OPEN CALL FOR TENDERS

*concludes with **Framework service contracts in cascade***

Tender Documentation

Supporting ENISA for the provision of cybersecurity services under the Cybersecurity Support Action

ENISA F-OCU-22-T31

LOT 28 – Supporting ENISA for the provision of cybersecurity services EU wide

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(b)	Financial Offer form (Lot 28 only)
Annex V(b)	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 contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with European Union 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 European Union 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 European Union 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 European Union 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 European Union 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 European Union 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

ENISA is tasked to roll-out the *implementation of the Cybersecurity Support Action in 2022* that includes the provision of support to European Union Member States to further mitigate the risks of large-scale cybersecurity incidents in the short term. In this context, ENISA, in accordance with its mandate, in particular Article 6 and Article 7 of the Cybersecurity Act (881/2019), will provide (on request) support services to the European Union Member States.

The purpose of this Call for Tenders is to provide support to ENISA in the implementation of the aforementioned task and specifically in the delivery of cyber security services to increase support for preparedness (ex-ante), and response (ex-post) cyber security services in the Union. 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.

ENISA will establish framework contracts using the cascading system with multiple economic operators, in order to ensure proper coverage of a fluctuating workload in the areas covered by this call for tenders, while maintaining high quality outputs. A maximum number of three framework contracts in cascade per Lot, will be awarded. A more detailed description of the cascade system can be found in Section 17.

This call for tenders is divided into 28 Lots. Tenders may be submitted for one or several lots. Each lot will be evaluated independently of any other Lot. Tenders which cover only part of one lot or are declared as being conditional on the award of any other Lot are not permitted. If a tenderer decides to apply for more than one Lot, it must submit a separate set of technical and financial offers for each Lot.

Each lot constitutes an individual framework contract to be awarded separately. If several lots are awarded to the same tenderer, a single contract covering all the awarded Lots will be signed.

Subject of the tender	Maximum budget
LOT 28 - Supporting ENISA for the provision of cybersecurity services EU wide (territory of the Member States of the European Union)	A maximum budget of **€ 4.000.000 (four million Euro)** over the maximum possible period of **3 years**
Last date for dispatch of offers	**3rd October 2022 until 18:00 CEST**
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 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

To support the implementation of its programme under the "Implementation of the Cybersecurity Support Action in 2022", ENISA aims to reinforce its capacity and capabilities by concluding framework contracts in cascade with economic operators specialized in the cybersecurity domain. ENISA has defined a list of services to be provided to European Union Member States under its task. This List includes both ex-ante and ex-post services.

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 help aforementioned entities to respond to an actual incident.

LOT 28 lays down the provisions for the performance of defined services (namely external support for different specific needs by means of intra or extra-muros service providers).

The contracting authority will request on a case-by-case basis, the exact profile(s) and services to be executed under specific contracts.

2. DESCRIPTION OF SERVICES TO BE PROVIDED

2.1 SUMMARY OF SERVICES

ENISA will make available to the European Union Member States the following indicative subset of services. The services are offered either as remote or on-site depending on the request.

The table below provides an overview of the services that ENISA may request support from the prospective contractor under this framework contract. A detailed description of each of the services is provided in section 2.2 of this Tender Documentation. The chosen contractor will be expected to provide these services to any EU Member State.

Service	Type	Description
Support for cybersecurity exercises and capability assessment	Ex-Ante	• Development of testing scenarios for MS[3] cybersecurity infrastructure (including infrastructure of Operators of Essential Services, Digital Service Providers and Governmental entities) • Provide support of executing these testing scenarios • Conducting cybersecurity exercises,

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

[3] European Union Member States

		• Evaluation and/or testing of MS cybersecurity capabilities (including capabilities to prevent, detect and respond to incidents) • Evaluation of the cybersecurity maturity of MS • Providing advice on how to improve infrastructure and capabilities.
Technical help with Incident management	Ex-Post	• Information Security Incident Analysis • Artefact and Forensic Evidence Analysis • Information Security Incident Coordination
Assistance with threat assessment	Ex-Ante	• Threat Assessment process implementation/ life cycle • Specific Threat Assessment • Threat landscape

Under this Lot ENISA intends to procure additional support from a contractor to support the provision of the listed services based on its needs.

If necessary the prospective contractor should be able to provide support for additional related services covered by the CSIRT Services Framework[4] and falling within the ENISA legal mandate[5].

2.2 DETAILED DESCRIPTION OF SERVICES

SUPPORT FOR CYBERSECURITY EXERCISES AND CAPABILITY ASSESSMENT

- Support in the development of testing scenarios for MS cybersecurity infrastructure (including infrastructure of Operators of Essential Services, Digital Service Providers and Governmental entities) and support the execution of these testing scenarios:
    - The contractor must be able to support ENISA to develop testing scenarios and support the execution of these scenarios.
    - The contractor must be able to, through on demand services, support ENISA to do a penetration test taking into account these scenarios.
    - The contractor must comply with applicable international standards and best practices in conducting penetration testing.
    - Penetration tests should be able cover Network, Virtualization solutions, Cloud solutions, Industrial Control systems, IoT[6] (including applications, software, middleware and hardware testing).

[4] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

[5] EUR-Lex - 32019R0881 - EN - EUR-Lex (europa.eu)

[6] https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy

- The contractor should be able to perform penetration tests within an Operational Technology (OT) environment (e.g. ICS, SCADA environment)
- The contractor should be able to conduct White, Grey or Black-box type Penetration tests.
- The contractor must be able to provide threat hunting services[7].
- The contractor should be able to deliver comprehensive report including Summary, Objective, Scope, Methodology, Findings, Recommendations and Remediation guidelines.
- The contractor should be able to deliver intermediate reports and presentations as required.

