the sub-sections 2.2.1 to 2.2.7;
- Good project management skills;
- Excellent quality management skills;
- Excellent customer support skills;
- Good communication and writing skills;

3.2.2 SENIOR EXPERT PROFILE

The **Senior Expert** shall have:

- At least two (2) years of professional experience and expertise relevant to the provision of the services listed in Section 2 (DETAILED DESCRIPTION OF THE SERVICES) and at least at the level of detail mentioned in the sub-sections 2.2.1 to 2.2.7;
- Excellent project management skills;
- Excellent quality management skills;
- Excellent customer support skills;
- Excellent communication and writing skills;
- Excellent project management skills including quality assurance.

4. PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATION

The execution of the activities will take place at the Contractor's premises. Network based collaborative tools (i.e. videoconferencing) will be used as normal working methods. At least the following communication with the contractor is expected:

- A kick off meeting either via teleconference or videoconference.

- Regular video or teleconferences on the progress achieved (in principle every two weeks, exact intervals to be agreed upon during the kick-off meeting).

The contractor, upon invitation, may visit ENISA's premises at Agamemnonos 14 St. Chalandri, 15231, Attiki, for ad hoc meetings.

It should be mentioned that the Contractor's costs of potential business trips - if deemed to be needed - should be included in the total offer. ENISA will not additionally reimburse the contractor for taking part in meetings or events. In order to save project resources, the information exchange will be performed mainly via electronic means, such as e-mail, web and phone conferencing.

5. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

In this section it is outlined how ENISA expects the tenderer to structure its technical offer responding to this tender. In general, ENISA expects the tenderer to explain how the below mentioned requirements will be met by the tenderer.

5.1 GENERAL REQUIREMENTS

The Tenderer shall enclose with their "Technical Offer", all documents and information that will enable its offer to be assessed in terms of quality and of compliance with the specifications above (the technical description).

The Technical Offer shall include the following:

- Presentation of the tender proposal;
- Summary in the form of a table of the ability of the tenderer to provide services listed in Section 2 (DETAILED DESCRIPTION OF THE SERVICES). Specifically, the offered services should at least meet the minimum requirements as described in the sub-sections 2.2.1 to 2.2.7., including requirements on personal data protection.
- For the Training Platform with pre-existing content, a good overview of the available training material should be provided.
- Examples of previous related works or activities that the contractor has undertaken in the past.
- Evidence and material demonstrating expertise in the fields covered by this call for tender;
- Management practices, planning and resource allocation to tasks and experts, available to be used in order to meet the Agency's requirements;
- Project management methodology that will be used for projects under this framework contract, explaining how possible projects would be carried out efficiently, timely and effectively. Specifically, for the Services different from the Training Platform Service, the contractor should provide which method of project management they will use during the delivery of the services;
- In the case of a tender being submitted by a consortium, a description of the input from each of the consortium members and the distribution and interaction of tasks and responsibilities between them;
- A description of sub-contracting arrangements foreseen (if any) with a clear indication of the tasks that will be entrusted to a sub-contractor and the award methods to be used in relation to these

tasks. A statement by the tenderer guaranteeing the eligibility of any sub-contractor shall be included as well, in case the subcontractor(s) are not known at the moment of the tender submission.

- A relevant risk analysis with mitigation measures. Specifically, this should include proposals on how to tackle potential issues with unavailability of the provided services due to issues encountered by the prospective contractor themselves and clear description on how both end users of the services can signal issues to the contractor and how ENISA can escalate any unsolved and/or important issues encountered with the service.

The content of the technical offer is important for the award of the contract and the future execution of any resulting contract. Some guidelines are given above, but attention is also drawn to the award criteria, which define those parts of the technical proposal to which the tenderers should pay particular attention.

The technical proposal should address all matters laid down in the technical specifications as described. Please note that, to ensure equal treatment to all tenderers, it is not possible to modify your offer after the expiry date. Consequently, incompleteness in this section can only result in a negative impact for the evaluation of the award criteria.

6. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

The Financial offer must be drawn up using the **Financial Offer form provided (see Annex IV)**.

In order to be considered a valid offer, it must be duly filled in, dated, stamped, and signed by the authorised person.

