OPEN CALL FOR TENDERS

Tender Documentation

"Development and maintenance services for the EU cybersecurity index tool"

ENISA F-KIT-22-T15

Part 1 **Introduction to ENISA**

Part 2 **Technical Specifications**

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

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 is actively contributing to European cybersecurity policy, in order to support Member States and European Union stakeholders to support a response to large-scale cyber incidents that take place across borders in cases where two or more EU Member States have been affected. This work also contributes to the proper functioning of the Digital Single Market.

1.2 SCOPE

The Agency shall assist the European Commission and EU Member States (EU MS), and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security, thereby ensuring the smooth functioning of the Internal Market. As described in ENISA regulation, one of the objectives of the agency is to assist the Union institutions, bodies, offices and agencies in developing policies in network and information security, so, including building expertise related to availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems. For instance, the new ENISA regulation mentions the necessity to analyse current and emerging risks (and their components), stating: "*the Agency, in cooperation with Member States and, as appropriate, with statistical bodies and others, collects relevant information*". In particular, under Art. 3, Tasks, d), iii), the new ENISA regulation states that ENISA should enable effective responses to information security risks and threats.

ENISA supports the development and implementation of the European Union's policy and law on matters relating to network and information security (NIS) and assists Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis.

Since 2019, following the bringing into force of the Cybersecurity Act (Regulation 2019/881), ENISA is tasked to prepare the 'European cybersecurity certification schemes' that serve as the basis for certification of products, processes and services that support the delivery of the Digital Single Market. The European Cybersecurity Act introduces processes that support the cybersecurity certification of ICT products, processes and services. In particular, it establishes EU wide rules and European schemes for cybersecurity certification of such ICT products, processes and services.

1.3 OBJECTIVES

The Agency's objectives are as follows:

- The Agency shall enhance the capabilities of the cybersecurity community including EU Member States to prevent, to address, and to respond to cybersecurity issues and threats.
- The Agency shall provide assistance and deliver advice to the Commission and EU MS on issues related to cybersecurity falling within its competencies as set out in the Regulation.
- Building on national and EU efforts, the Agency shall develop a high level of expertise.
- The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors.
- The Agency shall assist the Commission, in the technical preparatory work for updating and developing EU legislation in the field of cybersecurity.

2. ADDITIONAL INFORMATION

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

PART 2 TECHNICAL SPECIFICATIONS

I. SCOPE OF THIS TENDER

ENISA is seeking a suitably qualified contractor to provide software development and maintenance services for the EU Cybersecurity Index tool as stipulated in the Technical Specification outlined in Sections 1-3 below. The required services may also cover aspects related to the operational support of the cybersecurity index, including application data management, user support and data analytics.

The EU cybersecurity index tool will allow the collection, processing and display of data related to various cybersecurity metrics related to the EU Member States. The services in scope of this tender will involve both the development but also maintenance and administration of the application in accordance with arising needs and new requirements.

Deployment of all production and test environments will be on the Azure cloud computing platform but tenderers are free to propose the technologies on which the EU cybersecurity index tool will be developed. Given the nature of ENISA's work and focus on cybersecurity, the security of the tool is crucial and so security should receive maximum attention.

Subject of the tender	Maximum budget
Development and maintenance services for the EU cybersecurity index tool	A maximum budget of **€1.000.000,00 (one million euro)** over the maximum possible period of 4 years.
Last date and time for dispatch of offers	**28th March 2022 until 18:00 CET**

PLEASE NOTE: *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.

[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. BACKGROUND INFORMATION

The website and portal servers are built using the following technologies:

The European Union expressed the need for a high common level of security of the collaborative cyberspace, in which the Union, its Member States (MS) and allies operate, in its 2020 Cyber Security Strategy.[2] The European Union Agency for Cybersecurity (ENISA) is mandated and tasked by the EU's Cybersecurity Act [3] to actively support the MS and Union in their efforts to build and enhance capabilities and preparedness to prevent, detect and respond to cyber threats and incidents in Network and Information Systems (NIS). NIS and electronic communications networks and services play a vital role in society, are key to critical (information) infrastructures and services (CI/CII) and have become the backbone of economic growth.