- Conducting exercises
  - Support ENISA in developing an exercise kit portfolio. This kit portfolio will support and facilitate the execution of exercises requested by the European Union Member States. Together with ENISA and based on MS needs, the contractor must be able to develop and maintain an up-to-date exercise portfolio, in line with the ENISA Capacity Building strategies for Trainings and Exercises and of course the European Union Member Sates' needs. The exercise programme should cover critical sectors (including NISD, and NISD2), government and generic infrastructures, threats tied to the current geopolitical situation and consider cross-sectorial, national and cross-border cases.
  - Created exercise kits (output) should adhere to the "ISO 22398:2013: societal security — guidelines for exercises" standard, ENISA best practices, as well as respect individual European Union Member States' guidelines. These specific cases can also be covered by case-driven changes as the kits should be fit for purpose by all European Union Member States.
  - Exercise Kits should cover both Discussion-based and Operational-based exercise methods.
  - Kits will be stand alone, ready to allow the execution of realistic exercises. Included in the kits should be (but not limited to):
    - Templates for scenarios/storylines with events, incidents and injects[8],
    - guidelines on how to further extend, personalise, localise, and conduct,
    - guidelines and indicators on how to report and measure impact (pre, during and post exercise execution)
  - The contractor must be able to provide the exercise scenarios/injects in a:
    - Structured format; to be used with a compatible exercise platform
    - "pen & paper" format (e.g. to allow for a discussion-based table top execution format)

[7] Please note that threat hunting service must include at least – analysis of vulnerabilities and risks within specified entity, analysis of specific threats (including APTs).

[8] Writeups, step by step execution of the exercise.

- All textual outputs will have to be provided in English.
- The contractor must be able to support a full execution, if requested to do so (and planned in advance), this request might include an option to distribute injects to players via an exercise platform (system or environment).
- The contractor must be able to offer training, assistance, and support (including to third parties), as per ENISA's needs (for example, trainings on how to use the developed kits).

- Evaluation and/or testing MS cybersecurity capabilities (including capabilities to prevent, detect and respond to incidents)
  - The contractor must be able to conduct a capabilities evaluation and testing on-demand either directly or by purchasing service from other provider.
  - The contractor is expected to support the evaluation and testing and risk assessment using methodology indicated by ENISA.

- Evaluation of cybersecurity maturity of European Union Member State
  - The contractor is expected to support ENISA for the evaluation of cybersecurity maturity of European Union Member States, and the performance of Risk Assessments at National or sectorial level, using ENISA's guidelines and adhering to Member States' needs. ENISA will provide harmonised assessment guidelines, which might need to be localised according to European Union Member States' standards and best practices.
  - The contractor must be able to provide "lessons learnt" and suggested next actions and/or steps to take.
  - The contractor is expected to support ENISA to anonymise and aggregate data and results, in order to produce publicly available reports if needed.

- Providing advice on how to improve infrastructure and capabilities
  - The contractor is expected to support ENISA in the provision of advice on infrastructure and cybersecurity capabilities for different sectors of MS entities (for example energy, transport, financial)

For all of the abovementioned services, the prospective contractor must be able to deliver comprehensive reports including a Summary, Objective, Scope, Methodology, Findings and Recommendations. The contractor should also be able to deliver intermediate reports and presentations as required.

TECHNICAL HELP WITH INCIDENT MANAGEMENT

- Information Security Incident Analysis
  - The contractor must be able to support information and evidence collection (remotely or on premises if needed), in the analysis and gaining the understanding of cybersecurity incident upon demand.

- The contractor must be able to support using applicable international standards and best practices in incident management process.
- The contractor is expected to support ENISA in providing advice on triage of the incident.
- The contractor is expected to support ENISA in providing advice on information collection of the particular incident.
- The contractor is expected to support ENISA in providing advice on root cause analysis of a particular incident.
- The contractor is expected to support ENISA in providing advice on cross-incident correlation (including possible cross border impact).

- Artefacts and Forensics Evidence Analysis
  - The contractor is expected to conduct artefacts and forensics evidence analysis upon demand.
  - The contractor must comply with applicable international standards and best practices in artefacts and Forensics evidence analysis process.
  - The contractor is expected to support ENISA to conduct analysis on various types of technologies (including workstations and servers based on different OS; Mobile devices based on various OS, Industrial Control Systems, IoT devices, Virtualisation and Cloud solutions).
  - The contractor is expected to support ENISA to conduct log analysis (including system, application and network logs) including large amounts (more than 1 TB).
  - The contractor is expected to support ENISA to provide at least media or surface analysis, reverse engineering, runtime or dynamic analysis, comparative analysis.
- Information Security Incident Coordination
  - The contractor is expected to support ENISA to provide Information Security/Cyber Security Incident Response, Coordination and Crisis Communications as a retainer type of service.
  - The contractor should include conditions for unused IR retainer that could be converted in other services covered by the offer.
  - The contractor is expected to support ENISA to provide advice on Cybersecurity incident response and coordination.
  - The contractor must support end-to-end Cybersecurity Incident Coordination.
  - The contractor is expected to support ENISA to provide advice on crisis communication process.
  - The contractor must be able to support incident coordination either remotely or on-site as requested

- The contractor must be able to provide support for at least 4 large scale[9] incidents in parallel within the territories of all 27 Member States. The contractor should specify how many parallel incidents can be supported as maximum under the scope of this tender.

Please note that the estimated number of incidents within one year is less than 10 large scale incidents.

For all of the abovementioned services, the prospective contractor must be able to deliver comprehensive reports including a Summary, Objective, Scope, Methodology, Findings and Recommendations. The contractor should also be able to deliver intermediate reports and presentations as required.

