



INFORMATION AND COMMUNICATION TECHNOLOGY SERVICE

**Open Procedure for the provision of consulting
services on identity and access management for the
European University Institute**

Ref: **OP/EUI/ICTS/2026/002**

YEAR 2026

Contents

CHAPTER I – SCOPE AND DESCRIPTION OF THE PROCUREMENT PROCEDURE.....	3
Article 1. Definitions.....	3
Article 2. Contracting authority	3
Article 3. Subject	3
Article 4. Conditions for participation to tender.....	4
Article 5. Joint Tenders.....	4
Article 6. Subcontracting	4
CHAPTER II – TECHNICAL SPECIFICATIONS	5
Article 7. Description of the technical specifications	5
Article 7.1 Consultancy services	6
Article 7.1.1 Skills and qualifications of the contractor’s personnel	6
Article 7.2 Technical support services.....	7
CHAPTER III – EVALUATION AND AWARD CRITERIA.....	8
Article 8. Exclusion criteria	9
Article 9. Selection criteria.....	10
Article 10. Award criteria	11
CHAPTER IV - FINAL PROVISIONS	15
Article 12. Requirements for the signature of the contract.....	15
Article 13. Contract management.....	15
Article 14. List of tender documents	15

CHAPTER I – SCOPE AND DESCRIPTION OF THE PROCUREMENT PROCEDURE

Article 1. Definitions

‘candidate’ means an economic operator that has sought an invitation;

‘contract’ means a public contract awarded by the EUI for the procurement of services/supply;

‘EUI’ or ‘the Institute’ means the European University Institute, which is the contracting authority entrusting the services that are the subject of these tender specifications to the contractor;

‘contractor’ means to the successful tenderer awarded with the contract;

‘economic operator’ can refer to a ‘work contractor’, ‘supplier’, or ‘service provider’ and means any natural or legal person or public entity or group of such persons and/or entities which offers the execution of works, the supply of products or the provision of services on the market;

‘joint tenders’ means a situation where a *tender* is submitted by a group (with or without legal form) of economic operators regardless of the link they have between them. The group as a whole is considered a *tenderer*¹;

‘subcontracting’ means the situation where the *contractor* enters into legal commitments with other *economic operators* which will perform part of the *contract* on its behalf. The *contractor* retains full liability towards the *EUI* for performance of the *contract* as a whole;

‘tender’ / ‘offer’ defines the terms upon which the supplier is willing to be bound, which normally include price, date of delivery, payment terms and a description of the services/supplies/works;

‘tenderer’ means an economic operator that has submitted a tender;

‘tender specifications (TS)’ means any documents describing the needs and requirements of the EUI for the purposes of the relevant tender.

Article 2. Contracting authority

This procurement procedure is launched and managed by the *EUI*, that is the contracting authority for the purposes of this procurement procedure, through the **Information and Communication Technology Service (ICTS)**.

Article 3. Subject

Subject of the contract	The subject of this procurement procedure is the provision of consulting services on identity and access management for the European University Institute .
Lots	This procurement procedure is not divided into lots .
Type of contract	The procedure will result in the conclusion of a multiple framework contract in cascade . <i>Tenderers</i> need to take full account of the provisions of the draft <i>contract</i> as the latter will define and govern the contractual relationship(s) to be established between the <i>EUI</i> and the <i>contractor(s)</i> .

¹ References to tenderer or tenderers in this document shall be understood as covering both sole tenderers and groups of economic operators submitting a joint tender.

Duration of the contract	The framework <i>contract</i> to be awarded shall have a duration of 5 years . The details of the initial <i>contract</i> duration and possible renewals are set out in Article I.2 of the draft <i>contract</i> .
Estimated value of the contract	The estimated value of the framework <i>contract</i> to be awarded for the whole duration of 5 years is €250.000,00 (two hundred fifty thousand/00) VAT excluded . These volumes are estimates only and there is no commitment as to the exact volumes of the services to be ordered. The actual volumes will depend on the specific services which the <i>EUI</i> will order through specific <i>contracts</i> or <i>order forms</i> .
Place of performance	The services will be undertaken at the contractor's premises and the EUI's premises .