To support the EU as a whole in making informed decisions on identified challenges and gaps in cybersecurity, insights on the cybersecurity maturity and posture of the Union and Member State's policies, capabilities and operations are required. A European Cybersecurity Index may provide this insight by:

- assessing the current level of maturity of cybersecurity and relevant cyber capabilities,
- identifying opportunities for collaborative and local cybersecurity enhancements,
- identifying areas of network and information system security weaknesses which may provide a risk to the Union and its MS as well as its citizens, governmental structures, CI/CII and digital services, and small, medium, and large enterprises.

The insights may highlight gaps within policies and intended levels of maturity. To remedy these, actions can be drafted by MS and the European Commission (EC) to improve individual and collaborative policies, capacities and capabilities.

Therefore, as part of its Single Programming Document 2022-2024 [4] set of activities, ENISA intends to develop and maintain a European Cybersecurity Index (Output 8.1) which should reflect the maturity and posture of cybersecurity at the MS and Union levels.

In 2021, a project started to provide the basis for building an effective cybersecurity index for the Union and its MS. Among the deliverables of this project are two documents of relevance to the present tender:

- *Draft framework for a composite cybersecurity index*, which outlines the key metrics, areas, domains, indicators, data sources, weights etc. comprising the index
- *Design and specifications to tools to support the framework for a composite cybersecurity index*, which includes the draft design for tools to support the implementation of the draft framework for the index

Both documents will be made available to the successful contractor in the course of the 2022 project to be launched under the ensuing framework contract.

---

[2] European Commission: Communication on the EU Security Strategy COM(2020) 605 final, Brussels, Belgium (2019). https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf

[3] European Commission: Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation, Brussels, Belgium (2019)

[4] ENISA, ENISA Single Programming Document 2021-2023, ENISA, Heraklion, Greece, 2021. https://doi.org/10.2824/325038.

2. PROJECTS FORESEEN FOR 2022

Without this being binding, ENISA envisages to deal with the following project related to the development and maintenance of tools to support the EU cybersecurity index:

a) Development of EU cybersecurity index tool

An estimation of the budget available for this project for 2022 is up to €170.000,00. The specific request for this service will be launched immediately after the conclusion of this tender procedure upon signature of contract with the selected contractor.

This project will involve the development of the back-end and front-end (multiple views of the index data based on roles and assorted access privileges) of the index tool and the interfaces to facilitate the input of data, including manual input and web service APIs.

3. DESCRIPTION OF TASKS AND SERVICES TO BE PROVIDED

The foreseen services to be provided intend to cover the full lifecycle of development and maintenance of tools to support the implementation and operation of the EU cybersecurity index. Requests for these services may involve one-off projects, such as software development projects to deliver parts of the index tool, or continuous services such as user support and application data management to be provided over a defined time period.

The following list includes the different services ENISA may request over the course of the contract though ENISA is not bound to request all of the listed services. The tenderer shall demonstrate sufficient expertise to provide all of the services listed below.

3.1 SOFTWARE DEVELOPMENT PROJECTS

The successful contractor will need to deliver software development projects related to the development and deployment of back-end and front-end components of the EU cybersecurity index tool.

During each project initiation, the contractor will be asked to provide a detailed project plan together with a relevant timeline of the project flow (e.g. Gantt chart) and key milestones that will be agreed with ENISA. Project management methodology (i.e. waterfall or agile methodology) should be the point of reference for all major web development projects. The methodology to be used in each project will be defined by the project manager of ENISA and the contractor should be able to follow either methodology.

Specific activities that the contractor will be expected to carry out for software development projects include:

- **Requirements collection**: ENISA will typically provide the functional and/or technical requirements for any new software development project. However, the contractor may be requested to support with the collection and analysis of requirements from relevant stakeholders (e.g. EU Member State representatives) or assist with the further elaboration of functional and/or technical requirements.
- **Functional/technical design**: The contractor is expected to produce technical and functional specifications for software development projects that incorporate the provided requirements. Particular emphasis is placed on the design of the front-end (e.g. design of mock-ups) in order to optimise user experience for different types of users of the index tool and for which the contractor

will be expected to follow state-of-the-art practices and propose modern and user-friendly navigation concepts.