ASSISTANCE WITH THREAT ASSESSMENT

- Threat Assessment process implementation/life cycle
  - The contractor is expected to support ENISA in providing advice on threat assessment process implementation upon request
  - The contractor is expected to support ENISA in providing analysis of the threat assessment process implementation based on international standards and best practices.
- Specific Threat and Risk Assessments
  - The contractor is expected to support ENISA in delivering specific threat assessment on demand (on entity, specific sector or MS level).
  - The contractor must be able to deliver specific continuous risk monitoring services such as attack surface monitoring, risk monitoring for assets and vulnerabilities of a particular entity, and be able to draw a risk overview for a particular sector or geography. The services should be provided as subscription service (either directly or acting as an authorized reseller) for the provider indicated by ENISA.
  - The contractor must indicate the amount of commission or any administrative overhead required for providing specific risk monitoring as a subscription service.
- Threat landscape
  - The contractor must be able to support the creation of a threat landscape and risk scenarios within given parameters (for example for particular sector, particular MS).
  - The contractor is expected to provide access to a portal type solution that gives comprehensive overview of risks with ability to investigate details if needed.

For all of the abovementioned services, the prospective contractor must be able to deliver comprehensive reports including a Summary, Objective, Scope, Methodology, Findings and Recommendations. The contractor should also be able to deliver intermediate reports and presentations as required.

[9] As understood in Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises https://eur-lex.europa.eu/eli/reco/2017/1584/oj

2.3 REQUIREMENTS OF SERVICE PROVISION

The prospective contractor must be able to support ENISA capabilities for all the aforementioned services. Support of these services is 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 services.

The prospective contractor must be able to fit into ENISA service provision procedure and support ENISA service provision workflow as necessary. Service provision procedure will be made available to contractor as needed.

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

The prospective contractor must be able to provide secure infrastructure and measures for service support including securing information in transit (using PGP and/or S/MIME) and at rest. The contractor should describe infrastructure and specific security measures in their offer.

Services support should be available upon request. ENISA will provide notification to the prospective contractor upon receipt of such a request. The contractor should make available an email and phone number (e.g. hotline) that can be used for the services that require support on a 24/7/365 basis.

For ex-ante services requested service support level shall be:

- Availability: normal working hours (8 working hours between 9AM and 5PM CET time);
- Time to acknowledge notification from ENISA – up to 1 work day;
- Geographical coverage – throughout the territory of Member States of the European Union.
- In case of providing support for exercises - Meeting to discuss request with ENISA need to be booked within 5 working days.

For ex-post requested service support level shall be [10]:

- Availability: 24/7/365;
- Time to acknowledge notification from ENISA – up to 4 hours;
- Time for triage of the notification – up to 4 hours upon receiving notification;
- Time to begin remote assistance – up to 6 hours upon receiving notification;
- Time to begin on-site assistance – up to 24 hours upon receiving notification;
- Geographical coverage – territory of the Member States of the European Union.

The tenderer is expected to provide a formal proposal for a Service Level Agreement (SLA) covering support of both ex-ante and ex-post services and at least the items above. This SLA proposal shall be included as part of your technical offer (as an Annex).

The contractor should be able to provide a team of experts able to provide the necessary level of support for the requested service. It is considered advantageous if the team members have certifications applicable to the requested service (for example certified incident responders and logs analysts). The

[10] Service levels could be negotiated if circumstances of the incident require that.

tenderer is expected to provide CVs of the proposed team members mentioning relevant prior experience.

The contractor should be able to provide also technical equipment necessary to fulfil the support for requested service(s) (including necessary hardware and software if applicable).

The contractor is expected to be able to fulfil specific requirements regarding Non-Disclosure of Information if required in particular request.

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

All reports, presentations and other deliverables within this contract should be done using ENISA templates, unless specifically agreed otherwise.

2.4 EXTRA-MUROS ASSIGNMENTS OF CONTRACTOR(S) STAFF

Any tasks carried out by the contractor's staff outside its premises will be considered as extra-muros activities.

Extra-muros rates are intended as daily rates, where 1 working day corresponds to 8 hours. The contractor's staff shall track the time worked using in a timesheet (the template to be provided by the contractor).

At the end of each assignment, the contractor's staff shall submit a timesheet to ENISA's project manager for prior approval before invoicing.

In exceptional cases and given the complexity of the assignment, overtime can be justified given that it has been notified and agreed with the responsible ENISA manager; a clear indication of the overtime linked to the deliverables/ services should be inscribed on the timesheet.

ENISA will only pay for the time actually worked and tracked by the contractor to carry out an assignment. Travelling time to reach the place of work will not be eligible.

Extra-muros rates shall include subsistence costs incurred by staff (e.g. meals, accommodation, local transport etc.) and exclude return trip travel costs, as these will paid as lump sums (see table below) based on the shortest itinerary between the contractor's headquarters and the place where extra-muros assignments are carried out:

Distance	Lump sum (per return trip)
0 to 100 km	€ 0
101 to 200 Km	€ 50
201 to 500 km	€ 150
501 to 1000 km	€ 250
1001 to 2000 km	€ 350
2001 to 3000 km	€ 450
Over 3000 km	€ 500

One only travel lump sum (inbound and outbound) per expert will be paid in conjunction with *extra-muros* activities, independently from the length of the assignment.

3 SPECIFIC REQUIREMENTS

3.1 PROVISION OF SERVICES – CONTRACT MANAGER

ENISA will designate a contact point 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 having a minimum of three (3) years of professional experience in managing contracts and shall be able to communicate fluently in the English language as well have proven experience in large project management. The contractor shall provide its 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 ticketing system proposed by ENISA. The tenderer should provide a CV of the Contract manager.