Article 4. Conditions for participation to tender

If you are interested in this *contract*, you should submit a *tender* in one of the official languages of the European Union (with preference for the use of English) provided you comply with the conditions for participation to tenders as set out in Article 3.4 of President's Decision n. 24/2025 of 6 May 2025 implementing title V concerning procurement of the EUI's Financial Rules (Public Procurement Regulation), available for consultation at: <https://www.eui.eu/en/public/about/procurement/tenders-regulatory-framework>.

Article 5. Joint Tenders

In case of *joint tender*, all members of the group assume joint and several liability towards the *EUI* for the performance of the *contract* as a whole.

Group members must appoint a Group leader, and a single point of contact authorised to act on their behalf in connection with the submission of the *tender* and all relevant questions, clarification requests, notifications, etc., that may be received during the evaluation, award and until the *contract* signature.

The *joint tender* must clearly indicate the role and tasks of each member and of the Group leader who will act as the *EUI's* contact point for the *contract's* administrative or financial aspects and operational management. The Group leader will have full authority to bind the group and each of its members during *contract* execution. If the *joint tender* is successful, the *EUI* shall sign the *contract* with the Group leader, authorized by the other members to sign the *contract* on their behalf via power of attorney.

Changes in the composition of the group during the procurement procedure (after the submission deadline and before *contract* signature) shall lead to rejection of the *tender* except in case of a merger or takeover of a member of the group (universal succession), provided that the new entity has access to procurement (see Article 4) and is not in an exclusion situation, (see Article 8).

In any case the selection criteria must be still fulfilled by the group and the terms of the originally submitted *tender* may not be altered substantially, i.e. all the tasks assigned to the former entity must be taken over by the new entity member of the group, the change must not make the *tender* non-compliant with the *tender specifications*, and the evaluation of award criteria of the originally submitted *tender* may not be modified.

Article 6. Subcontracting

All contractual tasks may be subcontracted unless the *tender specifications* expressly reserve the execution of certain critical tasks to the sole *tenderer* itself, or in case of a *joint tender*, to a member of the group.

Tenderers are required to give an indication of the proportion of the *contract* that they intend to subcontract in the technical offer, as well as to identify and describe briefly the envisaged contractual roles/tasks of *subcontractors* meeting the following conditions (hereafter referred to as identified *subcontractors*):

- are not in one of the exclusion situations listed in Article 8;
- on whose capacities the *tenderer* relies upon to fulfil the selection criteria as described under Article 9;
- whose individual share of the *contract*, known at the time of submission, is above 20 %.

Any such *subcontractor* must provide the *tenderer* with a commitment letter signed by its authorised legal representative.

Changes concerning *subcontractors* identified in the *tender* (withdrawal/replacement of a *subcontractor*, additional subcontracting) during the procurement procedure (after the submission deadline and before *contract* signature) require the prior written approval of the *EUI* subject to the following verifications:

- any new *subcontractor* is not in an exclusion situation;
- the *tenderer* still fulfils the selection criteria and the new *subcontractor* fulfils the selection criteria applicable to it individually, if any;
- the terms of the originally submitted *tender* are not altered substantially, i.e. all the tasks assigned to the former *subcontractor* are taken over by another involved entity, the change does not make the *tender* non-compliant with the *tender specifications*, and the evaluation of award criteria of the originally submitted *tender* is not modified.

Subcontracting to *subcontractors* identified in a tender that was accepted by the *EUI* and resulted in a signed contract, is considered authorised.

CHAPTER II – TECHNICAL SPECIFICATIONS

Article 7. Description of the technical specifications

The aim of this procurement procedure is to award a framework contract for the provisioning of consultancy and technical support services for the development, testing and implementation of advanced technical solutions using, among others, the following IAM and PAM technologies currently in use at the *EUI*:

- Knowledge of One Identity - family products, including Identity Manager,
- Knowledge of One Identity (Safeguard) and Privileged Access Suite for UNIX.

