Scan to verify source & version of document.

OPEN CALL FOR TENDERS

"Web Hosting and (Plone) Web Development services"

ENISA F-SRAD-17-T28

Part 1 **Introduction to ENISA**

Part 2 **Terms of Reference**

Part 3 **Tender Specifications**

Annex A	*Service Level Requirements*
Annex I	Legal Entity & Financial ID Forms
Annex II	Declaration on honour on exclusion criteria and selection criteria
Annex III	Financial Offer form
Annex IV	Draft Framework Service contract
Annex V	Administrative Identification and Declaration form
Annex VI	Power of Attorney for Consortium Form
Annex VII	Sub-Contractors Form
Annex VIII	Checklist of documents to be submitted.

CONTENTS

PART 1 INTRODUCTION TO ENISA

1. Background on ENISA

1.1 Introduction

E-communication infrastructures and online services are essential factors, both directly and indirectly, in economic and societal development. They play a vital role for society and have in themselves become ubiquitous utilities in the same way as electricity or water supplies and also constitute vital factors in the delivery of electricity, water and other critical services. Communications networks function as social and innovation catalysts, multiplying the impact of technology and shaping consumer behaviours, business models, industries, as well as citizenship and political participation. Their disruption has the potential to cause considerable physical, social and economic damage, underlining the importance of measures to increase protection and resilience aimed at ensuring continuity of critical services. The security of electronic infrastructures and services, in particular their integrity, availability and confidentiality, faces continuously expanding challenges which relate, inter alia, to the individual components of the communications infrastructure and the software controlling those components, the infrastructure overall and the services provided through that infrastructure. This is of increasing concern to society not least because of the possibility of problems due to system complexity, malfunctions, systemic failures, accidents, mistakes and attacks that may have consequences for the electronic and physical infrastructure which delivers services critical to the well-being of European citizens.

1.2 Scope

The European Union Agency for Network and Information Security (ENISA, hereinafter 'the Agency') was established in order to undertake the tasks assigned to it for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the establishment and proper functioning of the internal market.[1]

1.3 Objectives

The Agency's objectives are as follows:

- The Agency shall develop and maintain a high level of expertise.
- The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
- The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
- The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
- The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

2. Additional Information

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

[1] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

PART 2 TERMS OF REFERENCE

I. SCOPE OF THIS TENDER

Within the framework of this Open tender procedure, ENISA would like to find a suitably qualified contractor to provide the services for the procurement of dedicated (Plone) Web Development and Web Hosting services for ENISA's main website and several ENISA portal sites as stipulated in the Technical Specification outlined below.

ENISA uses various digital communication channels. The ENISA website is an important communication tool to get its message across to government organizations, businesses and citizens across Europe. The scope of this tender includes ENISA's main website (www.enisa.europa.eu) and several ENISA portal sites, i.e. extranets dedicated to specific user groups (for example, working groups, groups of stakeholders, etc.) collaborating with ENISA.

Both the website and the portals are based on the Plone Content Management System; therefore, prospective tenderers should demonstrate experience and have in-depth knowledge of CMS platforms and Plone in particular. Given the nature of ENISA's work and focus on cyber security, the security of the websites is crucial and so security should receive maximum attention.

Subject of the tender	Maximum budget
Web Hosting and (Plone) Web Development services	An estimated overall budget of **€470,000.00** over the maximum possible period of 4 years[2]. ***PLEASE NOTE:*** *Out of the overall budget of EUR. 470.000,00 a* ***maximum of €90,000.00*** *can be attributed to "Web hosting services" over the maximum possible period of 4 years – including the costs of the one-off 'Migration'*
PLEASE NOTE: *This tender procedure is limited to tenderers which are legally incorporated in a member state of the European Union/EEA, or which have an incorporated subsidiary in one of the EU/EEA member states. (The Agreement on Government Procurement (GPA) does not apply to EU Regulatory Agencies.)*	

[2] conditional upon extension of the Agency's mandate which currently ends on 18 June 2020.

Method for submitting a tender:	Send your offer **electronically** to this restricted functional email account: tenders-F.SRAD.17.T28@enisa.europa.eu
Deadline for dispatch of offers for this tender: *(See Part 3: Section 1.1 for details)*	**Friday 16th June 2017 at 15:00 CEST** **(Central European Summer Time)**

PLEASE NOTE:

a) You are asked to also send an email to procurement@enisa.europa.eu confirming that you have sent an offer for this particular tender.

b) It is important to note that there can be **NO EXCEPTIONS** regarding reception of electronic offers by the expiry date and time. It is entirely the responsibility of the tenderer to despatch its offer by email well before the expiry time, as ENISA cannot be held responsible for internet connection problems resulting in late arrival to our servers.

Any offers received after the expiry time will be ineligible for evaluation and subsequent award of contract!

It would therefore be prudent to despatch your offer as soon as possible and not in the last few minutes before expiry. Be assured that all offers received are locked and inaccessible to anyone within ENISA until the functional email account is unlocked soon after the expiry time. It is also worth noting that Greece is one hour ahead of Central European time.

An automated confirmation email is sent from our email server when you submit your offer by email. Due to limitations of our system, any subsequent emails you send (for reasons such as splitting a large offer into multiple emails) will not result in any further confirmation emails being generated – please do not therefore re-send the same email multiple times. (for more information please refer to *Part 3 – Section 1.1 – 'Address and deadline for submission of the Tender')*

1. OVERVIEW OF CURRENT ENISA IMPLEMENTATION

1.1 Domain, subdomain and URL structure

The main ENISA website is at http://www.enisa.europa.eu . The website is a Plone CMS instance.