- **Software development:** Development of the different software components of the EU cybersecurity index tool should comply with state-of-the-art practices and methodologies, be supported by appropriate tools (e.g. for collaboration, source code management/software versioning etc.) and follow a security-by-design approach.
- **Testing:** The contractor should integrate appropriate testing in all phases of development, e.g. including functional testing, load testing, security testing[5], browser compatibility testing, FAT etc. User acceptance tests should typically be developed for all software development projects.
- **Documentation**: The contractor should be able to draft documentation for different types of users and administrators of the system. The documentation may be requested in different formats (e.g. manuals/documents, FAQs, website content, graphics) and should be drafted in a language suitable for each target audience. Suitable documentation (e.g. release notes) should also accompany new software releases/updates.
- **Deployment:** The contractor may also be requested to provide services related to the migration of a software product from testing to production, including designing and implementing roll-back procedures if necessary.

In parallel, ENISA will make sure to provide crucial deliverables, feedback, and other necessary information on time for the delivery of web development projects/tasks or to inform the service provider in case of delays.

3.2 SECURITY

Given the nature of the agency's work/focus, it is of paramount importance that ENISA's environment, including applications developed and managed by the Agency, remains as secure as possible at all times. Security mechanisms, secure functions and security good practices in both coding, configurations and connections shall be utilised to ensure application level security. Corresponding safeguards, e.g. SSL certificates, ISO27001 compliance, etc. shall be considered an advantage. Indicatively, the contractor may be expected to:

- Follow security by design practices in developing software and establishing baseline/default system and application configurations.
- Implement appropriate access control mechanisms both in the context of software development but also in relation to the tool's operation. With respect to the latter, depending on the use role different access and authentication mechanisms could be foreseen (e.g. MFA, access via EULogin etc.)
- Comply with security policies or standards determined by ENISA. This may involve for instance compliance of software components and/or workflows with ENISA's own security policies or standards or compliance with industry standards such as ISO 27001.
- Develop and document an information security policy for the EU cybersecurity index tool, taking

[5] Aside from any penetration testing / security testing conducted independently by ENISA on any developed software.

into consideration ENISA's security policy.

- Design and implement a Disaster Recovery framework for the EU cybersecurity index tool, including backup and restore procedures. Backup and recovery time objective requirements will be defined by ENISA and the contractor may be requested to test and/or manage the backup / restore procedure.

3.3 MAINTENANCE

The contractor may be requested to provide services related to ensuring that the operation of the EU cybersecurity index tool remains functional, stable and secure. These may include:

- **Evolutive maintenance** involving the incremental evolution of the tool through the development of new modules, interfaces etc., addition and/or modification of indicators, improvements to the user interfaces etc.
- **Corrective maintenance** involving identifying, analysing and resolving issues and problems or defects of the tool. The contractor may be requested to provide regular or ad hoc reports on resolved issues and maintain a registry of open/unresolved issues.
- **Security patching / hardening** involving activities required to maintain an acceptable level of application/software security, to support security reviews and testing and to recommend, agree and implement security patching on the tool. This also includes following-up and resolving findings / vulnerabilities following penetration tests and maintaining secure system configuration.

3.4 ADMINISTRATION

The contractor may be requested to provide services related to supporting the system and application administration. These may include:

- **System administration** including for instance system administration, system health monitoring, system maintenance, data backup etc.
- **User management** including management of user profiles, assigning roles/privileges, periodic review of access rights etc.
- **User support** including first and/or second level support for users of the application. In case first level support is required, the contractor may be requested to provide multichannel help desk services (e.g. phone, functional mailbox, ticketing system, self-service FAQ pages etc.).
- **Application data management** may involve services related to validation, sanitisation and cleaning of application data. Application data will be provided by privileged users representing EU Member States and will relate to the various indicators; requirements for the management of this data will depend on the data validation workflows to be defined for the tool and may involve handling missing data, fixing syntax/structural errors, validating data, quality assurance, following up with users submitting data etc.

3.5 DATA ANALYTICS

The EU cybersecurity index tool will store data related to a plethora of indicators for all EU Member States, collected over multiple years. The contractor should be able to provide data analytics services that will allow for the identification of patterns and correlations in the dataset and identify areas for

improvement of the cybersecurity index framework (e.g. through the identification of indicators that can be optimised or modified).