The 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.

.All communication with ENISA will be in English, being the working language of ENISA, and deliverables must be provided in English unless specifically agreed otherwise. If applicable and required some of the communication/documents might be in the official language of the European Union Member State being provided the service.

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.
- Relevant national legislation knowledge and compliance.
- Experience in developing processes and procedures related to incident response, management and coordination.
- Providing technical, operational and strategic support and assistance in case of cybersecurity incidents to third parties.
- Practical experience in provision of all the services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* described in the offer at least at the level of detail mentioned in the sub-section 2.2.
- Practical experience in handling large-scale cybersecurity incidents involving multiple stakeholders (expertise in the domain of how the members of the CSIRTs Network[11] and/or European Union Member States handle cyber incidents will be considered as advantageous).
- Experience in all service areas (including services in each area) covered by CSIRT Services Framework in particular: information security incident management, vulnerability management, information security event management and knowledge transfer.

[11] https://csirtsnetwork.eu/

- Good knowledge of areas that might be impacted by large-scale incidents (e.g. ICS, IoT, Operators of Essential Services, Digital Service Providers etc.).
- Practical experience in Crisis communication.
- Practical experience in provision of Cybersecurity Exercises.
- Practical experience in cybersecurity capabilities assessment and cybersecurity infrastructure assessment (e.g. maturity assessments, penetration testing, vulnerability assessment).
- Presenting complex technical issues to various stakeholders (e.g. operational and political decision makers).
- Practical experience of working with government organizations and/or critical infrastructure operators in the MS.
- Practical experience with using and complying with service management frameworks (ITIL or similar)

3.3 EXPERTS PROFILES

The tenderer shall provide CVs of relevant experts describing their experience in similar projects and possible certifications if available. The team of experts will be selected depending on their experience with regard to the specific requirements related to each project. 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.

The Curricula Vitae (CVs), preferably in the Common European format, of the proposed members of the team must be enclosed and clearly showing qualifications, professional experience within the relevant business area with the start and the end date (i.e. from DD.MM.YYYY to DD.MM.YYYY) and the linguistic skills. The form can be downloaded from:

https://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions

The successful tenderers may be requested to provide the diplomas and professional qualifications of the persons responsible for providing the services, and/or any other type of relevant work in the field that is the object of this contract.

For this call in particular, it is expected the inclusion of enough experts to be able to provide all of the services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* at the required service level (indicatively a minimum of 8 experts; 4 of 'Senior Experts' and 4 of 'Junior Experts' (see below reference profiles)).

3.3.1 JUNIOR EXPERT PROFILE (CAPABILITY ASSESSMENT)

The **Junior Expert** shall have:

- Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent;
- At least three (3) years of professional experience and expertise relevant to the provision of the capability assessment services listed in *Section 2. DESCRIPTION OF SERVICES TO*

BE PROVIDED described in the offer at least at the level of detail mentioned in the sub-section 2.2., including professional experience and expertise web application and network security testing, manual and tool aided, vulnerability assessment, penetration testing and generating reports using tools;

- Extensive knowledge of hardware, software and networking technologies;
- Very good and clear writing and speaking communication skills;
- Excellent command of the English language (at least C1 level according to the Common European Framework of Reference for Languages (CEFR));

Advantageous:

- Certified Pentester;
- Certified Information Systems Security Professional;
- Other relevant professional certifications.

3.3.2 SENIOR EXPERT PROFILE (CAPABILITY ASSESSMENT)

The **Senior Expert** shall have:

- Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent;
- At least five (5) years of professional experience and expertise relevant to the provision of the capability assessment services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* described in the offer at least at the level of detail mentioned in the sub-section 2.2., including professional experience and expertise web application and network security testing, manual and tool aided, vulnerability assessment, penetration testing and generating reports using tools;
- Extensive knowledge of hardware, software and networking technologies;
- Very good and clear writing and speaking communication skills;
- Excellent command of the English language (at least level C1 according to the Common European Framework of Reference for Languages (CEFR));
- Excellent project management skills including quality assurance.

Advantageous:

- Certified Pentester;
- Certified Information Systems Security Professional;
- Other relevant professional certifications.

3.3.3 JUNIOR EXPERT PROFILE (CYBERSECURITY EXERCISES)

The **Junior Expert** shall have:

- Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent;
- At least three (3) years of professional experience and expertise relevant to the provision of the capability assessment services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* described in the offer at least at the level of detail mentioned in the sub-section 2.2., including professional experience and expertise provision of different types of cybersecurity exercises, support of exercise platform or system and localization/personalization of cybersecurity exercises;
- Very good and clear writing and speaking communication skills;
- Excellent command of the English language (at least C1 level according to the Common European Framework of Reference for Languages (CEFR));

Advantageous:

- Certified Information Systems Security Professional;
- Other relevant professional certifications.

3.3.4 SENIOR EXPERT PROFILE (CYBERSECURITY EXERCISES)

The **Senior Expert** shall have:

- Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent;
- At least five (5) years of professional experience and expertise relevant to the provision of the capability assessment services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* described in the offer at least at the level of detail mentioned in the sub-section 2.2., including professional experience and expertise provision of different types of cybersecurity exercises, support of exercise platform or system and localization/personalization of cybersecurity exercises;
- Very good and clear writing and speaking communication skills;
- Excellent command of the English language (at least level C1 according to the Common European Framework of Reference for Languages (CEFR));
- Excellent project management skills including quality assurance.

Advantageous:

- Certified Information Systems Security Professional;
- Other relevant professional certifications.