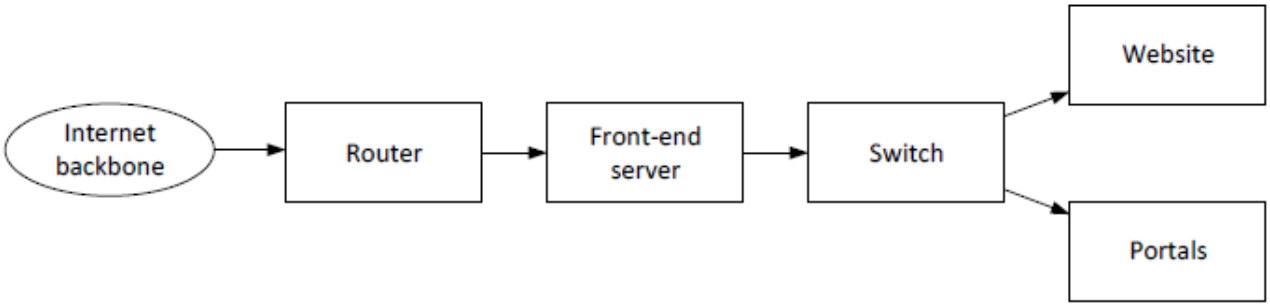
On a separate webserver there are two portal sites. They are two Plone CMS instances reachable via http://mbportal.enisa.europa.eu, and http://resilience.enisa.europa.eu. The former is referred as 'the management board portal' and the latter as 'the exercises portal' or the 'resilience portal'. At the moment, ENISA's Incident Reporting tools are also part of ENISA's resilience portal.

There is also one website dedicated to ENISA's European Cyber Security Month (ECSM) campaign reachable via https://www.cybersecuritymonth.eu/ and an event website dedicated to ENISA's Annual Privacy Forum http://privacyforum.eu/ (based on Naaya CMS).

The websites and portals are accessible via IPv6 and IPv4 and use mostly HTTPS and sometimes HTTP.

1.2 Hardware infrastructure

There are three servers hosting the ENISA website and portals: a frontend webserver, a server for the main website and a server for the portals. The set-up is depicted in the following diagram:



The 3 servers are identical (frontend, website and portals). The server architecture is as follows:

- Quad Core processors, CPU frequency 2.40GHz, 64bit chipset architecture
- 16 GB RAM
- 2 x 300GB SATA HDD in RAID 1
- 2 GBit NIC internet connections

A fourth server is hosting the dedicated website for the European Cyber Security Month website. The server architecture is as follows:

- Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz, 64-bit architecture
- 32 GB of RAM, DDR3
- 2 x 2 TB SATA 6 Gb/s 7200 rpm

The total storage space used by ENISA:

- For frontend server: 100 GB
- For ENISA website: 90 GB
- For portal sites: 60 GB.
- For ECSM website: 20 GB

1.3 Software infrastructure

The website and portal servers are using the following software:

Front end:

- OS: Red Hat Enterprise Linux Server
- Apache
- Piwik

WWW:

- OS: Red Hat CentOS
- Zope
- Plone
- Varnish
- HAproxy
- ClamAV

Portals:

- OS: Red Hat CentOS
- Zope
- Plone
- Varnish
- HAproxy

ECSM website:

- CentOS
- Apache
- Varnish
- Pound
- Zope
- Plone

2. SERVICE REQUIREMENTS for WEB HOSTING

The minimum service requirements regarding the webhosting services are defined in this section.

The tenderer should elaborate in its proposal how each of these requirements will be implemented.

Important notice: Hosting services are restricted to the European Union area and **must not** be transferred outside the EU (e.g. backup datacentre).

2.1 General conditions for the provision of services

The nature of the service requested will be described in this section. They should be understood as the minimum service requirements.

The tenderer is allowed to propose additional or higher level service requirements in their offer. In this case, should the proposal be accepted, the tenderer will be bound to its proposal of higher service levels (and the tenderer cannot afterwards refer to the minimum requirements as set out in this section).

We allow proposals including alternative solutions to any of the detailed technical requirements presented in this tender, provided that the tenderer explains that this would yield at least a comparable service level.

2.2 Web hosting

The tenderer shall provide hosting services. The tenderer may offer web-hosting via a sub-contractor. The proposal should be clear as to which services are being sub-contracted. As a minimum the following should be provided:

- Separate machines for the website, portals and ECSM website - all servers should have at least quad core processors and at least 16GB of RAM. All machines should have at least 500 GB of data storage;
- All servers must be able to offer HTTP and HTTPS connection and must be reachable using both IPv4 and IPv6;
- Servers should have streaming audio and video capabilities;
- Direct connection to a major internet backbone;
- Adequate physical and environmental protection of the servers, and the software and data on these servers, such as fire detection, automatic fire extinguishers, burglary alarms or guards;
- Adequate (logical) access control mechanisms to prevent unauthorized access;
- Adequate security measures to address and prevent cyber-attacks, such as for example, firewalls, intrusion detection systems, anomaly detection, DoS protection, etc.;
- Adequate screening of staff (security clearances, background checks, - where relevant) and adequate training of staff;
- Redundant physical infrastructure to allow for business continuity (minimum downtime) in case of memory, disk, cpu or power supply failure;
- Redundant physical infrastructure to allow for business continuity in the face of local natural disaster (floods, power cuts, fire, etc.). In other words, a second, physically distant, site should be in use or available in case of need. It should be possible to restore backups in such a way that in case of a disaster the website and portals can be restored online within 24 hours;
- Daily backups of the infrastructure to cater for a restore to a point in time; at most 24 hours in the past;
- 24/7 support to respond to critical issues with the webhosting environment.

Recognised information security accreditations for the organization (or for the sub-contractor that would provide for the hosting services), such as ISO/IEC 27001:2013, are preferred. In this case, the proposal should enclose a certificate from a third-party auditor indicating compliance with the standard practices.

The technical details of the hosting services provided should be elaborated in the tenderer's proposal and in particular the above-mentioned topics should be addressed.

Whether or not the web hosting is provided in-house or outsourced, the relevant profile(s), for instance the System Administrator, should be provided. A detailed description of the company which will undertake the web hosting is required in case it is outsourced

2.3 Production and acceptance test environments

The contractor should provide two separate environments: a production environment (referred to as P) and a test environment (referred to as T). The tenderer is responsible for making sure that the two environments are identical in terms of software and hardware. In case of real data use on the test environments the security requirements of the test environments are exactly the same as the production environment.