In calculating your fixed costs and fees as well as for the scenarios, due regard should be given to the following when filling in Annex IV – Financial Offer form:

- Cost of the junior and senior experts. Experts' fees should be calculated as all-inclusive of any relevant costs i.e. necessary insurance (liability insurance), technical equipment necessary to provide services requested, accommodation and subsistence costs, costs of any additional supporting and complementary actions needed to provide requested service;
- Cost of provision of platform licences (price per user with scale of volume with provision of validity of 356 days after start date)
- Optional skill validation services (if applicable). A catalogue of optional services with pricing are welcomed. You can either fill in page 3 of the Financial offer form or provide your own price catalogue. Please provide a description of the services in the respective box. It should be noted that any optional services will not be calculated as part of the price points formula.

Please take special care to enter prices **in all compulsory boxes**, as described. Failure to provide a fully completed form may result in your offer being declared invalid and not being further evaluated.

7. TENDER RESULT AND ESTIMATED CONTRACT VALUES

The result of the evaluation of tenders will be the awarding of a single Framework Service Contract. The estimated overall maximum contract value without this being binding for ENISA is **four million Euro (€ 4.000.000,00)** over a maximum possible period of four (4) years.

(Please note that in the case where unforeseen circumstances result in this contract being consumed faster than originally planned, the Agency reserves the right to consider conducting a 'Negotiated procedure without prior publication of a contract notice' with the existing contractor in order to increase the maximum amount stated above by up to 50%. This procedure being fully in accordance with Annex I - point 11.1(e) of the EU Financial Regulation (FR)).

8. DATA PROTECTION AND TRANSPARENCY

Processing of personal data in the context of this contract shall comply with the legal framework on data protection, i.e.:

- **Regulation (EU) 2018/1725[9] ('the EDPR')** as concerns personal data processing by the selected contractor, processing data in execution of the contract with ENISA.

The EDPR constitutes the specific data protection legal framework applicable to institutions, bodies, offices and agencies of the European Union, including ENISA, mirroring the GDPR applicable within the Union.

ENISA is the controller under this Regulation and the prospective contractor is the processor. The processor shall act only under the instructions of ENISA. ENISA's terms and conditions concerning procurement contracts are included in Article II.9.2 of the draft contract in Annex V.

- **Regulation (EU) 2016/679[10] (General Data Protection Regulation – 'the GDPR')** as concerns personal data processing carried out by the contractor on its proper behalf as a controller.

Processing of personal data by ENISA as contracting authority:

Information on the processing of personal data by ENISA as contracting authority in charge of the present procurement procedure is available in the Privacy Statement on the ENISA website as well as in Article II.9.1 of the draft contract in Annex V. In this context, please be informed that ENISA may register your personal data as a tenderer or selected contractors in the Early Detection and Exclusion System (EDES) if you are in one of the situations mentioned in Article 136 of the Financial Regulation. The relevant Privacy Statement is available on the European Commission's website, here: http://ec.europa.eu/budget/explained/management/protecting/protect_en.cfm#BDCE.

Processing of personal data by the selected contractor:

[9] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295/39 21.11.2018

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88

Personal data processing in execution of the contract between ENISA and the selected contractors shall comply with Regulation (EU) 2018/1725 (the EDPR).

The processing of personal data shall happen in accordance with Article 29 of the EDPR. In particular, the selected contractor shall comply with the following:

- to process the personal data only on documented instructions of ENISA, in particular with regard to the purposes of the processing, the categories of data that may be processed, the recipients of the data and the means by which the data subject may exercise its rights;
- to ensure that access to personal data is granted to the extent strictly necessary for the implementation of the contract and to ensure that persons authorised to process the personal data have committed themselves to confidentiality;
- to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the personal data, processed or stored;
- not to engage another processor of personal data (i.e. by means of a subcontract), without prior written authorisation of ENISA. Where another processor is engaged for carrying out specific processing activities on the personal data, the same data protection obligations as set out in the contract shall be imposed on the other processor;
- to assist ENISA in the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the EDPR;
- to assist ENISA with its obligations with regard to security of processing, the notification obligations in case of a personal data breach, as well as where applicable cooperation in data protection impact assessments (DPIAs) and prior consultations with the European Data Protection Supervisor (the EDPS)[11], outlined in Art. 33 to 40 of the EDPR;
- to make available to ENISA all information to demonstrate compliance with the obligations laid down in the EDPR and to allow for and to contribute to audits, including inspections, conducted by ENISA or another auditor mandated by ENISA;
- As concerns the localisation of and access to the personal data, to comply with the following:
    - the personal data shall only be processed and held in data centres within the territory of the European Union and the European Economic Area and will not leave that territory. This includes also any backup centres and location of backup data.;
    - the contractor may not change the location of data processing without the prior written authorisation of ENISA;
    - The contractor shall inform ENISA in case of any need for transfer of personal data to third countries or international organisations and will perform such transfer only after written authorisation by ENISA. Any transfer of personal data to third countries or international organisations shall fully comply with the requirements laid down in Chapter V of the EDPR;
    - The contractor shall notify ENISA without delay of any legally binding request for disclosure of the personal data processed on behalf of ENISA made by any national public authority, including