4. DESCRIPTION OF PROFILES

Tenderers shall provide the following requested profiles for the requested services. Tenderers shall provide the CVs of at least the minimum number indicated in the table at the end of section 4, but are also encouraged to provide as many experts as deemed relevant and experienced in the fields related to the subject matter of this tender procedure.

4.1 PROJECT MANGER PROFILE

The **Project Manager** shall have:

- Minimum 4 years' experience in IT Project Management. Practical experience with software development life-cycle or auditing.
- A level of education which corresponds to completed university studies of at least four (4) years attested by a diploma
- Proven experience in project management including proposals for project strategies, planning, definition of tasks and deliverables, review of project deliverables, quality control, risk analysis and management, project status reports, problem reporting and management systems, follow up and organisation.
- Proven experience with quality procedures.
- Project management skills and experience as team leader;
- Excellent drafting skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Proficient in both written and spoken English

Advantageous:

- Certifications in project management (e.g. PRINCE2) and/or service management (e.g. ITIL)
- Professional experience in Cybersecurity
- Hands on experience on DevOps and/or Continuous Integration (CI), Continuous Delivery (CD) and continuous testing tools
- Experience in projects for EU Institutions Agencies and Bodies

4.2 BUSINESS ANALYST PROFILE

The **Business Analyst** shall have:

- A level of education which corresponds to completed university studies of at least four (4) years attested by a diploma in one of the following fields: Computer Science, Information Technologies, Mathematics, Physics, Engineering, Business Administration, Business Management or related areas.
- A minimum of four (4) years of experience in Information Technology development and/or

Information Technology consulting.

- Experience with business process analysis, documentation, and change management
- Experience in analysis and programming, databases and web application development.
- Experience creating detailed project documentation and reporting
- Excellent communication and presentation skills.
- Proficient in both written and spoken English

Advantageous:

- Knowledge of international standards like W3C and WAI
- Professional experience in Cybersecurity
- Experience in working with and analysing composite indexes, indicators and KPIs

4.3 DEVELOPER PROFILE

The **Developer** shall have:

- University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and software development technologies.
- Hands-on Development/maintenance experience of web-enabled applications.
- Experience on development of front-end and back-end systems including database development tasks[6]
- The ability to cooperate with ENISA and UI/UX designers to match visual design intent.
- The ability of increasing program operating efficiency and adapt system to new requirements, as necessary.
- The ability of report status and flag issues to the ENISA Project/Product Manager.
- Experience with version control systems and source code management system for software development, git (preferred) or svn.
- Experience with secure software development practices
- Strong interest in follow-up of trends in web development.
- Written and oral English at European language level B2 or better

Advantageous:

- Knowledge of international standards like W3C and WAI
- Professional experience in Cybersecurity
- Experience in working with and analysing composite indexes, indicators and KPIs

[6] The tenderer may propose developer profiles specialised in either back-end or front-end/UI development

- Excellent drafting skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Proficient in both written and spoken English
- Experience working in an Agile/Scrum development process
- Hands on experience on DevOps and/or Continuous Integration (CI), Continuous Delivery (CD) and continuous testing tools

4.4 QUALITY AUSSURANCE/DevOps/TESTER PROFILE

The **Quality assurance/devops/tester** shall have:

- University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and software development technologies
- Hands on experience on DevOps and/or Continuous Integration (CI), Continuous Delivery (CD) and continuous testing tools
- Experience working in an Agile/Scrum development process
- Analysis, design, planning and execution of a test strategy for new features and sustaining projects.
- Developing and executing automated tests to enable delivery of high-quality software on time and on budget.
- Performing functional and non-functional tests in order to ensure the quality and the proper goal of the end product / feature.
- Implement test tools and utilities to improve the efficiency and effectiveness of the development life-cycle
- Configuration and maintenance of a test lab environment that resembles complex customer environments
- File detailed bug reports and follow up on the problems until complete resolution
- Comply with good engineering practices, coding standards and contribute to automation code reviews
- Collaboration with development team to assure correct replication, integration and deployment on production.
- Experience with a Test Automation Frameworks (e.g. Selenium, QTP, Sikuli)
- Experience with QA methodologies
- Great understanding of testing throughout the product lifecycle, including unit, integration, regression, component and end-to-end system testing
- Familiarity with SSH, and one of the following deployment automation tools (Jira/Bamboo, Jira/Zephyr, Chef, Puppet, Maven, Jenkins, Kubernetes, Capistrano etc.)
- Strong scripting programming knowledge (e.g. Shell/Ruby/Python)

- Experience with version control systems and source code management system for software development, git (preferred) or svn.