The test environment will be used by ENISA to check and test new developments, changes and bug fixes before deploying them in the production environment. The test environment will also be used by ENISA to run intrusive tests, like vulnerability scans, and performance/load tests.

Logical access to the test environment should be restricted to designated IP addresses

2.4 Availability and response time

Below we define the minimum service levels for availability and response time:

- A minimum availability of 99.0 % must be guaranteed. Availability is to be measured monthly as the number of total available hours divided by the measurement period.
- Planned downtime must be agreed with the Agency at least 3 days prior to the scheduled date, and should be scheduled between 2000 CET and 0600 CET. Planned down-time should not exceed two hours per month. For urgent cases, direct contact with ENISA must be made via telephone to the assigned ENISA contact person (or his/her backup) beforehand.
- Average server response time should be less than 1 second (first byte). Average network time should be less or equal to 3 seconds.

The contractor shall measure and report about availability and response times (see Monitoring and reporting). The measurement of response time should be done in such a way that measurement is representative for normal usage, for example using a probe located in another city or country. Measurements should reveal the average response time

The contractor shall report about these measurements in the monthly reports (*see section 2.8 Monitoring and reporting*).

2.5 Backups

Below we define the minimum backup requirements:

- Daily backups must be made and kept for 8 days.
- Weekly backups must be made and kept for 35 days.
- Monthly backups must be made and kept for 6 months.
- Backup restore requests should be handled within a maximum of 12 hours.

The contractor should test backups regularly by testing the backup restore procedure. The contractor should report about success or failure of these tests in monthly reports (*see section 2.8 Monitoring and reporting*).

2.6 Patching and updates of servers

The requirements around patching and updates of servers are described below.

Critical system updates and security patches must be deployed within 12 hours of their public release. Normal updates to be performed on a weekly basis. ENISA should be notified prior to each update or patch and all patches and updates should be tested first on a testing environment and then deployed to production.

The contractor should report about deployed updates and patches in the monthly reports (*see section 2.8 Monitoring and reporting*).

2.7 Testing and scanning

Below we define the requirements around testing and scanning:

- The contractor should periodically test for dead links across the website and portals;
- The contractor should carry out vulnerability scans periodically, to identify software vulnerabilities in the deployed operating systems or applications. The results of these scans must be reported to ENISA within 5 working days. Serious vulnerabilities should be reported to ENISA immediately;
- Independent vulnerability scans will be performed by ENISA annually in consultation with the contractor;
- The contractor should perform load or performance tests periodically.

The contractor shall report about the results of these tests and scans in the monthly reports *(see section 2.8 Monitoring and reporting)*.

ENISA can also perform penetrations tests at a given and predefined time after notifying the contractor. With the penetration testing ENISA will attempt to evaluate the security of the IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, service and application flaws, improper configurations etc.

2.8 Monitoring and reporting

The contractor shall monitor service levels continuously and report about them monthly. The service level reports should address the following items – for the website and the portals separately:

- Overall availability;
- Average response time during the day (hourly averages);
- Average response time per day;
- 404 responses (page not found) per day;
- Number of page hits per day;
- Tests;
- Dead links;
- Security scan results;
- Load test results;
- Backups restore test results

Alternatively, the tenderer could offer a dashboard, instead of using monthly reports.

3. SERVICE REQUIREMENTS for WEB DEVELOPMENT

Web development will be requested on a case-by-case basis with requests varying from simple bug fixing, small tasks and enhancements to major web development projects. The contractor shall identify and shall apply appropriate modern technologies and techniques for the web development that will improve and optimize overall all web-based products of ENISA.

ENISA will provide a functional or technical specification of a new development, new project or a simple change needed and the methodology to be followed will be decided on a case-by-case basis.

Web development projects (requests for proposal)

Taking into consideration the complexity of the project, the contractor is expected to provide a preliminary business analysis, a risk assessment, a project plan and a quotation of the amount of work needed (in person hours), a timeline for delivery, and the total costs.

Analysis of business requirements and transposition to technical requirements of most complex tasks/projects (i.e. production of a new tool/web application/website), workflows and wireframes are expected to be done by the contractor as part of the overall web development project. The contractor is also expected to share its expertise on the analysis phase with ENISA project managers in order to facilitate the whole project management flow and assure the end result will reflect all the needs ENISA has on business level. A section which identifies project risks must always be included in the analysis of the contractor at the initial stage.

3.1 Description of tasks (web development projects)

The contractor will need to perform a number of tasks towards the delivery of each major development (i.e. production of a new tool/web application/website). In this section, a short description of the tasks can be found.
During project initiation, the contractor will be asked to provide a detailed project plan together with a relevant timeline of the project flow (e.g. Gantt chart) and key milestones that will be agreed with ENISA. Project management methodology (i.e. waterfall or agile methodology) should be the point of reference for all major web development projects. The methodology to be used in each project will be defined by the project manager of ENISA and the contractor should be able to follow both methodologies. Depending on the complexity of the project, all steps of project management should be followed including validation checks and all have to be applied in every major project depending on the project management methodology.

To this end, the activities mentioned in this section contain an indicative framework for the entire project and will be refined during the project, when deemed necessary.

- **Activity 1**: Set up of the scope
- **Activity 2**: Develop interaction model for the web application/tool – including the development of wireframes/mock ups.
- **Activity 3:** Development of necessary functions
- **Activity 4:** Testing (functional and non-functional)

- **Activity 5:** Deployment
- **Activity 6:** Documentation
- **On-going Activity:** Project Management

3.2 Security by Design

Given the nature of the agency's work/focus, it is of paramount importance that ENISA's environment remains as secure as possible at all times. Security mechanisms, secure functions and security good practices in both coding, configurations and connections shall be utilised to ensure application level security. Corresponding safeguards, e.g. SSL certificates, ISO27001 compliance, etc. shall be considered as a plus.