3.3.5 JUNIOR EXPERT PROFILE (INCIDENT MANAGEMENT)

The **Junior Expert** shall have:

- Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent;
- At least three (3) years of professional experience and expertise relevant to the provision of the capability assessment services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* described in the offer at least at the level of detail mentioned in the sub-section 2.2., including professional experience and expertise in logs monitoring, analysis, artefacts and forensics evidence analysis, incident response and incident response coordination;
- Extensive knowledge of hardware, software and networking technologies;
- Very good and clear writing and speaking communication skills;
- Excellent command of the English language (at least C1 level according to the Common European Framework of Reference for Languages (CEFR));

Advantageous:

- Certified Logs analyst, Incident responder, Forensic Analyst;
- Certified Information Systems Security Professional;
- Other relevant professional certifications.

3.3.6 SENIOR EXPERT PROFILE (INCIDENT MANAGEMENT)

The **Senior Expert** shall have:

- Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent;
- At least five (5) years of professional experience and expertise relevant to the provision of the capability assessment services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* described in the offer at least at the level of detail mentioned in the sub-section 2.2., including professional experience and expertise in logs monitoring, analysis, artefacts and forensics evidence analysis, incident response and incident response coordination;
- Extensive knowledge of hardware, software and networking technologies;
- Very good and clear writing and speaking communication skills;
- Excellent command of the English language (at least level C1 according to the Common European Framework of Reference for Languages (CEFR));
- Excellent project management skills including quality assurance.

Advantageous:

- Certified Logs analyst, Incident responder, Forensic Analyst;
- Certified Information Systems Security Professional;
- Other relevant professional certifications.

3.3.7 JUNIOR EXPERT PROFILE (THREAT ASSESSMENT)

The **Junior Expert** shall have:

- Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent;
- At least three (3) years of professional experience and expertise relevant to the provision of the capability assessment services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* described in the offer at least at the level of detail mentioned in the sub-section 2.2., including professional experience and expertise in threat hunting, threat analysis, situational awareness reporting;
- Extensive knowledge of hardware, software and networking technologies;
- Very good and clear writing and speaking communication skills;
- Excellent command of the English language (at least C1 level according to the Common European Framework of Reference for Languages (CEFR));

Advantageous:

- Certified Information Systems Security Professional;
- Other relevant professional certifications.

3.3.8 SENIOR EXPERT PROFILE (THREAT ASSESSMENT)

The **Senior Expert** shall have:

- Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent;
- At least five (5) years of professional experience and expertise relevant to the provision of the capability assessment services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* described in the offer at least at the level of detail mentioned in the sub-section 2.2., including professional experience and expertise in threat hunting, threat analysis, situational awareness reporting;
- Extensive knowledge of hardware, software and networking technologies;
- Very good and clear writing and speaking communication skills;

- Excellent command of the English language (at least level C1 according to the Common European Framework of Reference for Languages (CEFR));
- Excellent project management skills including quality assurance.

Advantageous:

- Certified Information Systems Security Professional;
- Other relevant professional certifications.

4. PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATION

The execution of the tasks will take place either remotely or on the site at the place of assignment. Network based collaborative tools (i.e. videoconferencing) will be used as normal working methods. The contractor, upon invitation, may visit ENISA's premises at Agamemnonos 14 St. Chalandri, 15231, Attiki, for ad hoc meetings. A kick off meeting shall be convened virtually.

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" (max 20 pages), 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 descriptions for each of the six (6) 'Scenarios', as well as the CVs of the experts and draft SLA, shall be submitted as Annexes to the Technical Offer, and are thus NOT included in the 20 page limit.

The Technical Offer shall include the following:

- Presentation of tender proposal;
- Summary in form of table of ability of the tender to provide services listed in *Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED* described in the offer at least at the level of detail mentioned in the sub-section 2.2.;
- Evidence and material demonstrating expertise in the fields covered by this call for tender (including Incident response and penetration testing for Union's essential and important entities);
- Management practices, planning and resource allocation to tasks and experts, available to be used in order to meet the Agency's requirements.
- Proposal on operationalize service towards ENISA for both ex-ante and ex-post services based on required Service level (for example, request of the service, change request, proof of delivery)
- Project and Service management methodology that will be used for projects under this framework contract, explaining how possible projects would be carried out efficiently, timely and effectively;
- The procedure for the provision of experts (e.g., backup solutions etc.) and workflow of provision of service support;

- 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.
- Description of considerations and measures[12] of information protection, secure communications and data storage during services support.
- Relevant risk analysis with mitigation measures.

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, (see Part 3 – Section 3.3), 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.

5.2 SCENARIOS

The following scenarios must be assessed and a technical description of how you would implement and deliver the final deliverable be provided as part of your technical offer (see section 5.1 above). Your actual estimations of volume of work required in 'person days' per profile and overall project cost shall then be entered into the appropriate 'scenario' boxes in the Financial Offer form (Annex IV(b)). These scenarios refer to possible situations in accordance with ENISA needs, in order to facilitate the tenderer towards building a reliable and comparable financial offer. Daily/half daily rates are also required to be provided in Part a) and b) of the Financial Offer form for the requested profiles, which must then be used as the basis, together with estimation of person days/half days required, for each scenario. The actual projects to be awarded to the successful contractor will have a much more detailed level of technical specifications.

Please note: Failure to provide a technical description and price estimation for scenarios may result in your offer being declared invalid and not further evaluated.

5.2.1 SCENARIO 1: EX-ANTE SERVICE SUPPORT (PENETRATION TESTING)

ENISA is requested to provide a "black box" penetration test for an administrative IT infrastructure of an essential and important entity (an SME energy provider) in a European Union Member State. For the sake of this scenario the tenderer should assume 400 end-points; using Windows environment and Active directory; 200 users and an internet facing web application providing portal services. The requirement is to provide testing with a team on site for duration of 15 working days. The deliverable must be a presentation summary, a report with detailed information on how to reproduce the findings and

[12] Including ability to comply with conditions specified by ENISA

recommendations to address or mitigate them. ENISA is responsible for the delivery of the service supported by the contractor.