[11] http://www.edps.europa.eu

an authority from a third country. The contractor may not give such access without the prior written authorisation of ENISA;

- To contact the Data Protection Officer (DPO) of ENISA, in charge of monitoring data protection compliance, with any questions arising or in case of need for assistance concerning personal data protection dataprotection@enisa.europa.eu,

In addition, **Article II.9.2 of the draft contract** provided in Annex V is applicable.

Confidentiality:

ENISA will disregard general statements that the whole tender or substantial parts of it contain confidential information. Tenderers need to mark clearly the information they consider confidential and explain why it may not be disclosed. The EU body reserves the right to make its own assessment of the confidential nature of any information contained in the tender.

9. MARKING OF SUBMITTED DOCUMENTS

The tenderer SHOULD NOT mark tender documents (for e.g. the header or footer) with any of the following words: RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET. If the tenderer considers that such markings are required, a prior approval from the ENISA Procurement Coordinator should be obtained BEFORE sending the tender documents. The tenderer should be aware that the information sent to ENISA for procurement purposes is handled in accordance with the governing rules for EU Public Procurement and the EU Financial Regulation framework.

10. PRICE

Prices submitted in response to this Tender must be inclusive of all costs involved in the performance of the contract. Prices shall be submitted only in Euro and VAT excluded.

11. PRICE REVISION

The price quoted must be fixed and not subject to revision during the first year of performance of the contract. From the beginning of the second year of performance of the contract, prices may be revised in accordance with Article I.3.3 of the framework contract.

12. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER

ENISA will not reimburse any costs incurred in the preparation and submission of a Tender. Any such costs must be paid by the Tenderer.

13. PERIOD OF VALIDITY OF THE TENDER

Tenderers must enclose a confirmation that the prices given are valid for (90) ninety days from the date of submission of the tender.

14. PROTOCOL ON PRIVILEGES & IMMUNITIES OF THE EUROPEAN UNION

ENISA is exempt from all taxes and duties, including value added tax (VAT), pursuant to the provisions of Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Union. Tenderers must therefore give prices, which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

15. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out within 60 days of submission of an invoice based on the conditions and provisions set out in Art. I.6 of the draft contract.

16. CONTRACTUAL DETAILS

A Framework Service Contract will be proposed to the successful candidate. Selection of the candidate and / or signature of the Framework Service Contract imposes no obligation on ENISA to order services.

The contract and its annexes draw up the legal, financial, technical and administrative provisions governing the relations between the Agency and the Contractor during its period of validity.

The tender will conclude, valid as of the date of the last signature, with a one-year Framework Service contract, tacitly renewable up to three times for a maximum of four years.

The Agency reserves the right to end the contract at any time, without any obligation to invoke the reason for it, at one months' notice. The Tenderer's offer must be drafted taking fully into account the provisions of the draft Framework Service contract annexed to this call for tenders (See draft contract, in Annex V).

Execution of the Framework Contract will be performed via Specific Contracts/Order Forms.

***Please note** that the general conditions of our standard framework service contract cannot be modified. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. **It is strongly recommended** that you have this draft contract checked and passed by your legal services before committing to submitting an offer.*

PART 3 TENDER SPECIFICATIONS

1. INFORMATION ON TENDERING

1.1 CONTRACTUAL CONDITIONS

In drawing up their offer, the tenderer should bear in mind the provisions of the draft contract (Annex V) attached to this invitation to tender particularly those on payments, performance of the contract, confidentiality, and checks and audits. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. Any limitation, amendment or denial of the terms of contract will lead to automatic exclusion from the procurement procedure.