3.3 Compatibility

Web development should always apply cross-platform and responsive design, meaning that all websites and web apps of ENISA are mobile friendly. The contractor shall use all cutting edge frameworks or boilerplates to satisfy that need and provide always web solutions that reflect the current trends.

The successful contractor should ensure and monitor that the website, portals and tools are accessible from (at least) the top five desktop and mobile browsers and applications. Requirements set in section 2. refer to all these browsers and applications.

Service requirements specified in Section 3 should be met by the contractor wherever applicable to web development and software, e.g. patching, backups, testing and scanning, monitoring and reporting, availability and response time

4. SKILLS OF WEB-DEVELOPERS

The website and portals currently use Plone, Zope, Apache, Varnish, and Pound Load balancer. The tenderer should demonstrate experience in these tools and applications. ENISA may want to explore the possibility of using another Content Management System (e.g. Drupal, WordPress) so additional experience with other (widely used) platforms will be considered advantageous.

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

- Proven expertise and experience in programming Python, HTML and JavaScript;
- Proven skills in creative development of interactive interfaces covering end-user accessibility and functionality requirements in an attractive/innovative manner (user experience);
- Proven experience in transforming user requirements into demonstrable prototypes;
- Experience in systems integration, availability and security of web and mobile infrastructures;
- Experience in testing, optimization and secure software development;
- Experience in automation tools (eg. automated testing, automated deployment) and scripting languages (eg. bash, perl, python);
- Experience in relevant tasks in both the private and public sector;

- Good project management, interpersonal and coordination skills;
- Excellent command of written and spoken English.

Proven expertise and experience in programming PHP SQL and NoSQL and using Wordpress API and Codex and/or Drupal API will be considered advantageous.

5. DESCRIPTION OF PROFILES

The following list is an indicative one of the requested profiles for web development services. Whilst not mandatory, any profiles provided which are not at the levels suggested below will be evaluated and points will be awarded accordingly.

5.1 Project Manager

Nature of the tasks	• Project management including proposals for project strategies, planning, definition of tasks and deliverables, review of project deliverables, quality control, risk analysis and management, project status reports, problem reporting and management systems, follow up and organisation. • Provide effective leadership for the project team ensuring that team members are motivated and constantly developing their skills and experience. Be in-charge of project activities and review deliverables. • Participate in functional and technical working groups and progress meetings. • Estimate and monitor costs, timescales and resource requirements for the successful completion of each project to agreed terms of reference. • Prepare and maintain project and quality plans and tracks activities against the plan, provide regular and accurate reports.
Education & Experience	• A level of education which corresponds to completed university studies of at least four (4) years attested by a diploma • Minimum 4 years' experience in IT Project Management. Practical experience with software development life-cycle. • Proven experience with quality procedures.

Knowledge and skills	• Project management and leadership. • Usage of project management office tools (e.g. Asana, Atlassian / Jira, MS Project or equivalent). • In depth technical knowledge of the project's main aspects and general technical knowledge on the other aspects touched by the project. • Usage of methods and techniques for reporting. • Ability to give presentations. • Participate in meetings and give status report presentations, be a good communicator. • Capability of integration in an international/multi-cultural environment. • Written and oral English at European language level B2 or better.

5.2 Business Analyst

Nature of the tasks	• Liaise with business managers and end-users to understand and document business requirements • Analyse requirements and transform them into technical specifications • Consultancy studies in a specific technical domain regarding information systems. • Production of use case models, software architecture documentation. • Provide expertise in a specific technical domain regarding information systems. • Technical evaluations and provide expertise on integration of IS into the working environment.
Education & Experience	• A level of education which corresponds to completed university studies of at least four (4) years attested by a diploma in one of the following fields: Computer Science, Information Technologies, Mathematics, Physics, Engineering, Business Administration, Business Management or related areas. • A minimum of four (4) years of experience in Information Technology development and/or Information Technology consulting. • Experience with business process analysis, documentation, and change management as well as experience in working with Plone-related methodologies and technologies • Experience in analysis and programming, databases and web application development. • Experience creating detailed project documentation and reporting

Knowledge and skills	• Knowledge of international standards like W3C, WAI and IPG(desirable) standards • Conceptual understanding of content structuring, storage, access and presentation elements • Strong interest in follow-up of trends in web development • Ability to participate in multi-lingual meetings • Good communicator • Written and oral English at European language level B2 or better

5.3 Developer

Nature of the tasks	• Development of web-enabled applications. • Creating/maintaining web applications. • Development of front-end and back-end systems including database development tasks • Develop both simple and complex solutions. • Translate software requirements into concise and robust programming code. • Increase program operating efficiency and adapt system to new requirements, as necessary. • Report status and flag issues to the ENISA Project/Product Manager. • Cooperate with ENISA and UI/UX designers to match visual design intent
Education & Experience	• University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and software development technologies. • At least five (5) years of experience for senior developers and three (3) years of experience for junior developers, developing in a web environment working with python and PLONE – related technologies.
Knowledge and skills	• Top-notch programming skills and in-depth knowledge of modern HTML/CSS • Extensive knowledge of Python, HTML, Javascript and PLONE related technologies (including ZODB) • Experience with version control systems and source code management system for software development, git (preferred) or svn. • Strong interest in follow-up of trends in web development. • Basic knowledge of Search Engine Optimization process • Written and oral English at European language level B2 or better.