The contractor is expected to suggest an appropriate methodology and approach for the testing, and execution of the technical plan. ENISA will be responsible for coordinating the engagement with the SME energy provider.

The contractor must be able to support ENISA in the execution of at least the following stages of penetration testing: planning, exploration of systems and services within scope, identifying vulnerabilities of the systems and/or services within limits agreed, identifying potential impact, coordination of test delivery, analysis and reporting.

5.2.2 SCENARIO 2: EX-POST SERVICE SUPPORT (INCIDENT RESPONSE)

ENISA will use the retainer service from the contractor to provide incident response support to the impacted entity within a defined Service support level. For this scenario the contractor should provide a quote and description for an Incident response retainer providing 100 expert days available for incident response. For the costing of this scenario, the 100 days shall all be utilised. The contractor must be able to provide support throughout the life cycle of incident response – identification, containment, eradication and recovery. The contractor must be able to support creation of the report with lessons learned. The contractor should also describe a particular response to a ransomware incident affecting at least the administration network and a suspected personal data leak) for an essential and important entity in a European Union Member State (an SME hospital). For the sake of this scenario the tenderer should assume 400 end-points, using the Windows environment and Active directory.

Furthermore, please also describe, in the case of having unused person days, your proposed approach for any unused part of the Retainer - please propose for the situation of having 10 / 20 / 30 / 40 / 50 person days). It should be noted that any unused Retainer approaches will be evaluated only as part of the Award Criteria and are not required to be entered in the Financial offer form.

5.2.3 SCENARIO 3: EXERCISE PROGRAMME SETUP

ENISA has decided upon a prioritised list of sectors/areas or entities for which operational-type exercise kits need to be created. ENISA will need to establish an Exercise Programme to control and guide the portfolio of such exercise kits.

The contractor must be able to suggest and describe an appropriate method and approach for setting up and managing the Exercise Programme (Planning, Conducting and Improving phases).

The method should support a continuous improvement approach and it should also include specific elements and indicators that allow measuring the impact of participation to the programme.

5.2.4 SCENARIO 4: OPERATIONAL-TYPE EXERCISE KIT CREATION

ENISA has decided upon a prioritised list of sectors/areas or entities for which operational-type exercise kits need to be created and agreed on an Exercise Programme to control and guide the portfolio of such exercise kits.

For purposes of this scenario a generic ransomware attack scenario exercise kit needs to be created. The kit shall include:

- a total of 100 injects (mails, media injects, etc.)
- a total of 10 artefacts, some examples of typical artefacts are:
    - malware samples, including dropper(s) for the ransomware;
    - Logs of infected machines and failed attempts to infect;
    - Infected Office documents;
    - Communication logs of infected machines with C&C servers;
    - Network traffic logs (PCAP files);
    - Virtual Machines with an image of e.g. infected computers;
    - Memory dumps.

ENISA will set up and manage an Exercise Project team comprised of contractor's experts per sector/area. The contractor must be able to suggest an appropriate method, approach and resource allocation for the creation of the kit.

The contractor must be able to provide support for such a team in at least the following stages of the planning phase: scoping of the kit, project planning, communications, design and development, and documentation.

5.2.5 SCENARIO 5: OPERATIONAL-TYPE EXERCISE EXECUTION

ENISA has developed a template exercise kit and will set up an Exercise Execution Project team for the particular exercise (assembled from ENISA staff and supporting experts of the contractor). For the sake of this scenario, please assume 100 participants and the exercise kit that is provided, is based on a generic ransomware attack scenario, with 100 injects (mails, media injects, etc) created in English. This scenario must be personalised for the energy sector and it should be translated in the local language. The contractor must be able to suggest an appropriate method and approach for executing the exercise. The contractor must be able to deliver on all of the following stages:

- preparation phase:
    - Extending, personalising, and localising the kit content to better suit the particular setting (specific goals and objectives for the energy sector, adaptation to players' functions and roles, translation into local language of mails and media injects, etc.).
    - Three types of communications activities should be considered:
        - Setting up and testing the communications methods planned for use during the exercise;
        - Managing communications for the purpose of exercise planning and interested party engagement:
            - communicating the pertinent parts of the exercise programme to interested parties and informing them periodically of its progress);
            - communicate the benefits to those who have responsibility for an exercise
        - Managing communications among the project team during the exercise

- on boarding participants (planners, observers, players etc.) onto the platform (for this scenario assume the platform is provided by ENISA/host).

- conducting phase: launch, execute, terminate (based on a one-day exercise execution).
- improving phase: observation collection and analysis, debriefing (hot/cold-wash), After Action Report/Review (AAR), kit feedback/improvements.

5.2.6 SCENARIO 6: OPERATIONAL-TYPE EXERCISE PLATFORM

ENISA has developed a portfolio of exercise kits (see Scenarios 3 and 4) and requests a platform that will support the execution of operational-type exercises (simulations). This platform should be able to import the kits that are provided in a structured format. The contractor must be able to support a suitable platform for conducting exercises with players across the EU MS, without undue technical restrictions on the participants' side (e.g. support BYOD, not rely on the existence of bespoke software/hardware on site etc.)

The platform should be able to import exercise kits and allow for modification of exercise parameters, personalisation and localisation. The contractor must be able to provide support, ensure security and high availability of the platform. For the purposes of costing this Scenario please assume the platform will be required for a period of one year.

6. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

The Financial offer must be drawn up using the **Financial Offer form (see Annex IV (b) for LOT 28 only)**. It is important to note that only the Financial Offer form for LOT 28 shall be used for this LOT.

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(b) – Financial Offer form:

- Cost of the junior and senior experts for each separate Profile. 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 retainer of service (when applicable);
- Cost of providing a subscription service (when applicable)

Please take special care to enter prices in all 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 maximum 3 Framework Service Contracts for this LOT. 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 three (3) years.

It is important to note that the amount stated above applies to **all** framework contracts signed under the 'cascade' system in total and not for each framework contract. There will be a minimum of two and a maximum of three framework contracts signed, if there are a sufficient number of admissible tenderers that meet the award criteria and minimum quality points following the evaluation of offers.

(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[13] ('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[14] (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:

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:

[13] 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

[14] 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

- 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)[15], 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 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.

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

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, subject to prior approval of the report accompanying the invoices, listing the services rendered, within 60 days of submission of an invoice accompanying the final report or deliverable based on the conditions set out in the draft contract.

16. CONTRACTUAL DETAILS

A Framework Service Contract will be proposed to the successful candidates. Selection of candidates 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 two times for a maximum of three 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 Contracts will be performed via Specific Contracts following the 'Cascade' procedure. (see Section 17 below).

***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.*

17. PROVISION OF SERVICES – CASCADE SYSTEM

At the conclusion of this tender procedure, at least two and up to three tenderers who are top-ranked following the outcome of the evaluation, will be awarded framework contracts.

ENISA sends a 'Request for Services' on a specific subject matter to the first contractor in the cascade, and only in case the contractor does not accept the request for reasons which do not entail terminating the contract, or fails to observe the deadline for submission of an offer, or is in a situation of conflicting interests that may negatively affect the performance of the specific contract, ENISA may place the order with the next contractor in the cascade. The proposal shall only consist of a technical offer and will not require any administrative paperwork or proof of economic stability to be re-submitted.

- The Framework Contractors will be required to respond typically within 7 - 14 working days with a detailed technical proposal, depending on the complexity of the project. This offer will contain all aspects regarding:
    - Technical content relevant to the specific subject matter
    - Experts proposed (*they should be from the pool of experts already included in the contract but alternatives can be proposed in exceptional circumstances which are well documented*)
    - A project plan
    - Proposed duration of consultancy in person-days
    - Cost

ENISA will evaluate the offer received by the closing date for reception of the proposal. A Specific Contract will be concluded if the proposal is compliant with the specifications set in the Request for services:

For each Specific Contract the contractor will designate a Project Manager. The Project Manager will be responsible for overall management of the assignment, the timely completion of the activities and the quality and timely delivery of the deliverables.

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[16] 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[17], all tenders must provide information and supporting documentation in two sections:

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

[17] *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(b).**

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[18].

- 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;

[18] 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*.

> ***PLEASE NOTE:*** *Due to the urgency in concluding framework contracts for each LOT, so that actual services may be subsequently ordered via specific contracts, we wish to reduce the likelihood of delays in obtaining documentary evidence supporting your Declaration that your entity/authorised persons are NOT in a situation of exclusion. In some EU Member States, our experience has shown that there are lengthy waiting periods for requests to the National Authorities and/or Courts.*
>
> *It is therefore requested that you provide this evidence together with your bid. In the case that your bid is successful, then delays in checking your evidence are minimised and the contracts can be signed on time. In case you do not receive the evidence before submitting your bid, please indicate in your offer documentation that you have already requested the documentation and it is pending.*
>
> *Please refer to 'Annex III Declaration on Honour' for more information on what evidences are required – here is an indicative minimum list:*
>
> *- Judicial Record*
>
> *- Taxes Certificate*
>
> *- Social Security Certificate*

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[19].

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 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 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.

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.

3.2.2 FINANCIAL AND ECONOMIC CAPACITY

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

- 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.

- **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**

[19] 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

- **For LOT 28: €1.300.000,00 (one million three hundred 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 **€1.300.000,00**.

(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:

a) Support for the service - Support for cybersecurity exercises and capability assessment.

The contractor is expected to be able to develop and provide testing scenarios for cybersecurity infrastructure of requestor, provide support in executing various testing scenarios (including penetration testing), conducting exercises, provide actionable advice for improvement. Support should be available according to the Requested service support level (*Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED*).

b) Support for the service - Assistance with threat assessment

It is expected by the contractor to be able to go through the log analysis to identify trends and do threat hunting as well as be able to do assessment of specific threat and provide coverage of threat landscape. Support should be available according to the Requested service support level (*Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED*).

c) Support for the service - Technical help with Incident management Incident response

The potential contractor should be able to provide incident response services. Incident response should be available according to the Requested service support level (*Section 2. DESCRIPTION OF SERVICES TO BE PROVIDED*). Incidents management process should include at least detection, containment, root cause analysis, remediation, restoration, lessons learnt.

Criteria and Evidences for Lot 28:

Criterion T1 The tenderer must demonstrate ability to provide penetration testing services using industry best practices as well as having proven service provision process in place.

Evidence for T1: Proven provision of penetration testing for Union's essential and important entities - Reference list (including contact details or anonymized information which must include sector, size, and

length of the engagement) of minimum three (3) current and/or past customers[20] to whom the tenderer has supplied 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.

Criterion T2: The tenderer must prove experience in supporting cybersecurity capability assessment.

Evidence for T2: 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.

Criterion T3: The tenderer must prove experience in supporting cybersecurity exercises.

Evidence for T3: 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.

Criterion T4: The tenderer must prove experience in incident management services.

Evidence for T4: 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.

Criterion T5: The tenderer must prove experience in threat assessment services.

