European University Institute

INFORMATION AND COMMUNICATION TECHNOLOGY SERVICE

Technical Specifications, Selection and Award Criteria - Lot 2

Technical Specifications for consulting services in the field of Information Security with the European University Institute

OP/EUI/ICTS/2020/03/LOT 2

YEAR 2020

Summary

CHAPTER I – DESCRIPTION OF REQUIRED SERVICES

1. Description of Services

The object of this tender procedure is to identify, within the Framework Contract Agreement, a company for the security consultancy; suppliers will provide the EUI with strategic, technological knowledge and expertise in the information security domains such as cloud and digital services security, security architecture, security of website and web services, defensive and offensive security. These services also include security assessments, elaboration of studies (e.g. benchmarking), and contribution to security architecture, support in security incidents, fine tuning of specific security technologies and digital forensics.

With the Framework Contract Agreement for Information Security consultancy services, the EUI intends to strengthen the security of various technologies, improve the resilience of EUI infrastructure, network, system and applications as well as to address cyber risks. The services will be requested with the corresponding request of services under this framework agreement.

The provisioning of consultancy for the development, testing and implementation of advanced technical solutions require the knowledge of the following **security technologies**:

- SPLUNK log management
- Intrusion detection system (CISCO FirePower)
- Microsoft Windows Defender Advance Threat Protection
- Microsoft Office 365 Security services
- Microsoft Azure Security
- Amazon Web Services Security
- Akamai security services
- Web application firewall
- Vulnerability assessment tools
- Digital forensic tools
- Network security

The technical support requires the knowledge of the following **IT technologies**:

- Microsoft Windows 10 and Windows server versions
- Apple iOS and Mac OS
- Lamp Stack (Linux, Apache, MySQL, Perl, PHP e/o Python)
- Microsoft Office 365
- Microsoft Azure Cloud
- Amazon Web Services

Due to the international nature of the EUI, every written communication and most of the meetings that will require the involvement of the appointed system experts, will be held in English. For this reason, it is strictly required for the technical personnel to have a sound knowledge of the English language, both spoken and written.

1.1. Consultancy services

The consultancy services will be provided on premise or from remote by various technical professional profiles with a demonstrated experience. The activities will take place in the office made available by Data Security Officer (DSO), currently located at Villa Il Poggiolo, Piazza Edison 11, during office hours (9 am to 6 pm) under the supervision and collaboration of Data Security Officer.

As to simplify the operations scheduling and planning, when possible the activities will be planned well in advance (normally two weeks before).

Outside office hours activities might be requested when necessary. No additional compensation is foreseen for consultancy services provided “Off-hours” but a conversion of worked hours spent in activities performed during “off-hours” hours and regular office hours will be performed. The Company is therefore requested to specify a conversion rate of “off-hours” hours into regular office hours (e.g. “3 hours of activities performed during “off-hours” is equivalent to 5 hours of activities performed between 9 am and 6 pm”). See Annex II-F_Vacation-Days-2020.

CHAPTER II – SPECIFIC SELECTION CRITERIA

2. Skills and qualifications: requirements for the service personnel of consultancy service

Essential requirements:

The following minimum requirements will be requested, with no exception, to the personnel involved in the service activities and execution:

- Deep knowledge of Information security
- Good knowledge of the English language (written and spoken)
- For Senior security consultant, at least 8 years of demonstrated experience in the role supporting the security technologies indicated in the profile.
- For Security consultant, at least 5 years of demonstrated experience in the role supporting the security technologies indicated in the profile.

Advantageous requirements: the following qualifications and certifications are considered optional but they will be considered in the evaluation process:

- Security certifications issued by ISACA, (ISC)2
- Security certifications issued by IT vendors such as Microsoft, Cisco, AWS, or security vendors (e.g. CompTIA, TrendMicro, etc...)
- English language certifications or qualifications

The achievement of desired organization objectives requires the following profiles:

Senior Security consultant

- A Senior Security consultant has a specific expertise in offensive\defensive security and security architectures. He/she holds relevant professional certifications and a Computing or Information technology degree or equivalent professional expertise. The consulting services will be offered by a team of experts, the Security consultant has some of the following competencies in the information security field:
- Deep knowledge of security monitoring (Splunk and IDS) and search for Indicator of Compromise (IoC)
- Good knowledge of security architectures
- Good knowledge of securing network, remote connections, wireless and wired networks
- Good knowledge of Office 365 security services and web security (both on-premises and in the cloud)
- Expert knowledge of PKI and digital certificate management
- Expert knowledge of conducting vulnerability assessments on applications, websites and technologies on premises
- Expert knowledge of conducting Vulnerability assessments of Internet facing applications and websites running in the cloud including Microsoft Azure and Amazon Web Services
- Expert knowledge of conducting security audit and security assessment of applications, websites, network infrastructure and technologies
- Good knowledge of Auditing source code for security vulnerabilities
- Expert knowledge of performing forensic analysis in case of investigation, malware and data breach
- Deep knowledge of conducting penetration tests against networks, websites and cloud resources

Security consultant

A Security consultant has an expertise and hands-on in the technologies to perform security incident analysis and to detect, identify and respond to attacks. He/she holds professional certifications from IT vendors and a level of education to provide an effective contribution. The consulting services will be offered by a team of experts, the Security consultants have some of the following competencies in the information security field:

- Deep knowledge of Incident response (on-premises) being able to collect relevant data in case of Phishing and cyber-attacks and to perform root cause analysis.
- Deep knowledge of Incident response in the cloud including Microsoft Azure and AWS.
- Good knowledge of phishing, spear-phishing and malware identification and eradication.
- Expert knowledge to interpret alerts and to assess the severity of threats and escalating

3. Skills and qualifications: suppliers' requirements of consultancy service

Essential requirements

The following minimum requirements will be requested, with no exception, to the company providing the service activities and execution:

- ISO 9001 Certification
- ISO 27001 Certification

Technical and professional capacity criteria and evidence

Supplier must comply with the following selection criteria in order to prove that they have the necessary technical and professional capacity to perform the contract.

The Supplier must prove experience in the field of Information security:

- Offensive and defensive security, digital forensics and incident response in the Cloud (including private, public and hybrid infrastructures).
- IT Security: design, implementation, management and operation of security services, security procedures, security monitoring, detecting and handling of security events.
- Cloud security: design, implementation, management and operation of security capabilities and Incident response in private, public and hybrid cloud computing environments.
- Minimum level capacity. The Supplier should demonstrate at minimum five relevant references:
  - The delivery of security consulting and projects in the last 3 years
  - Project's total contract value at least of 50,000 (fifty thousand euro) for the technologies mentioned above
  - Project's client: organisation/institution/company with over 10 staff members in total
  - Provide evidence mentioning Client name, project period, indicative amount and reference person. (We reserve the right to verify the information before finalising the tender award)

Advantageous requirements. Listed, by way of example but not limited to, any additional elements that the Supplier may highlight in the technical offer as an added value to the standard supply of requested services.

CHAPTER III – SPECIFIC AWARD CRITERIA

4. Assigning Points for Technical and Qualitative aspects of the Service

In evaluating the technical and qualitative aspects of the offered service, the Evaluation Committee, at its own discretion, shall use the scores shown in **Table 1**, the maximum sum of which is equal to 70.

According to the level of adequacy and conformity requested in this STS, the Evaluation Committee shall assign a scoring between **0** and **70**.

Each technician proposed by the Company will be evaluated according to the scores defined in **Table 1** (from **A1** to **A7**) and has to obtain always at least the minimum score for each requirement, on pain of exclusion. The total score will consist in the average of the points obtained by each evaluated technician.

Companies that will offer more than one technician to be evaluated might obtain a higher score in section **A8** in case all the proposed technicians obtain a score higher than **39** points in the "qualifications of support personnel" section of Table 1. Companies not obtaining the minimum score in **A8** section will be rejected from this tender.