5.4 Graphical Interface Designer

Nature of the tasks	• Definition and creation of the graphical layout of web pages, prototyping. • Collaborate with ENISA project manager and software and website developers to define and implement innovative solutions • Execute all visual design stages from concept to final hand-off to ENISA • Conceptualize original ideas that bring simplicity and user friendliness to complex design roadblocks • Create wireframes, storyboards, user flows, process flows and site maps to effectively communicate interaction and design ideas • Conduct user research and evaluate user feedback • Establish and promote design guidelines, best practices and standards
Education & Experience	• Course on web design at University, or at a specialized institute/school followed by 3 years of experience. • Minimum 3 years of experience in the above tasks. • BS/MS in Human-Computer Interaction, Interaction Design, or related will be considered advantageous • Experience working in an Agile/Scrum development process
Knowledge and skills	• Up-to-date with the latest UI trends, techniques, and technologies • Knowledge of international standards like W3C, WAI and IPG(desirable) standards • Demonstrable UI design skills with a strong portfolio • Solid experience in creating wireframes, storyboards, user flows, process flows and site maps • Proficiency in HTML, CSS, and JavaScript for rapid prototyping. • Excellent visual design skills with sensitivity to user-system interaction • Experience in creating vector graphic images –svgs (desirable) • Written and oral English at European language level B2 or better.

5.5 Quality Assurance/Tester/DevOps

Nature of the tasks	• Analysis, design, planning and execution of a test strategy for new features and sustaining projects. • Developing and executing automated tests to enable delivery of high-quality software on time and on budget. • Performing functional and non-functional tests in order to ensure the quality and the proper goal of the end product / feature. • Implement test tools and utilities to improve the efficiency and effectiveness of the development life-cycle • Configuration and maintenance of a test lab environment that resembles complex customer environments • File detailed bug reports and follow up on the problems until complete resolution • Comply with good engineering practices, coding standards and contribute to automation code reviews • Collaboration with development team to assure correct replication, integration and deployment on production.
Education & Experience	• University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and software development technologies. • At least three (3) years of experience developing/testing in a web environment working with PLONE – related technologies.
Knowledge and skills	• Extensive knowledge of Python, HTML, Javascript and PLONE related technologies • Experience with a Test Automation Framework (e.g. Selenium, QTP, Sikuli) • Experience with QA methodologies • Great understanding of testing throughout the product lifecycle, including unit, integration, regression, component and end-to-end system testing • Familiarity with SSH, and one of the following deployment automation tools (Jira/Bamboo, Jira/Zephyr, Chef, Puppet, Maven, Jenkins, Kubernetes, Capistrano etc.) • Strong scripting programming knowledge (e.g. Shell/Ruby/Python) • Strong system administration knowledge of Linux platforms. • Experience with version control systems and source code management system for software development, git (preferred) or svn.

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

ID	Profile	
1	Project Manager	1 CV
2	Business Analyst	1 CV
3	Developer*	3 CVs
4	Graphical Interface Designer	1 CV
5	Quality Assurance/Tester/DevOps	1 CV

*****At least one of the three 'Developers' should be at a senior level, i.e. more than 5 years of experience in web development and database experience, as well as in working with python and Plone-related technologies.

All key roles/resources needed for a project lifecycle should be used in a web development project to assure quality of end result (e.g. analyst, designer, developer, tester, pm, etc.). In each phase of the project, the participation in meetings and interaction of the corresponding key expert with ENISA personnel is expected. However not all the roles/resources are needed for helpdesk support and smaller basic tasks and enhancements of the website and portals. The contractor should be able to propose the relevant team members based on the project's/task's requirements.

In case of the departure of one or more members of the proposed team, the contractor is expected to provide people with the same qualifications and similar experience to cover ENISA's needs.

6. SOFTWARE DEVELOPMENT

Software development should be documented and new code, or new features should be deployed first in the test environment.

On a case by case basis (e.g. for the production of a new tool or an enhancement of existing complex applications) automatic testing of the newly developed code will be required by ENISA. The contractor should be in place to propose the relevant tools for automatic testing, set them up at the beginning of the contract (or when required) and operate them to ensure the overall code quality and performance.

Testing of the overall code performance should also take place annually as an additional exercise and the output should be reported to ENISA.

The contractor is also expected to make sure that the documentation of functionality of the website is alwaysupdated.

Access to the code, databases and Version Control System (e.g. git) of ENISA's projects should be granted to ENISA upon request. ENISA can also perform penetrations tests at a given and predefined time after notifying the contractor.

7. ISSUE TRACKER –TICKETING SYSTEM

The use of purchase orders will be periodically issued for general development services (e.g. bug fixing, small updates) or for new development projects. Within this legal framework, the contractor is expected to operate a ticketing system (such as redmine, flow etc.) to register bug reports, change requests, requests for information, and so on.

Each ticket, together with approval provided by the ENISA responsible person, shall be referred to in the ensuing invoice, which may be partly or fully issued against the amount of the Purchase Order, depending on the mutually agreed periodicity of the invoicing.

The tenderer is free to suggest a regular invoicing period, however the Agency would suggest either bi-monthly or quarterly invoicing, in order to reduce administrative burden on both sides

8. BUGS AND ISSUE REPORTS

The contractor should respond to bug and issue reports based on their classification as per the following table:

Critical: With descending priority, attacks, security updates, website and portals availability, a critical service of the website/portal (e.g. Submission with deadline, such as procurement and recruitment or submission of incident report on incident reporting period) – immediate response (within 2 hours)

High: an issue that prevents an application from meeting requirements or carrying out a feature – response within the same day

Normal: a minor defect that it has no direct effect on the general functionality of the application itself – response within the next 2 days

Low: bugs/issues with no real impact on the functionality of an application (design or cosmetic errors – response within 3 days.

The specific response time per category is further defined in the Service Level Requirements (SLR) which will be annexed to the resulting Framework contract - *see Annex A*.

9. REQUESTS FOR CHANGES

The contractor should respond to change requests (small enhancements, change of behaviour) at the latest within 3 working days. Request for changes will be reported and monitored using the dedicated ticketing system. The specific response time per type of request or incident is further defined in the Service Level Requirements (SLR) according to the urgency of the latter - *see Annex A.*

10. REQUESTS FOR INFORMATION AND CONSULTANCY

The contractor may be asked to provide consultancy services on the feasibility of implementing various ideas put forward by the ENISA staff. The contractor should respond to requests for information within 5 working days

11. DESIGN AND WEBSITE STRUCTURE

The contractor may be asked to provide advice and technical support in improving the Information Architecture of ENISA's website and portals. The contractor should have (or collaborate with) skilled designers, architects and web usability experts to respond to such requests.