The One Identity platform has been in use at the *EUI* for several years and is fully integrated with authoritative sources such as Human Resources and Academic systems.

Furthermore, One Identity provides interfaces and workflows that feed identity and access information into multiple target systems, including Microsoft Entra ID/M365, on-premises directories, and business applications.

In view of the above, with the aim of maintaining operational continuity and avoiding unnecessary redevelopment costs or service risks, the contractor shall ensure full

compatibility with the existing One Identity environment and shall design any deliverables to operate seamlessly within the IAM architecture currently in use.

The contractor must have proven experience in Identity and Access Management, particularly in identity security, identity governance, privileged access management, business analysis, and business development. The following qualifications and certifications will be considered in the evaluation process:

- Having, or having started the process to have, a direct support channel with One Identity, with the possibility of escalating to the highest level in the case of necessity.
- Completed or started the One Identity Manager Certification Process.

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

Article 7.1 Consultancy services

The consultancy services will be provided on-premises or remotely by various technical profiles. The activities will take place in a specific office located at the EUI premises in Florence, during office hours (9 am to 6 pm), under the supervision of the Director of the Information and Communication Technology Service.

The consultancy services will be assigned with priority to the economic operator that ranks first in the cascade, by issuing specific order forms.

To simplify operations scheduling and planning, when possible, activities will be planned well in advance (normally 2 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" slots and regular office hours will be performed. The contractor is therefore requested to specify a conversion rate of "off-hours" slots into regular office hours (e.g. "3 hours of activities performed "off-hours" is equivalent to 5 hours of activities performed between 9 am and 6 pm").

Article 7.1.1 Skills and qualifications of the contractor's personnel

The achievement of desired organisational objectives requires a team of **Cybersecurity Technical Analysts** with varying levels of seniority and specialisations.

Tasks: These are the tasks needed for technical studies, usually executed by a blended team with profiles that bring technical analysis capability, technological expertise, and the ability to manage customer relationships and projects.

Typical composition: Typically, but not exclusively, composed of the following profiles to drive and execute the requested tasks: IAM specialist, IAM Architect, Cybersecurity Technology Expert, Business analyst, and Project Manager.

Activities: Analysis of business and technical requirements, detailed technical assessments of services' and solutions' architectures, security, compliance, and risks, evaluation of resource requirements, drafting implementation plans, preparation of documents and delivery of analysis results.

Specific expertise requirements:

- Knowledge of operational models in the Identity and Access Management and cybersecurity field, knowledge of Identity and Access Management and Privilege Access management processes and supporting tools. Ability to draft structured technical and architectural documents. Practical knowledge of applicable standards and regulations (notably, cybersecurity and data protection). Estimate the efforts and resources needed to deliver service and mobilise resources to implement and deploy services according to an agreed plan.
- Expert knowledge and integration of Microsoft Active Directory and AD Azure, Entra ID, Oracle Database, SQL database.
- Expert knowledge and good command of use of connectors with Microsoft Active Directory, Entra ID, Exchange on-premises and Exchange Online; coding and configuring cloud apps and API keys.

Seniority level: The minimum qualifications per seniority levels are Junior, Confirmed and Senior:

- ❖ **Junior:** post-secondary education of at least 2 years is mandatory in the specific areas defined above, and a minimum required professional experience of 2 years in the field. Good understanding of the on-premises and cloud contexts.
- ❖ **Confirmed:** post-secondary education of at least 2 years is mandatory in the specific areas defined above, and a minimum required professional experience of 6 years in the field. Good understanding of the on-premises and cloud contexts. Holding one or two specific certifications in the IAM\PAM areas.
- ❖ **Senior:** Bachelor's degree of 3 years or more; master's degree or PHD in specific areas defined above per profile or in other equivalent areas. (Subject to the acceptance of the Contracting Authority). 12 years of experience in the profile and excellent knowledge of the understanding of the on-premises and cloud contexts. Holding one or two specific certifications in the IAM\PAM areas.