Table 1 – Technical and Qualitative aspects scoring			
Description		**Min. Score**	**MAX. Score**
	Qualifications of support personnel		
A1	Knowledge of security monitoring (Splunk and IDS)	**5**	**10**
A2	Knowledge of Office 365 security services and web security (both on-premises and in the cloud)	**5**	**10**
A3	Knowledge of conducting vulnerability assessments	**5**	**10**
A4	Knowledge of conducting security audit and assessments	**5**	**10**
A5	Knowledge of performing forensic analysis	**5**	**10**
A6	Information Security certifications	**2**	**6**
A7	Knowledge of the English language	**2**	**4**
	Qualifications of the Company		
A8	Technical and professional capacity criteria and evidence	**5**	**10**

Maximum score for the parameter **A** is **70**:

A = (**A1**+**A2**+**A3**+**A4**+**A5**+**A6**+**A7**+**A8**) = **70**

As far as **Table 1** criteria are concerned, coefficients shall be assigned according to the following **Table 2**

Table 2 - Quality coefficients

Evaluation	Description	Coefficient
Excellent	Requirements, knowledge, certifications and previous experience are of a very high level, providing added value with respect to the Contracting Authority's expectations. As a guidance, the following evaluation criteria will be applied: **Qualifications of support personnel (Table 1 A1-A7)** **Essential requirements**: Exceed expectations presenting team members with more years of demonstrated experience in the role than required. **Advantageous requirements:** Presenting team members that have one or more of the qualifications and certifications indicated. **Qualifications of the Company (A8)** **Company's certification**: Meet the essential requirements **Technical and professional capacity criteria and evidence**: **Valuable team**: Presenting a team composition covering all required competencies (also indicating the number of consultants composing the team) and showing the redundancy of team's members with more than two Senior security consultants and two security consultants holding the key competences, experience and seniority required. **Company's capabilities:** Exceed the minimum requirements such as the number of projects run in the last three years, or bigger project's size. **Advantageous requirements** Working across different sectors and for institutions and international organisations such as EUI. Showing expertise in handling complex information security incidents and data breaches.	**1,00**
Good	Requirements, knowledge, certifications and previous experience exceed expectations. As a guidance, the following evaluation criteria will be applied: **Qualifications of support personnel (Table 1 A1-A7)** **Essential requirements**: Meet expectations presenting team members with demonstrated experience in the role as required. **Advantageous requirements:** Presenting team members that have one or more of the qualifications and certifications indicated. **Qualifications of the Company (A8)** **Company's certification**: Meet the essential requirements **Technical and professional capacity criteria and evidence**:	**0,75**

	Valuable team: Presenting a team composition covering all required competencies (also indicating the number of consultants composing the team) and showing the redundancy of team's members with more than one Senior security consultant and one security consultant holding the key competences, experience and seniority required. **Company's capabilities:** Meet the minimum requirements such as the number of projects run in the last three years, or alternatively less projects of bigger size. **Advantageous requirements** Working across different sectors and/or for institutions and international organisations such as EUI. Showing expertise in handling complex information security incidents and data breaches.	
Satisfactory	Requirements, knowledge, certifications and previous experience are in line with what was foreseen in the STS. As a guidance, the following evaluation criteria will be applied: **Qualifications of support personnel (Table 1 A1-A7)** **Essential requirements**: Meet expectations presenting team members with demonstrated experience in the role as required. **Advantageous requirements:** Presenting team members that have at least one security certifications among those indicated. **Qualifications of the Company (A8)** **Company's certification**: Meet the essential requirements **Technical and professional capacity criteria and evidence**: **Valuable team**: Presenting a team composition covering all required competencies (also indicating the number of consultants composing the team) and showing the redundancy of team's members with more than one Senior security consultant and one security consultant holding the key competences, experience and seniority required. **Company's capabilities:** Meet the minimum requirements such as the number of projects run in the last three years, or alternatively less projects of bigger size. **Advantageous requirements** Showing expertise in handling complex information security incidents and data breaches.	**0,50**
Poor	Requirements, knowledge, certifications and previous experience are partially unsatisfactory As a guidance, the following evaluation criteria will be applied: **Qualifications of support personnel (Table 1 A1-A7)** **Essential requirements**: Meet the minimum requirements presenting team members with demonstrated experience in the role as required. **Advantageous requirements:** None are met.	**0,25**