ENISA always seeks to improve the website's information structure and design. It would therefore be considered advantageous if tenderers are able to demonstrate expertise in this respect

12. MIGRATION AND TRANSITION

The contractor is required to migrate the website and portals from the existing hosting environment to the new environment. It is expected that this migration should not take longer than one month.

- The tenderer shall provide a one-off costing for this migration, to be scheduled for the first year of the contract, separately from the normal hosting costs (see Annex III Financial Offer form).
- Towards the end of the contract, the contractor will be required to provide ENISA recent backups of data and copies of the source code or binaries, together with a manual that explains how the website and portals can be set-up and operated in a new environment.

At the end of the contract the contractor is expected to facilitate the handover of the data and the source code and binaries to a new contractor or to a new environment, depending on the needs of ENISA. This could require parallel running of the website on the contractor's infrastructure and on another infrastructure

13. PLACE OF WORK AND DELIVERY

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

One face-to-face kick off meeting between ENISA and the contractor will be held at ENISA's premises (either in Athens or Heraklion,). All other meetings between ENISA and the contractor can be made by using video conference systems, telephone or e-mail.

14. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

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

14.1 Web hosting

The tenderer should provide a full description of the web hosting infrastructure, including technical details about how the detailed requirements are being met (physical security measures, physical redundancy, etc. - *please see sub-sections 2.1 until 2.8 above.*

14.2 Web development Services

- Description of your company and how requirements in Section 4 are being met. Up to 5 recent

projects that show relevant expertise and experience in developing and maintaining similar websites or portals;

- Up to 5 recent projects in developing similar Plone-based websites (if the above-mentioned projects do not involve Plone);
- The project team responsible for delivering the services, indicating the project manager and/or the technical experts that will be involved;
- CV's (of max 3 pages) of members of the project team, clearly indicating their relevant experience in the Plone (and other platforms) web development field;
- Description of how you intend to deliver these services, addressing issues such as testing of new features, automated deployment in the test environment, automated deployment in the production environment, test data to test resolved bugs in the test environment and delivery of documentation;
- Quality control and assurance methodology;
- Brief project plans, methodology to be used and estimation of man hours and budget, for fulfilling 4 change/development request scenarios as described below:

14.3 Scenarios - Web development

The following four scenarios must be assessed and your estimations of volume of work required in 'person hours' per profile and overall project cost shall be entered into the appropriate boxes in the Financial Offer form (Annex III). Failure to provide an estimation for each of the 4 scenarios may result in your offer being declared invalid and not further evaluated.

(i) Scenario 1: **Update of the ENISA website news section.**

The news section of the ENISA website (https://www.enisa.europa.eu/news/ has currently two sections: One landing page where the latest news from all major categories are listed and a second section where all news are accessible using faceted navigation. The two sections need to be merged gracefully, with a user friendly, responsive layout. Other features such as "subscribe to newsletter" and access to the press and media centre need to be also preserved.

(ii) Scenario 2: **Upgrade the ENISA website and portals (2) to the latest Plone version.**

(iii) Scenario 3: **Development of a visual tool for ENISA's incident reporting tool.**

ENISA hosts in one of its portals an incident reporting application. This application hosts various information such as:

- asset affected;
- service affected;
- significance of an incident reported;
- year;
- root cause;
- detailed cause etc.

The above mentioned information is reported to ENISA from all the EU Member States, using a form, which is part of the application. There is one entry for each incident. ENISA's requirement is the development of a "visual tool", which will produce a number of graphs (e.g. bars, pie charts, etc.) in order to have a graphical representation of the above mentioned information. However, these graphs

should display “anonymised” information, meaning that they shouldn’t be linked with the Member States. For example, we can have a graph with how many incidents caused by natural causes (e.g. earthquake), but this concerns all the MS. There won’t be a graph showing that we had “x” incidents by natural cause at the “y” MS.

(iv) Scenario 4: Submission of annual report to ENISA’s Incident Reporting tool

- ENISA hosts in one of its portals an incident reporting application, where a type of users is the one called SB (stands for Supervisory Body).
- Each Member State can appoint more than one SB.
- ENISA as the administrator of the application can add/remove users.
- Each Member State has the obligation to report to the European Commission an activity report on an annual basis (starting from 1st January until 31st March).
- ENISA’s requirement is to provide SBs with a platform that they can submit this activities’ report (one per each SB).
- EC users can access this report and view it or export it but not edit it.
- ENISA users can't view/edit/export the report but they have to be informed that this report has been submitted.
- Each time this report is accessed a notification e-mail should be sent to the authorised users.

15. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

The Financial offer must be drawn up using the **Financial Offer form (see Annex III)**. In order to be valid, it must be duly filled in, dated, stamped, and signed by the authorised person.

16. TENDER RESULT AND ESTIMATED CONTRACT VALUE

This tender procedure will conclude with the award of a Framework Service contract

The contract value without this being binding for ENISA is limited to **four hundred and seventy thousand Euros (€470,000.00) over a maximum possible period of 4 years**[3], for all services requested in this tender.

It is emphasized that a maximum of ninety thousand Euros (€90,000.00) shall be assigned to ‘Web Hosting services’ over the maximum 4-year period - including the costs of the one-off ‘Migration’.

(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(s) in order to increase the maximum amount stated above by up to 50%. This procedure being fully in accordance with Article 134(e) of the Rules of Application (RAP) implementing the EU Financial Regulation (FR)).

17. DATA PROTECTION

Personal contact information will normally be professional contact data only, so no special confidentiality requirements are envisaged.

Regarding personal data, the following EU data protection regulations have to be respected:

[3] conditional upon extension of the Agency’s mandate which currently ends on 18 June 2020

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
2. Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;
3. Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

18. 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 office should be attained 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.