Advantageous:

- Certification in software testing (e.g. ISTQB)
- Experience in security testing
- Professional experience in Cybersecurity
- Experience in working with and analysing composite indexes, indicators and KPIs

4.5 SYSTEM ADMINISTRATOR PROFILE

The **System Administrator** shall have:

- University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and system administration.
- Hands-on experience in web-enabled applications administration.
- Experience in network administration and OS support.
- Experience in first and second level user support and/or help desk services
- Experience in user account management
- Experience in application data management, including data sanitisation, cleaning and quality control
- Experience in drafting user support documentation
- Proficient in both written and spoken English

Advantageous:

- Certification in service management (e.g. ITIL)
- Experience in working with EU Institutions, Agencies and Bodies

4.6 DATA SCIENTIST PROFILE

The **Data Scientist** shall have:

- PhD or MSc in a relative area of data processing, data management, data analytics, data science, information science.
- Excellent knowledge in statistics (preferably validated by relative studies)
- Excellent knowledge of at least one programming language (e.g. Python, R)
- At least 3 years of experience in data extraction, transformation, data wrangling and data exploration

- Excellent knowledge of Big Data Processing Frameworks
- Excellent knowledge on Data Visualization

Advantageous:

- Professional experience in Cybersecurity
- Experience running research projects and teams, as well as research collaborations
- Experience using Machine Learning algorithms.

The **minimum** number of CVs requested per profile is presented below:

ID	Profile	
1	Project Manager	2 CVs
2	Business Analyst	1 CV
3	Developer	5 CVs
4	Quality Assurance/ DevOps /Tester	2 CVs
5	System Administrator	2 CVs
6	Data Scientist	2 CVs

In case of the departure of one or more members of the proposed team, the contractor is expected to provide ENISA with CVs of replacements with at least the same level of qualifications and similar experience to cover ENISA's needs. ENISA will evaluate the CV and experience in order to decide within 5 working days, whether to accept, or reject and request an alternate replacement candidate.

5. PLACE OF WORK AND DELIVERY

The implementation of the services will be undertaken at the contractor's premises.

One face-to-face kick off meeting between ENISA and the contractor might be held at ENISA's premises in Athens depending on the restrictions imposed by the current ongoing COVID-19 pandemic. If a face-to-face meeting is not possible, the first and all other meetings between ENISA and the contractor can be made by using video conference systems, telephone or e-mail.

6. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

6.1 STRUCTURE OF THE TECHNICAL OFFER

The Tenderer should submit a **Technical Offer** containing relevant documents and information which enables ENISA to assess its quality and compliance with the specifications above (the technical description).

The technical offer shall be structured as follows:

- **Section 1: Methodology and work plan for the provision of the required services**
    - For each of the foreseen types of services, the Tenderer will have to present the proposed methodologies, frameworks, tools etc. to be used for their delivery.
    - The tenderer shall provide a high level overview of the organisation of the work for the delivery of the required services, including any specific interfaces with the ENISA project team.
- **Section 2: Framework contract organisation to deliver the required services**
    - Description of relevant **roles/responsibilities** within the proposed framework contract management team
    - Description of **tasks/activities** to be undertaken by each team member and foreseen allocation of resources to the global management of the framework contract.
    - Provisions for **continuity of service** in case of absence of a member of a project team.
    - 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 quality assurance methods to be used in relation to these tasks.
- **Section 3: Project Management and Quality Assurance**
    - The approach and methodology for the **project management of the specific projects**.
    - The approach and methodology for the **quality assurance** of specific project deliverables.
    - Specific methodologies to be followed for the delivery of the required services (e.g. software development methodologies followed by the contractor).
    - The foreseen **project risks** and how are going to be mitigated.
- **Section 4: Project scenario – "Development of EU Cybersecurity Index Tool'.**
    - As per section 6.2 - Scenario – 'Development of EU Cybersecurity Index Tool'

The Technical Offer shall consist of **20 pages maximum**, including **up to 10 pages for sections 1-3** and **up to 10 pages for section 4**. **Pages over the limit shall not be considered for evaluation**. Any detailed CVs of proposed team members shall be submitted separately or in Annex. The Tenderer is encouraged to provide specific details for each section of the offer; simply repeating the tender requirements will result in a low score.