It is strongly recommended that you have this draft contract checked and passed by your legal representative before committing to submitting an offer.

Before the contract is signed, the Agency may decide to abandon the procurement procedure or cancel the award procedure without the tenderers being entitled to claim any compensation.

1.2 JOINT TENDERS (IF APPLICABLE)

A joint tender is a situation where a tender is submitted by a 'group' of economic operators (consortium). Joint tenders may include subcontractors in addition to the joint tenderers.

Tenders can be submitted by groupings of service providers/suppliers who will not be required to adopt a particular legal form prior to the contract being awarded. However, the Agency will require the grouping:

- Either to have the contract signed by all members (partners) of the grouping. In this case, one of them, as 'Lead Partner', will be responsible for the receipt and processing of payments for members of the grouping, for managing the service administration and for coordination of the contract;
- Or to have the contract signed by the 'Lead Partner' only, who has been duly authorised by the other members to bind each of them (a fully completed 'power of attorney' form for each member of the Group will be attached to the contract according to the template provided by the Agency).

In addition, the composition and constitution of the grouping, and the allocation of the scope of tasks amongst the members, shall not be altered without the prior written consent of the Agency, which can be withheld at its discretion.

In case of a joint offer, each member of the grouping shall provide the following:

- a **Legal Entities form** and a **Power of Attorney of each consortium partner**, must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

- a **Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest** must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

1.3 LIABILITY OF MEMBERS OF A GROUP

Partners in a joint offer assume **joint and several liability** towards the Agency for the performance of the contract as a whole.

Statements, saying for instance:

- That one of the partners of the joint offer will be responsible[12] for only one part of the contract and another one for the rest, or

- That more than one contract should be signed if the joint offer is successful

are thus incompatible with the principle of joint and several liability. The Agency will disregard any such statement contained in a joint offer, and reserves the right to reject such offers without further evaluation, because they do not comply with the tendering specifications.

1.4 SUBCONTRACTING

Subcontracting is permitted in the tender but the contractor will retain full liability towards the Contracting Authority for performance of the contract as a whole.

If the tenderer intends to subcontract part of the service, they shall indicate in their offer which part will be subcontracted and to what extent (% of the total contract value).

Tenderers must ensure that Article II.7 of the contract (Annex V) can be applied to subcontractors.

Tenderers must give an indication of the proportion of the contract that they intend to subcontract.

Tenderers are required to identify all subcontractors.

During contract execution, any change of a subcontractor identified in the tender will be subject to prior written approval of the Contracting Authority.

2. STRUCTURE AND CONTENT OF THE TENDER

2.1 GENERAL

Tenders must be written in **one of the official languages** of the European Union. The working language of ENISA is English.

[12] not to be confused with distribution of tasks among the members of the grouping

Tenders must be written in a clear and concise manner, with continuous page numbering. Since tenderers will be judged on the content of their written bids, they must make it clear that they are able to meet the requirements of the specifications/terms of reference.

2.2 STRUCTURE OF THE TENDER

Based on the ***e-Submission*** environment[13], all tenders must provide information and supporting documentation in two sections:

1) Qualification - data and documentation;

2) Tender offer - data and documentation.

2.3 QUALIFICATION DATA

a) Identification of the Tenderer

The tenderer must fill in all required fields in the qualification section. In case of a joint tender the consortium name has to be provided and an identification of every party in the consortium needs to be added.

The following information should also be provided:

(i) Legal Entities

In order to prove their legal capacity and their status, all tenderers and identified subcontractors must provide a Legal Entity Form with its supporting evidence.

However, the subcontractor(s) shall not be required to fill in or provide those documents when the services represent less than 20% of the overall contract value.

The Legal Entity Form can be generated via the e-Submission application. Alternatively, a standard template in each EU language is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm

Tenderers must provide the following information if it has not been included with the Legal Entity Form:

- For **legal persons**, a legible copy of the notice of appointment of the persons authorised to represent the tenderer in dealings with third parties and in legal proceedings, or a copy of the publication of such appointment if the legislation, which applies to the legal entity concerned, requires such publication. Any delegation of this authorisation to another representative not indicated in the official appointment must be evidenced.
- For **natural persons**, where applicable, a proof of registration on a professional or trade register or any other official document showing the registration number.