Evidence for T5: Reference list (including contact details) of minimum three (3) current and/or past customers to whom the tenderer has supplied 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.

Criterion T6 The tenderers must demonstrate ability to procure cybersecurity subscription services from a third party – such as attack surface monitoring, risk monitoring for assets of particular entity, sector or European Union Member State.

Evidence for T6: proven cooperation with relevant service providers or proof of ability to acquire third party services.

[20] Unless specified differently here and further in text preferably referenced customers should be MS governmental entities of critical infrastructure providers as well as 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[20])

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.	**Quality of the methodological approach and project management**	Quality of the technical proposal including: • Overall methodology and description of methodologies to be used for each of the services included under Part 2/section 2; • Approach to project management for services listed in Part 2/section 2, demonstrating good management of processes, information and time; • Compliance with the requirements indicated under Part 2/section 5.1; • Capacity and competence to manage multiple concurring assignments and ensure availability of the services • Quality of SLA provided	30
2.	**Internal Organisation**	Organisation of work and resources including: • Overall organisation of the project team and quality of the proposed members of the team in regards with the advantageous elements as outlined in section 3.2[21] • Measures to ensure effective communication among team members and between the contractor and ENISA • Work plan for implementing the framework contract and expected requests for services	30

[21] The knowledge and experience of the proposed team members as regards the advantageous elements as outlined in section 3.2, would be considered under the award criteria only in the way in which those aspects apply for the purpose of this contract.

3.	**Response to Scenarios** **Scenario 1** (max 8 points) **Scenario 2** (max 8 points) **Scenario 3** (max 6 points) **Scenario 4** (max 6 points) **Scenario 5** (max 6 points) **Scenario 6** (max 6 points)	Quality of technical proposal for each scenario: • Resource allocation, timing and process organisation; • Implementation of requirements outlined in Section 5.2; • Risk management of specific scenario; Demonstrated know-how of technical solutions;	40
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(b) page 3).

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:

$$PP = (PC / PB) \times 100$$

where:

PP = Price points

PC = Cheapest bid price received

PB = Bid price being evaluated

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.

3.3.3 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:

$$TWP = (Q_P \times 0.7) + (P_P \times 0.3)$$

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 **4th October 2022 at 10:00 EEST Eastern European Summer Time (Greek local time)** at ENISA Athens office, 14 Agamemnonos Street, Chalandri 15231 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 divided into (28) lots. You may submit a bid for either one or more Lots:

LOT 1: Supporting ENISA for the provision of cybersecurity services in Austria,

LOT 2: Supporting ENISA for the provision of cybersecurity services in Belgium,

LOT 3: Supporting ENISA for the provision of cybersecurity services in Bulgaria,

LOT 4: Supporting ENISA for the provision of cybersecurity services in Croatia,

LOT 5: Supporting ENISA for the provision of cybersecurity services in Republic of Cyprus,

LOT 6: Supporting ENISA for the provision of cybersecurity services in Czech Republic,

LOT 7: Supporting ENISA for the provision of cybersecurity services in Denmark,

LOT 8: Supporting ENISA for the provision of cybersecurity services in Estonia,

LOT 9: Supporting ENISA for the provision of cybersecurity services in Finland,

LOT 10: Supporting ENISA for the provision of cybersecurity services in France,

LOT 11: Supporting ENISA for the provision of cybersecurity services in Germany,

LOT 12: Supporting ENISA for the provision of cybersecurity services in Greece,

LOT 13: Supporting ENISA for the provision of cybersecurity services in Hungary,

LOT 14: Supporting ENISA for the provision of cybersecurity services in Ireland,

LOT 15: Supporting ENISA for the provision of cybersecurity services in Italy,

LOT 16: Supporting ENISA for the provision of cybersecurity services in Latvia,

LOT 17: Supporting ENISA for the provision of cybersecurity services in Lithuania,

LOT 18: Supporting ENISA for the provision of cybersecurity services in Luxembourg,

LOT 19: Supporting ENISA for the provision of cybersecurity services in Malta,

LOT 20: Supporting ENISA for the provision of cybersecurity services in Netherlands,

LOT 21: Supporting ENISA for the provision of cybersecurity services in Poland,

LOT 22: Supporting ENISA for the provision of cybersecurity services in Portugal,

LOT 23: Supporting ENISA for the provision of cybersecurity services in Romania,

LOT 24: Supporting ENISA for the provision of cybersecurity services in Slovakia,

LOT 25: Supporting ENISA for the provision of cybersecurity services in Slovenia,

LOT 26: Supporting ENISA for the provision of cybersecurity services in Spain,

LOT 27: Supporting ENISA for the provision of cybersecurity services in Sweden.

LOT 28: Supporting ENISA for the provision of cybersecurity services EU wide

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.

ENISA's Management Board has adopted the Decision MB/2022/8 in anticipation of DG CNECT's ‘Letter of Intent regarding ‘ENISA Cybersecurity Support to MS action’ as a prerequisite for concluding this tender procedure.

6. SPECIFIC INFORMATION

6.1 TIMETABLE

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

Title: '**Supporting ENISA for the provision of services under Cybersecurity Support Action'**

ENISA F-OCU-22-T31 LOTS 1 - 28

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	26th August 2022	
Deadline for request of information to ENISA	27th September 2022	
Last date on which clarifications are issued by ENISA	29th September 2022	
Deadline for **electronic reception** of offers via ***e-Submission***	**3rd October 2022**	**18:00 CEST** Central European Summer time
Opening of offers	4th October 2022	**09:00 CEST** Central European Summer time
Date for evaluation of offers	TBA	
Notification of award to the selected candidate + 10 day standstill period commences	TBA	
Contract signature	end October 2022	Estimated