	Qualifications of the Company (A8) **Company's certification**: Meet the essential requirements **Technical and professional capacity criteria and evidence**: **Valuable team**: Presenting a limited team composition without being able to cover all required competencies and without the redundancy of team's members with more than one Senior security consultant and one security consultant holding the key competences, experience and seniority required. **Company's capabilities:** The minimum requirements are not met concerning the number of projects run in the last three years. **Advantageous requirements:** No indications or the Company is focused only in one sector (not including Academic institutions or International organisations).	
Unsatisfactory	Requirements, knowledge, certifications and previous experience are completely inadequate. As a guidance, the following evaluation criteria will be applied: The essential requirements in one of the following categories are not met: **Qualifications of support personnel (Table 1 A1-A7)** **Qualifications of the Company (Table 1 A8)**	**0,00**

Once the tender is awarded, the successful Technical Offer becomes an integral part of the STS and of the Contract.

5. Assigning Points for Economic Aspects of the Service

In evaluating the economic aspects of the offered service, the Evaluation Committee, shall use the scores shown in **Table 3**, the maximum sum of which is equal to **30**.

Table 3		
Description of the Service		**MAX Points**
B1	**Senior Security consultant** per hour rate - ON SITE (Standard operation - 8 hours a day)	**10**
B2	**Senior Security consultant** per hour rate - REMOTE	**4**
B3	**Security consultant** per hour rate - ON SITE (Standard operation - 8 hours a day)	**10**
B4	**Security consultant** per hour rate - REMOTE	**4**
B5	**Conversion Ratio** between hours worked in "off-hours" (from 6 pm to 9 am) and hours worked in office hours (from 9 am to 6 pm) e.g. 1 ("off-hours") equal to 1,5 (Office Hours)	**2**

Maximum score for the parameter **B** is **30**:

B = (**B1**+**B2**+**B3**+**B4**+**B5**+**B6**) = **30**

The maximum score achievable of **B1** for the price **P** (**10 points**) will be awarded to the Tenderer who offers the best price for the "hour of on-site" consultancy (lowest price). The other companies will be awarded different scores (rounded off to the second decimal figure, if necessary) calculated in proportion to the ratio between the best price and the price offered by each Tenderer.

The following formula will be applied:

$$B1 = 10 \times \frac{\text{Best price}}{\text{Price offered}}$$

where P = points (score) awarded to the offer.

The maximum score achievable of **B2** for the price **P** (**3 points**) will be awarded to the Tenderer who offers the best price for the "hour of remote consultancy" (lowest price). The other companies will be awarded different scores (rounded off to the second decimal figure, if necessary) calculated in proportion to the ratio between the best price and the price offered by each Tenderer.

The following formula will be applied:

$$B2 = 4 \times \frac{\text{Best price}}{\text{Price offered}}$$

The maximum score achievable of **B3** for the price **P** (**5 points**) will be awarded to the Tenderer who offers the best price for the "hour of on-site" consultancy (lowest price). The other companies will be awarded different scores (rounded off to the second decimal figure, if necessary) calculated in proportion to the ratio between the best price and the price offered by each Tenderer.

The following formula will be applied:

$$B3 = 10 \times \frac{\text{Best price}}{\text{Price offered}}$$

where P = points (score) awarded to the offer.

The maximum score achievable of **B4** for the price **P** (**3 points**) will be awarded to the Tenderer who offers the best price for the "hour of remote consultancy" (lowest price). The other companies will be awarded different scores (rounded off to the second decimal figure, if necessary) calculated in proportion to the ratio between the best price and the price offered by each Tenderer.

The following formula will be applied:

$$B4 = 4 \times \frac{\text{Best price}}{\text{Price offered}}$$

As far as **B5** score is concerned, a proportion between the conversion ratio proposed by each Company and the most advantageous conversion offer received will be made, assigning 2 points according to the obtained coefficient.

$$B5 = 2 \times \frac{\text{Proposed Conversion Ratio}}{\text{Best Proposed Conversion Ratio}}$$

Example:
Company A: 1 hour worked in Off-Hours = 2 hours worked in office hours.
Proposed ratio 1:2 = 0,5
Company B: 1 hour worked in Off-Hours = 1 hour worked in office hours.
Proposed ratio 1:1 = 1
B3 Score for Company A = 2 x (0,5/1) =1
B3 Score for Company B = 2 x (1/1) = 2

For the economic evaluation each company will be requested to fill in the economic offer form (**Annex II-E-2**).