19. 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.

20. PRICE REVISION

Prices provided in the Financial Offer (Annex III) must be fixed and not revisable for the first year of the contract. From the second year of the contract prices may be revised as specified in the draft framework contract.

21. 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.

22. 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.

23. PROTOCOL ON PRIVILEGES AND IMMUNITIES OF THE EUROPEAN COMMUNITIES

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 Communities.

Tenderers must therefore give prices which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

24. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out within 30 days after an invoice is submitted to ENISA. Payments will be made after receipt and approval of the ordered services by ENISA. Each invoice must specify the specific services covered as per the relevant purchase order.

The 'e-Invoicing Web Portal' of the European Commission shall be used for submitting invoices. Use of this web portal requires the creation of an EU Login (ECAS) account to gain access.

For the 'hosting services' which will be ordered under a yearly Specific Contract, it is anticipated that an invoice will be issued by the contractor on a quarterly basis in arrears and in 4 equal instalments.

In other words, the first invoice, for a quarter of the total yearly amount for 'hosting services', will be due 3 months following the countersignature of the Specific Contract (under the Framework Service contract) by both parties.

While there is the possibility for negotiation on the abovementioned terms of payment, the Agency would prefer adherence to the stated terms.

25. CONTRACTUAL DETAILS

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

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

The tender will conclude, valid as of the date of the last signature, with a 12-month Framework Service contract, tacitly renewable three times for a further 12 months - in total a maximum of 4 years. (conditional upon the Agency's mandate).

The Agency reserves the right to end the contract at any time, without any obligation to invoke the reason for it, at one months' notice.

The Tenderer's offer must be drafted taking fully into account the provisions of the draft Framework Service contract annexed to this call for tenders (See draft contract, in Annex IV).

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

PART 3 TENDER SPECIFICATIONS

1. FORMAL REQUIREMENTS

1.1 Address and deadline for submission of the Tender:

You are invited to tender for this project and requested to submit your bid no later than **Friday 16th June 2017 by**:

a) Electronic means ONLY:
Your completed offer, including all signed documentation, to be scanned and sent as PDF files (or similar) by **email attachment**, and sent exclusively to:

tenders-F.SRAD.17.T28@enisa.europa.eu
Attention: The Procurement Officer

In order to ensure secure reception, the 'Subject' field of the email must contain the following text:

Tender offer - F-SRAD-17-T28 Web Hosting and Development services

***If your email file is quite large due to the attachments, it is recommended to split any attachments into files no larger than **9 - 10MB** each and spread over more than one email. In this case please add the following text to the 'Subject' field of each email:

Tender offer - F-SRAD-17-T28 Web Hosting and Development services (*nn of Tnn*)

If you have any questions regarding this procedure or clarifications are required, then please send them to our general procurement section email account **only**:
procurement@enisa.europa.eu

The **last date & time** for acceptance of offers is **strictly:**

Friday 16th June 2017 at 15:00 CEST - Central European Summer time.

Please note that late despatch will lead to exclusion from the evaluation and award procedure for this Contract.

The successful contractor may be required to send the original offer documents by courier/postal service to ENISA before any contract can be signed. Further documentary proof of financial and economic standing may also be required to be presented before contract signature.

1.2 Presentation of the Offer and Packaging

Offer to be sent by electronic means only as set out in article 1.1 above.

1.3 Identification of the Tenderer

Tenderers are required to complete the **Legal Entity Form (see Annex I)** which must be signed by a representative of the Tenderer authorised to sign contracts with third parties. There is one form for 'individuals', one for 'private entities' and one for 'public entities'. A standard form is provided for

each category - please choose whichever is applicable. In addition to the above, a **Financial Identification Form (see Annex I)** must be filled in and signed by an authorised representative of the Tenderer and his/her bank (or a copy of the bank account statement instead of bank's signature). An **Administrative Identification and Declaration form (Annex V)** must also be completed for internal administrative purposes.

1.4 Participation of consortia

Consortia, may submit a tender on condition that it complies with the rules of competition. The 'Power of Attorney for Consortium Form' (Annex VI) must be completed and submitted with your offer.

A consortium may be a permanent, legally-established grouping or a grouping which has been constituted informally for a specific tender procedure. Such a grouping (or consortia) must specify the company or person heading the project (the leader) and must also submit a copy of the document authorising this company or person to submit a tender. All members of a consortium (i.e., the leader and all other members) are jointly and severally liable to the Contracting Authority.

1.5 Subcontracting

In well justified cases and subject to approval by ENISA, a contractor may subcontract parts of the services. The 'Sub-contractors Form' (Annex VII) must be completed and submitted with your offer.

Contractors must state in their offers what parts of the work, if any, they intend to subcontract, and to what extent (% of the total contract value), specifying the names, addresses and legal status of the subcontractors.

The sub-contractor must not sub-contract further.

Where no sub-contractor is given, the work will be assumed to be carried out directly by the bidder.

1.6 Signatures of the Tender

Both the technical and the financial offer must be signed by the Tenderer's authorised representative or representatives (preferably in blue ink).

1.7 Total fixed price

A total fixed price expressed in Euro must be included in the Tender. The contract prices shall be firm and not subject to revision for the first year.

1.8 Language

Offers shall be submitted in one of the official languages of the European Union (preferably in English).

2. GROUNDS FOR EXCLUSION OF TENDERERS

2.1 Reasons for Exclusion

Candidates or tenderers shall be excluded from participation in a procurement procedure if:

a) They are bankrupt or being wound up, are having their affairs administered by the courts, have entered into an arrangement with creditors, have suspended business activities, are the subject of proceedings concerning those matters, or
b) Are in any analogous situation arising from a similar procedure provided for in national legislation or regulations;

c) They have been convicted of an offence concerning their professional conduct by a judgement which has the force of res judicata;

d) They have been guilty of grave professional misconduct proven by any means which the contracting authority can justify;

e) They have not fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which they are established or with those of the country of the contracting authority or those of the country where the contract is to be performed;

f) They have been the subject of a judgement which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;

g) Following another procurement procedure or grant award procedure financed by the Community budget, they have been declared to be in serious breach of contract for failure to comply with their contractual obligations.