6.2 SCENARIO – DEVELOPMENT OF EU CYBERSECURITY INDEX TOOL

This scenario will form the basis of the first specific contract to be awarded concurrently with the signature of the framework contract with the successful tenderer. It is therefore important that you provide a detailed and compliant technical and financial offer for this scenario.

The objective of this project is to develop and deploy into production the first version of the EU Cybersecurity Index Tool.

The foreseen start date for the project is 7 days after signature of the framework contract, estimated around the end of April, and the foreseen project end date is October 25th.

The maximum estimated budget assigned for this project is **one hundred and seventy thousand Euros (€170,000.00**), however this does not mean your scenario budget shall necessarily meet this figure. You are free to propose an amount which is supported with a sound technical offer which fully meets the minimum technical requirements as detailed below. The breakdown of costs between the 'profiles' in Section 4 above shall be provided in Section C) of the Financial Offer form (Annex III).

The requirements for the tool are outlined in two documents that will be made available at the start of the project:

- *Draft framework for a composite cybersecurity index*, which outlines the key metrics, areas, domains, indicators, data sources, weights etc. comprising the index
- *Design and specifications to tools to support the framework for a composite cybersecurity index*, which includes the draft design for tools to support the implementation of the draft framework for the index

However, ENISA foresees a period of consultation with stakeholders to validate the feasibility of the framework. This consultation period will finish by mid-July 2022 and may result in changes in some of the indicators (including weight of indicators, calculation formula, source/provider of data etc.).

The index consists of 4 areas, divided in 29 sub-domains and 64 indicators in total. Data for these indicators will be provided by primarily by authorised users from each EU Member State but 6 web service APIs will also need to be developed to get data automatically from various sources (e.g. The Digital Economy and Society Index - DESI[7]). Four main user groups with different access rights and privileges are foreseen. Workflows are foreseen to approve new data input for the indicators, to send out reminders for missing data and to calculate the index based on existing indicator values.

The tenderer shall provide a technical offer for the delivery of the project based on these high-level requirements. The offer should include the following:

- A project plan, including a Gantt chart with key milestones and identified dependencies for the delivery of the project
- Identified project risks and a description of the respective risk mitigation approach
- Composition of project team including roles and responsibilities as well as the foreseen allocation of man-days per profile to project activities. **The total number of person-days per profile for the project should be consistent with the man-days stated in the financial offer**.
- A description of the project management, software development and quality assurance methodologies selected for the project
- A description of the technologies / software proposed to be used for the delivery of the project. The testing and production environment itself will be based on the Azure cloud computing

[7] https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020

platform. Costs associated with Azure licenses and required software for the test and production environments will be covered by ENISA.

- A proposal for the visualisation of the index

7. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

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

All three sections (A. B and C) must be fully completed in order for the financial offer to be considered compliant.

Prices must be quoted in **EURO** and include all expenses necessary to perform the contract.

8. TENDER RESULT AND ESTIMATED CONTRACT VALUE

The estimated overall maximum contract value without this being binding for ENISA is **one million Euros (€1,000,000.00)** over a maximum possible period of 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 Article 164(4) and Annex I - point 11.1(e) of the EU Financial Regulation (FR)).

9. DATA PROTECTION

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[8] ('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 IV.

- **Regulation (EU) 2016/679[9] (General Data Protection Regulation – 'the GDPR')** as concerns personal data processing carried out by the contractor on its proper behalf as a controller.

[8] 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

[9] 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

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 IV. 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:

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 abide in particular by ENISA's data protection policies as regards the confidentiality of electronic communications (Section 3 EDPR) and the processing of personal data in web services;
- 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)[10], 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:

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

- 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 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 IV 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.