[13] For detailed instructions on how to submit a tender please consult the e-Submission Quick Guide available at: https://webgate.ec.europa.eu/digit/opsys/esubmission/assets/documents/manual/quickGuide_en.pdf

(ii) Financial identification

The tenderer (or the single point of contact in case of joint tender) must provide a Financial Identification Form and supporting documents. Only one form per offer should be submitted (no form is needed for subcontractors and other joint tenderers). The form is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm

Remark: Tenderers that are already registered in the Agency's accounting system (i.e. they have already been direct contractors **with ENISA** in the past) must provide the filled in form but are not obliged to provide the supporting evidence.

The form needs to be printed, filled in and then scanned and uploaded in the Qualification section. In case of a joint tender, it has to be uploaded in the ***"Documents"*** section of the Consortium Leader.

(iii) Power of Attorney

In case of a joint tender, an Agreement / Power of Attorney for each partner must be filled in, signed by (an) authorised representative(s), scanned and uploaded. Please choose 'Model A' for an ad hoc grouping or 'Model B' for a legally constituted consortium - see templates in Annex VI (a) and (b)

(iv) Lots interested in *(only in case the tender has multiple lots)*

The tenderer must indicate for which lots the tender is applicable, by ticking the relevant boxes in the section: ***"Interested in the following lots".***

b) Information regarding exclusion and selection criteria:

The tenderer is requested to submit the following documents:

1. Declaration by the Tenderer relating to the exclusion criteria (see 3.1 below)

   The filled-in Declaration form.

   In case of a joint tender, each member of the consortium has to submit a declaration under the respective party name (see template in Annex III)

2. Documents certifying economic and financial capacity (see 3.2.2 below)

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

3. Proof of technical and professional capacity (see 3.2.3 below)

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

If any of the above documents are associated with a specific Lot, please indicate for which Lot it is applicable inside the document AND in the Description field of the attachment *(only in case the tender has multiple lots).*

2.4 TENDER DATA

a) Technical proposal

The technical section is of great importance in the assessment of the bids, the award of the contract and the future execution of any resulting contract.

The technical offer must cover all aspects and tasks required in the technical specification and provide all the information needed to apply the award criteria. Offers deviating from the requirements or not covering all requirements may be excluded based on non-conformity with the tender specifications, and will not be evaluated.

The technical tender needs to be uploaded in the relevant section:

The tenderer selects the "Technical Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

b) Financial proposal

- All tenders must contain a financial proposal, to be submitted **using the form attached as Annex IV.**

The tenderer's attention is drawn to the following points:

- Prices must be quoted in **euro**, including the countries that are not in the euro-zone. As far as the tenderers of those countries are concerned, they cannot change the amount of the bid because of the evolution of the exchange rate. The tenderers choose the exchange rate and assume all risks or opportunities relating to the rate fluctuation.
- **Prices must be fixed amounts**.
- **Estimated travel and daily subsistence allowance expenses must be indicated separately**. *(only if applicable to this procedure)*
    - This estimate should be based on Articles I.5 and II.22 of the draft framework contract (Annex V). This estimate will comprise all foreseen travel and will constitute the maximum amount of travel and daily subsistence allowance expenses to be paid for all tasks.
- **Prices must be quoted free of all duties**, taxes and other charges, including VAT, as the European Union is exempt from such charges under Articles 3 and 4 of the Protocol on the privileges and immunities of the European Union. The amount of VAT may be shown separately.
- Prices shall be fixed and not subject to revision during the performance of the contract.

The total price needs to be encoded in the e-Submission application[14].

- In the box labelled ***'Total amount exclusive of taxes'*** – please add the amount Total P_B from your Financial Offer form.
- In the box labelled ***'Total taxes amount'*** – please put zero *(if this is not accepted by system then enter 0,01)*
- In the box labelled ***'Total amount'*** – again simply add the amount Total from your Financial Offer form or the maximum budget assigned for this tender

[14] In the case of framework contracts, unless otherwise instructed, please add the maximum budget given for this tender

The completed Financial Offer form(s), MUST ALSO be uploaded in the relevant section:

The tenderer selects the "Financial Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

3. ASSESSMENT AND AWARD OF THE CONTRACT

The assessment will be based on each tenderer's bid. All the information will be assessed in light of the criteria set out in these specifications. The procedure for the award of the contract, which will concern only admissible bids, will be carried out in three stages, normally in the order shown below.