Certifications:

➤ Cybersecurity Technical Analysts certifications:

The Cybersecurity Technical Analysts proposed by the Tenderer must hold at least some of the following certifications for Technical Analyst in the One Identity area:

- One Identity Identity Manager Implementation
- One Identity Identity Manager Instructor Led Training
- One Identity Identity Manager – Technical Specialist
- One Identity Safeguard – Technical Specialist

Any additional certifications in project management and cybersecurity will constitute an advantage.

➤ Company certifications

As part of the evaluation process, the Partner Circle Tiers will be assessed based on competency and contribution, including Registered, Silver, Gold, and Platinum, as well as Product-Based Partner Certification.

Article 7.2 Technical support services

The support service will be delivered according to the following Service Level Agreement – Terms and conditions:

The service is provided from Monday to Friday, working time 9 am to 6 pm (EUI opening calendar weeks based on its [2026 public holidays and closure days](#)).

The service requires daily checks on IAM systems and solving issues related to the IAM products:

- Daily checks should be conducted to ensure the IAM infrastructure is properly running.
- Take charge the request for intervention to solve problems:
 - blocking issues should be acknowledged within 4 hours
 - non-blocking issues is acknowledged on the Next business day

The Service must be ensured on specific days, such as:

- Onboarding of newcomers: day 1 and 16 of the month.
- Deprovisioning of leavers: day 16 and the end of the month.
- Onboarding Academic newcomers: mid-July yearly.

The technical support service will be assigned on an annual basis, taking into account the start of the framework contract and the beginning of each year covered by the contract, to the economic operator that ranks first in the cascade, by issuing an *ad hoc* order form.

The support should be provided by a Cybersecurity Technical Analyst skilled in the One Identity product family with the knowledge and expertise to maintain the development, test, and Production server infrastructure and application layers, including connectors.

CHAPTER III – EVALUATION AND AWARD CRITERIA

The evaluation of the *tenders* that comply with the submission conditions will consist of the following elements:

- Check if the *tenderer* has access to procurement (see Article 4);
- Verification of administrative compliance (if the *tender* is drawn up in one of the official EU languages and signed by duly authorised legal representative(-s) of the *tenderer*);
- Verification of non-exclusion of *tenderers* on the basis of the exclusion criteria;
- Selection of *tenderers* on the basis of selection criteria;
- Verification of compliance with the minimum requirements defined in the tender specifications;
- Evaluation of *tenders* on the basis of the award criteria.

The *EUI* will evaluate the abovementioned elements in the order that it considers to be the most appropriate. If the evaluation of one or more elements demonstrates that there are grounds for rejection, the *tender* will be rejected and will not be subjected to further full evaluation. The unsuccessful *tenderers* will be informed of the ground for rejection without being given feedback on the non-assessed content of their *tenders*. Only *tenderer(s)* for whom the verification of all elements did not reveal grounds for rejection can be awarded the *contract*.

The evaluation will be based on the information and evidence contained in the *tenders* and, if applicable, on additional information and evidence provided at the request of the *EUI* during the procedure. If any of the declarations or information provided proves to be false, the *EUI* may impose administrative sanctions (exclusion or financial penalties) on the entity providing the false declarations/information.

For the purposes of the evaluation related to exclusion and selection criteria the *EUI* may also refer to publicly available information, in particular evidence that it can access on a national database free of charge.