10. OWNERSHIP, INTELLECTUAL PROPERTY RIGHTS, USE OF RESULTS

As regards any product or delivery commissioned by ENISA and developed by the contractor in the context of the contract resulting from this call for tenders, as well as source codes of IT applications and models developed for ENISA, the intellectual property rights will be owned by ENISA only in its capacity as financial source of the contract. The contractor cannot file a trademark; patent, copyright or other IPR protection scheme in relation to any of the results or rights obtained by ENISA in performance of the contract, unless the contractor requests the ENISA ex-ante authorisation and obtains from ENISA a written consent in this regard.

ENISA does not acquire ownership or any license of pre-existing rights not incorporated in the deliverables. The full ownership is limited to the deliverables, which might include licensed pre-existing rights on excerpts, parts, texts etc., if fully or partially incorporated in the final deliverables.

The draft contract in Annex IV contains further provisions on ownership of intellectual property rights. All quotations or information the tenderer provides in the technical and financial offer for this tender, which originates from other sources to which third parties may claim rights, have to be clearly marked in the offer in a way allowing easy identification (source publications, including date & place, creator, number, full title etc.). The tenderer shall take account of the above specification on ownership and copyrights in their technical and financial offer.

11. 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.

12. 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.

13. 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

14. 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.

15. 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.

16. 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.

17. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out within 60 days of submission of an invoice accompanying the final report or deliverable based on the conditions set out in the draft contract. One single payment will be made after receipt and approval of the deliverables by ENISA. An invoice must specify the specific deliverables covered. A note that accompanies the final deliverables must present the resources used for each of the deliverables presented. Time sheets should be submitted as appropriate.

18. 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 yearly 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 IV).

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[11] 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.

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[12], all tenders must provide information and supporting documentation in two sections:

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

[12] *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*

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.

(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[13].

- 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

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;

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

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[14].

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.*"

[14] 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

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 must be fulfilled by each partner (unless otherwise stated).

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

3.2.1 PROFESSIONAL INFORMATION

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) A statement of the average turnover of the last two (2) financial years for which accounts have been closed. The **minimum annual <u>average</u> turnover** of the tenderer shall be **€250.000,00 (two hundred and fifty thousand 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 250.000,00 EUR.

(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 **<u>before</u>** the tender expiry date.

3.2.3 TECHNICAL AND PROFESSIONAL CAPACITY CRITERIA AND EVIDENCE

These criteria relate to the Tenderer's or subcontractor's skill, efficiency, experience, reliability and similar circumstances. Tenderers are required to prove that they have sufficient technical and professional capacity to perform the contract by providing the following documentation:

a) Criteria relating to tenderers

Tenderers (in case of a joint tender the combined capacity of all tenderers and identified subcontractors) must comply with the following criteria:

- The tenderer must prove its experience related with the areas of expertise listed in Part 2 section 3 with **at least two (2) projects/**deliverables delivered in this field within the last three years, each with a **minimum value of € 80,000.00**. The project references should include at least the development of **one multilingual web-based tool**.
- The tenderer must prove experience of working and drafting reports in the English language with at least three (3) projects delivered in this field in the last five years, showing the necessary language coverage.
- The tenderer must prove its experience of working in EU countries with at least 2 projects delivered in the last three years.
- The tenderer must prove experience in all services listed in Part 2, section 3.

Please note that your list of previous projects in the fields of expertise mentioned above can be from a wide cross-section of organisations including private industry, commercial enterprises and academia as well as with public or governmental organisations.

b) Criteria relating to the team delivering the service:

The team delivering the services should include, as a minimum, the following profiles:

- **Project Manager** (2 CVs)
- **Business Analyst** (1 CV)
- **Developer** (5 CVs)
- **Quality Assurance/ DevOps /Tester** (2 CVs)
- **System Administrator** (2 CVs)
- **Data Scientist** (2 CVs)

c) Evidence:

The following evidence should be provided to fulfil the above criteria:

- Details of the structure of the organisation
- List of **related** services provided in the past five years, with **provable evidence**.
- The educational and professional qualifications of the experts who will provide the services for this tender (CVs), including the management staff. Each CV provided should indicate their intended function in the delivery of the services.

3.3 COMPLIANCE WITH TENDER SPECIFICATION AND MINIMUM REQUIREMENTS

Your offer will be assessed for compliance with the tender specifications prior to its assessment against the award criteria.