Tenderers must certify that they are not in one of the situations listed in point 2.1 (see Annex II: Declaration on Honour on exclusion criteria form). If the tender is proposed by a consortium this form must be submitted by each partner.

2.2 Other reasons for not awarding the Contract

Contracts may not be awarded to Candidates or Tenderers who, during the procurement procedure:

a. Are subject to a conflict of interest;

b. Are guilty of misrepresentation in supplying the information required by the contracting authority as a condition of participation in the contract procedure or fail to supply this information;

c. Any attempt by a Tenderer to obtain confidential information, enter into unlawful agreements with competitors or influence the evaluation committee or ENISA during the process of examining, clarifying, evaluating and comparing tenders will lead to the rejection of his offer and may result in administrative penalties.

See last paragraph point 2.1.

2.3 Confidentiality and Public Access to Documents

In the general implementation of its activities and for the processing of tendering procedures in particular, ENISA observes the following EU regulations:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;
- Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

3. ASSESSMENT AND AWARD OF THE CONTRACT

The assessment will be based on each tenderer's bid. All the information will be assessed in the 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 successive stages.

The aim of each of these stages is:

1) to check on the basis of the ***exclusion criteria***, whether tenderers can take part in the tendering procedure;
2) to check on the basis of the ***selection criteria***, the 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 one step will pass on to the next step

3.1 EXCLUSION CRITERIA

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

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

The successful tenderer shall be asked to provide the documents mentioned as supporting evidence in Annex II 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 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.

3.2 SELECTION CRITERIA

The following criteria will be used to select the Tenderers. If the Tender is proposed by a consortium these criteria must be fulfilled by each partner.

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

3.2.1 Professional Information

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

3.2.2 Financial and Economic Capacity

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

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

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

(b) A statement of the average turnover of the last two (2) financial years for which accounts have been closed. The **minimum annual <u>average</u> turnover** of the tenderer shall be of **100,000.00 EUR**. 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 100,000.00 EUR.

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 request for clarification <u>before</u> the tender expiry date.

3.2.3 Technical and professional capacity

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

A detailed description of the resources (hardware & software) to be made available for this contract, subject to the contractual clause on subcontracting;

- Curriculum Vitae (CV) of the project manager and other staff related to the provision of services requested;
- Quality control and assurance methodology;
- List of the main <u>hosting services</u> performed in the past 3 years, with details of the values, dates and public or private recipients enclosing, where possible, documents concerning reliability and efficiency of the services performed issued by the beneficiaries of the service;
- List of the main <u>development services</u> performed in the past 3 years based on the Plone platform as well as other platforms, with details of the values, dates and public or private recipients enclosing, where possible, documents concerning reliability and efficiency of the services performed issued by the beneficiaries of the service.

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 on the basis of the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	**Technical compliance**	Compliance with the technical requirements (Part 2 of this document)	40/100
2.	**Quality and accuracy of content and structure**	Quality of the proposal and accuracy of the description to provide the requested services. Quality of scenario solutions offered.	30/100
3.	**Project Team**	Proposed team dedicated to the services and project management.	30/100
Total Qualitative Points (QP)			**100**

Minimum attainment per criterion

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

Minimum attainment overall

Offers scoring less than 60% after the evaluation process will be considered to be of insufficient quality and eliminated from the following phase.

The sum of all criteria gives a total of 100 points. The respective weighting between the different award criteria depends on the nature of the services required and is consequently closely related to the terms of reference. 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

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

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

$$P_B = [(P_{HC} / P_{HT}) \times 20] + [(P_{SC} / P_{ST}) \times 40] + [(P_{DC} / P_D) \times 40)]$$

where:

P_H = Hosting cost
P_M = Migration cost
P_D = Web Development consolidated cost (P_1 +P_2 + P_3 + P_4 + P_5 + P_6)
P_{DC} = Cheapest P_D
P_{ST} = Total Scenario cost (S_1 + S_2 + S_3 + S_4)
P_{SC} = Cheapest P_{ST}
P_{HT} = Hosting and Migration cost (P_H + P_M)
P_{HC} = Cheapest P_{HT}

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

3.3.3 Award of the contract

The contract will be awarded to the offer which is the most cost effective (offers the best value for money) which obtains the highest number of points after the final evaluation on the basis of the ratio between the **quality criteria (70%) and the price ratio (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 ratio
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 20th June 2017 at 10:30 EEST Eastern European Summer (Greek) time at ENISA Athens office, 1 Vasilissis Sofias Street, Maroussi 151 24 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 3 working days** prior to the opening session. Failing that, the contracting authority reserves the right to refuse access to its premises.

5. OTHER CONDITIONS

5.1 Validity

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

5.2 Lots

This Tender is not divided into Lots.

5.3 Additional Provisions

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

5.4 No obligation to award the contract

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

6. SPECIFIC INFORMATION

6.1 Timetable

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

Title: "**Provision of Web Hosting and (Plone) Web Development services"**

ENISA F-SRAD-17-T28

Summary timetable comments

Launch of tender: Contract notice to the Official Journal of the European Union (OJEU) Uploaded to e-Tendering website and ENISA website	**5th May 2017**	
Deadline for request of information to ENISA	9th June 2017	
Last date on which clarifications are issued by ENISA	13th June 2017	
Deadline for **electronic submission** of offers to the nominated email account	**16th June 2017**	**15:00 CEST** **Central** European time
Opening of offers	20th June 2017	**10:30 EEST** **Eastern** European Summer (Greek) time
Date for evaluation of offers	TBA	TBA
Notification of award to the selected candidate + 10 day standstill period commences	Early July 2017	Estimated
Contract signature	Mid July 2017	Estimated
Commencement date of activities	As per tender	Estimated
Completion date of activities	As per tender	Estimated