The aim of each of these stages is:

1) to check on the basis of the ***exclusion criteria***, whether tenderers can take part in the tendering procedure;
2) to check on the basis of the ***selection criteria***, the legal and regulatory capacity, the technical and professional capacity and economic and financial capacity of each tenderer;
3) to assess on the basis of the ***award criteria*** each bid which has passed the exclusion and selection stages.

Only tenders meeting the requirements of each stage will pass on to the next evaluation stage.

3.1 EXCLUSION CRITERIA

All tenderers shall provide a 'declaration on their honour' (see Annex III), stating that they are not in one of the situations of exclusion listed.

The 'declaration on honour' is also required for identified subcontractors whose intended share of the contract is above 20%.

The 'declaration on honour' has to be duly signed by parties that are not signing the Tender Preparation Report in *e-Submission*.

The successful tenderer shall be asked to provide the actual documents mentioned as supporting evidence in Annex III before signature of the contract and within a deadline given by the contracting authority. This requirement applies to all members of the consortium in case of joint tender.

Remark:

A tenderer may be waived of the obligation to submit the documentary evidence mentioned above if such evidence has already been submitted for the purposes of another procurement procedure launched by ENISA, provided that the documents are ***not more than one-year-old*** starting from their issuing date and that they are still valid. In such a case, the tenderer shall declare on his/her honour that the documentary evidence has already been provided in a previous procurement procedure, specifying the reference of the call for tender for which the documents have been provided, and confirm that no changes in their situation has occurred.

ENISA will also waive the obligation of the tenderer to submit the documentary evidence if it can access it on a national database free of charge.

Each tenderer (and each member of a consortium) shall declare in the relevant field in Annex VII (Administrative Identification form) whether it is a Small or Medium Size Enterprise (SME) in accordance with Commission Recommendation 2003/361/EC[15].

As a general guideline, here is an excerpt from the Recommendation:

"*The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.*"

3.2 SELECTION CRITERIA

The following criteria will be used to select the Tenderers for further evaluation. If the Tender is proposed by a consortium, these criteria apply to the tenderer as a whole (unless otherwise stated).

Documentary evidence of the Tenderers' claims in respect of the below-mentioned criteria is required.

3.2.1 LEGAL AND REGULATORY CAPACITY

The Tenderer must provide evidence of enrolment (declaration or certificates) in one of the professional or trade registers related to the subject of this tender, in the country of its establishment.

3.2.2 FINANCIAL AND ECONOMIC CAPACITY

Proof of financial and economic standing shall be furnished by the following documents and minimum requirements:

(a) Copy of the financial statements (balance sheets and profit and loss accounts) for the last two (2) financial years for which accounts have been closed, where publication of the accounts is required under the company law of the country in which the economic operator is established. In case of a consortium, each consortium member shall present their financial statements.

If the tenderer is not obliged to publish its accounts under the law of the state in which it is established, a copy of audited accounts for the last two (2) financial years should be presented. In case of a consortium/grouping, audited accounts for each consortium partner shall be presented.

(b) **Complete (also) the attached Annex II 'Simplified Financial Statement',** which summarises your recent financial capacity. Please note that the average turnover for the last two (2) financial years for which accounts have been closed must meet our **minimum annual average turnover** of **€1.000.000 (one million euro)**:

In case of a consortium/grouping, the annual average turnover for each of the partners shall be presented. The sum of the annual average turnovers of each partner will be taken into account to reach the annual average turnover of **€1.000.000**.

[15] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF

(c) If tenderers will call on the competences of another entity (for example, a parent company), a written undertaking by the said entity certifying that it will make available to the tenderers the resources required to implement the contract.

If for some exceptional reason which the Contracting Authority considers justified, the tenderer is unable to provide the documentary evidence requested above, he may prove his economic and financial capacity by any other means which the Contracting Authority considers appropriate, but only following a formal request for clarification **before** the tender expiry date.

3.2.3 TECHNICAL AND PROFESSIONAL CAPACITY CRITERIA AND EVIDENCE

The Tenderers are required to have sufficient technical and professional capacity to perform the contract. Evidence of the technical and professional capacity of the tenderers shall be furnished on the basis of the following requirements:

Support of the service: *Online Training Platform as a Service, including pre-existing training portfolio*.