Tenders do not comply with the tender specifications and will be rejected if they:

- do not comply with minimum requirements laid down in the tender specifications;
- propose an alternative solution from the one imposed;
- propose a price above the fixed maximum set in the specifications;
- are submitted as variants, when the specifications do not authorise them;
- do not comply with applicable obligations under environmental, social and labour law established by Union law, national law and collective agreements or by the international environmental, social and labour law provisions listed in Annex X to Directive 2014/24/EU9 and compliance with data protection obligations resulting from Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

These grounds for rejection are assessed before the award criteria stage, so in the case of non-compliance, this tender will not be evaluated. The tenderer will thus be informed of the grounds for rejection without being entitled to receive feedback on aspects of the tender other than on the non-compliant elements.

3.4 AWARD CRITERIA

3.4.1 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.	**Quality and relevance of methodology and work plan for the provision of the specific services**	This criterion assesses the suitability and strength of the proposal as measured against the requirements of the illustrative tasks in terms of the technical content.	30
2.	**Quality and adequacy of organization to deliver the proposed services**	This criterion will assess the quality and adequacy, completeness and suitability of proposed organization and applied processes to fulfil tasks, including allocation of tasks, roles and responsibilities and coordination among team members and of the economic operators (in case of joint tenders, including subcontractors if applicable). It also assesses the global allocation of time and resources to the global management of the framework contract.	20
3.	**Project management and quality assurance**	This criterion will assess the quality control system applied to the management of the framework contract concerning the quality of the deliverables, the project management approach for the specific contracts and the suitability of the methodologies followed by the tenderer to deliver the required services. It should be noted that submitting a generic quality control system would result in a low score.	20
4	**Project Scenario**	Compliance with the requirements set out in the scenario description. Quality of the proposal and accuracy of the description to provide the requested services.	30
Total Qualitative Points (QP)			**100**

Tenderers shall elaborate in the technical offer on all points addressed in the technical specifications, bearing also in mind the above indicated award criteria, in order to score as many points against the quality award criteria as possible. The mere repetition of mandatory requirements set out in the technical

specifications, without going into detail or without giving any benefit in the technical offer, would be insufficient.

Minimum attainment per criterion

Offers scoring less than 50% for any criterion will be deemed to be of insufficient quality and eliminated from further consideration.

Minimum attainment overall

Offers scoring **less than 60/100** overall, after the quality award criteria evaluation phase will be considered to be of insufficient quality and eliminated from the following phase.

The sum of all quality criteria gives a total of 100 points. The respective weighting between the different award 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.

3.4.2 PRICE OF THE OFFER

Tenderers must provide prices (in Euro) in **each** blank box as shown in Annex IV – 'Financial Offer form' – failure to provide a price in each box may lead to exclusion of your offer.

The total bid price ratio '**P_B**' will be calculated using the following formula and weightings:

$$P_B = [(P_{DC} / P_D) \times 150)] + [(P_{SC} / P_S)] + [(P_M / P_{MC}) \times 12]$$

where:

P_D = Profiles consolidated daily cost (P_1 +P_2 + P_3 + P_4 + P_5 + P_6)

P_{DC} = Cheapest P_D

P_M = Maintenance services monthly cost

P_{MC} = Cheapest P_M

P_S = Scenario cost

P_{SC} = Cheapest P_S

Please note: If any price box is left blank by the tenderer then the Financial Offer may be considered to be invalid and will be eliminated from further evaluation.

3.4.3 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 = (Q_P x 0.7) + (P_P x 0.3)

where;

Q_P =	Qualitative points
P_P =	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 on **29th March 2022 at 10:30 EET Eastern European Time (Greek local time)** at ENISA Athens office, 14 Agamemnonos Street, Chalandri 151 31 Attiki, Greece.

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: "**Development and maintenance services for the EU cybersecurity index tool"**

ENISA F-KIT-22-T15

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	22nd February 2022	
Deadline for request of information to ENISA	21st March 2022	
Last date on which clarifications are issued by ENISA	22nd March 2022	
Deadline for **electronic reception** of offers via ***e-Submission***	**28th March 2022**	**18:00 CET** Central European time
Opening of offers	29th March 2022	**10:30 EET** Eastern European **(Greek local)** Time
Date for evaluation of offers	TBA	TBA
Notification of award to the selected candidate + 10 day standstill period commences	TBA	Estimated
Contract signature	TBA	Estimated