- The tenderer is expected to be either already be providing such a service or should demonstrate that they are able to develop such a platform, populate it with a pre-existing training portfolio and support it operationally.
- Both pre-existing platforms or newly developed ones (including a pre-existing training portfolio) should be supported according to the requested levels described in Section 2.2 (DETAILED DESCRIPTION OF THE SERVICES) and more specifically Sections 2.2.1to 2.2.4.

Support of the service: *Setup of Training Platform according to ENISA specifications*.

- The tenderer is expected to be able to setup in their pre-existing training platform (or in their newly developed one) an environment that meets the requirements described in Section 2.2 (DETAILED DESCRIPTION OF THE SERVICES) and more specifically subsection 2.2.5, and provides a smooth experience for all enlisted users.

Support of the service: *Training Module Development Services*.

- The tenderer should be able to provide these bespoke training module development services for the main categories of trainings described in Section 2.2 (DETAILED DESCRIPTION OF THE SERVICES).
- The tenderer should be able to make these modules available to ENISA subscribers only and the trainings should be developed in such a way that they meet the requirements for a self-paced training, again as described in more detail in Section 2.2 (DETAILED DESCRIPTION OF THE SERVICES) and more specifically Section 2.2.6.

Support of the service: *Platform Development Services*.

- The tenderer is expected to be either already be providing such a service or should demonstrate that they are able to develop such a platform, populate it with a pre-existing training portfolio and support it operationally.
  Both pre-existing platforms or newly developed ones (including a pre-existing training portfolio) should be supported according to the requested levels described in Section 2.2 (DETAILED DESCRIPTION OF THE SERVICES) and more specifically Section 2.2.7.

Criterion T1: The tenderer must prove experience in developing, offering and supporting an operational Online Training Platform as a Service, including pre-existing training portfolio.

Evidence for T1: The tenderer must provide evidence of either currently offering an existing service that matches the ENISA expectations and they are free to choose the most compelling way to do so.

However, ENISA requires the tenderer to include a clear list of the pre-existing training portfolio that they are currently offering via the aforementioned platform. They must also provide a reference list (including contact details) of minimum three (3) current and/or past customers to whom the tenderer has supplied the core services, in the past five (5) years; specifying the tenderer's share (at least 50%) in provision of the services and if subcontractors were used for any of the services.

In case the tenderer does not currently have an operational platform in place, they must provide evidence that supports their claim that they are capable of developing, exploiting and supporting such a service, including the creation of a portfolio of trainings. They should provide references of similar projects or achievements that support their claims by providing a reference list (including contact details) of minimum three (3) current and/or past customers to whom the tenderer has supplied the services they bring forward as evidence, in the past five (5) years; specifying the tenderer's share (at least 50%) in provision of the services and if subcontractors were used for any of the services.

Criterion T2: The tenderer must prove experience in setting up Training Platforms (including customisations in the area of "look and feel") and in Platform Development Services.

Evidence for T2: The Curricula Vitae (CVs), preferably in a common European format, of the proposed members of the team must be enclosed and showing clearly qualifications, professional experience within the relevant business area (and if applicable the projects they contributed to and their contributions to the projects) with the start and the end date (i.e. from DD.MM.YYYY to DD.MM.YYYY. The form can be downloaded from:
https://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions

Criterion T3: The tenderer must prove experience in development of self-paced online training module development.

Evidence for T3: The Curricula Vitae (CVs), preferably in a common European format, of the proposed members of the team must be enclosed and showing clearly qualifications, professional experience within the relevant business area (and if applicable the projects they contributed to and their contributions to the projects) with the start and the end date (i.e. from DD.MM.YYYY to DD.MM.YYYY. The form can be downloaded from:
https://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions

3.3 AWARD CRITERIA

3.3.1 QUALITY OF THE OFFER

Once the Tenderer has demonstrated the appropriate capacity to perform the Contract on the grounds of the selection criteria, the offer will be assessed based on the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	**Technical compliance with the Core Services**	Compliance of the offer with the technical descriptions of the required service (including requirements on personal data protection and security) and advantageous elements.	40
2.	**Quality and accuracy of content and structure**	Quality of the proposal and accuracy of the description of the implementation and provision of the required services; quality reviews of deliverables.	40
3.	**Internal organisation**	Organisation of the work and resources including: Composition of the project team (ratio senior/juniors), work flows and review cycles of the output, direct involvement of senior staff and distribution of tasks amongst experts;	20
Total Qualitative Points (QP)			**100**

Minimum attainment per criterion and overall

Tenders which do not obtain at least 50% of the maximum score for each award criterion and at least 70% of the overall score for all the criteria will be considered to be of insufficient quality and will not be admitted to the next stage of the evaluation procedure.

The sum of all criteria gives a total of 100 points. The respective weighting between the different awards criteria depends on the nature of the services required and is consequently closely related to the Technical Specifications. The award criteria are thus quantified parameters that the offer should comply with. The qualitative award criteria points will be weighted at 70% in relation to the price.

3.3.2 PRICE OF THE OFFER

The evaluation of Financial Offers is based on the total price (overall total referred in Financial Offer form Annex IV.

The cheapest offer will receive the maximum points and the rest of the candidate's offers will be awarded points in relation to the best offer as follows:

PP = (PC / PB) x 100

where:

PP = Price points
PC = Cheapest bid price received
PB = Bid price being evaluated

3.3.3 AWARD OF THE CONTRACT

The contract will be awarded to the offer that is the most cost effective (offers the best value for money) which obtains the highest number of points after the final evaluation, based on the ratio between the **quality criteria (70%) and the price (30%).** The following formula will be used:

TWP = (QP x 0.7) + (PP x 0.3)

where;

QP = Qualitative points
PP = Price points
TWP = Total weighted points score

In case the successful tenderer is unable to sign the contract for any reason, the Contracting Authority reserves the right to award the contract to other tenderers as per the ranking order established following the evaluation procedure.

4. TENDER OPENING

The public opening of received tenders will take place online on **8th November 2022 at 09:30 CET Central European Time**.

A maximum of one legal representative per participating tenderer may attend the opening session. Tenderers shall inform the Agency in writing of their intention to attend, by email to procurement@enisa.europa.eu **at least 2 working days** prior to the opening session.

Alternatively, please note *that all tenderers may simply request a copy of the Opening Report to be sent to them by email after the conclusion of the Opening Session procedure.*

5. OTHER CONDITIONS

5.1 VALIDITY

Period of validity of the Tender: 90 days from the closing date stated in Invitation to Tender. The successful Tenderer must maintain its Offer for a further 120 days from the notification of the award.

5.2 LOTS

This tender is not divided into lots.

5.3 ADDITIONAL PROVISIONS

- Changes to tenders will be accepted only if they are received on or before the final date and time set for the receipt of tenders.
- Expenses incurred in respect of the preparation and presentation of tenders cannot be refunded.
- No information of any kind will be given on the state of progress with regard to the evaluation of tenders.
- All documents submitted by Tenderers will become the property of ENISA and will be treated as confidential.

5.4 NO OBLIGATION TO AWARD THE CONTRACT

Initiation of a tendering procedure imposes no obligation on the Contracting Authority to award the contract. Should the invitation to tender cover several items or lots, the Contracting Authority reserves the right to award a contract for only some of them. The Contracting Authority shall not be liable for any compensation with respect to Tenderers whose tenders have not been accepted. Nor shall it be so liable if it decides not to award the contract.

6. SPECIFIC INFORMATION

6.1 TIMETABLE

The timetable for this tender and the resulting contracts is as follows:

Title: "**External Cloud based Training Platform Access and Support Services"**

ENISA F-CBU-22-T34

Summary timetable comments

Launch of tender: - Contract notice to the Official Journal of the European Union (OJEU) - Uploaded to e-Tendering website - Uploaded to ENISA website	05/10/2022	
Deadline for request of information to ENISA	03/11/2022	
Last date on which clarifications are issued by ENISA	04/11/2022	
Deadline for **electronic reception** of offers via ***e-Submission***	**07/11/2022**	**18:00 CET** Central European time
Opening of offers	08/11/2022	**09:30 CET** Central European time
Date for evaluation of offers	TBA	
Notification of award to the selected candidate + 10 day standstill period commences	TBA	
Contract signature	End November	Estimated