Article 8. Exclusion criteria

The *tenderer* must not be in one of the exclusion situations listed below:

- a. is bankrupt or being wound up, is having their affairs administered by the courts, has entered into an arrangement with creditors, has suspended business activities, are the subject of proceedings concerning those matters, or is in any analogous situation arising from a similar procedure provided for in national legislation or regulations;
- b. has been convicted of an offence concerning their grave professional conduct by a final judgment of a competent judicial authority or administrative decision or decisions of international organisations;
- c. is not in compliance with the 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 Italy being the country of establishment of the *EUI* or those of the country where the contract is to be performed. This breach needs to have been established by a judgment or administrative decision having final and binding effect in accordance with the legal provisions of the country in which the economic operator is established or of those of Italy being the country of establishment of the *EUI*;
- d. has been the subject of a final judgment for fraud, corruption, involvement in a criminal organisation, money laundering, terrorist-related offences, child labour or other forms of trafficking in human beings or any other illegal activity, where such illegal activity is detrimental to the *EUI*'s financial interests;
- e. has been in serious breach of a contract financed by the *EUI* or have been the subject of an offense of serious irregularity established by a final judgment of a competent judicial authority or administrative decision;
- f. is subject to an administrative penalty for being guilty of grave professional misconduct, or of having made substantial errors or committed irregularities or fraud or have been declared to be in breach of their obligations under contracts covered by the *EUI*'s budget (Article 41 of the *EUI*'s Public Procurement Regulation ([President's Decision No.24/2025 of 6th May 2025](#))).

In addition to the above, *contracts* cannot be awarded to a *tenderer* who, during the procurement procedure, is proven to be:

- g. subject to a conflict of interest in connection with the *contract* which cannot be effectively remedied by other less intrusive measures;
- h. guilty of misrepresentation in supplying the information required by the *EUI* as a condition of participation in the *contract* procedure or fail to supply this information;
- i. has created a shell company;
- j. is a shell company.

Evidence requested:

The *tenderer* must certify that it is not in one of the exclusion situations by providing in the *tender* a signed and dated Declaration on Honour available in Annex II A.

In addition, the successful *tenderer* shall provide, within 15 days following notification of award and preceding the signature of the *contract*, the following documentary proofs to confirm the declaration referred to above:

- for points (a), (b), (d), (e), (i) and (j): a recent extract from the judicial record of the legal representative of the *economic operator* that submitted the *tender* or, failing that, an equivalent document recently issued by a judicial or administrative authority in the country of origin or provenance showing that those requirements are satisfied;
- for the situation described in point (c) above, recent certificates or letters issued by the competent authorities of the State concerned are required. These documents must provide evidence covering all taxes and social security contributions for which the *tenderer* is liable, including for example, VAT, income tax (natural persons only), company tax (legal persons only) and social security contributions.

For any of the situations (a), (b), (d), (e), (i) or (j), where any document described in the paragraph above is not issued in the country concerned, it may be replaced by a sworn or, failing that, a solemn statement made by the interested party before a judicial or administrative authority, a notary or a qualified professional body in his country of origin or provenance.

The *EUI* reserves the right to verify the information and to request further supporting evidence prior to the signature of the *contract*.

In the event that the successful *tenderer* does not promptly execute the fulfilment of the above, fails to present all documentation requested or does not provide proof of possession of all requirements declared in the *tender*, as well as if any checks reveal failure of compliance with the declarations submitted during the tendering period, the *EUI* reserves the right to declare a compliance failure and to award the procedure to the following *tenderer* in the list or to launch a new procurement procedure.

Article 9. Selection criteria

General requirements:

The *tenderer* must have the following minimum requirements to perform the *contract*:

- a) being compliant with obligations relating to the payment of social security contributions for workers, according to the current legislation, and application of employment conditions envisaged in the sector's national collective labour agreement;
- b) being compliant with the current labour laws and regulations;
- c) being compliant with the current health and safety laws and regulations;
- d) being compliant with the current environmental laws and regulations;

Economic and financial capacity:

- e) having generated a minimum annual turnover in the last 3 (three) financial years for which accounts have been closed of at least €100.000,00 (one hundred thousand/00).
- f) having a risk indemnity insurance policy.

Technical and professional requirements:

- g) being authorised to perform the contract under national law, as evidenced indicatively by inclusion in a trade or professional register, or a sworn declaration or certificate, membership of a specific organisation, or entry in the value added tax (hereinafter 'VAT') register.
- h) a team composed of Cybersecurity Technical Analysts with different levels of seniority, such as Junior, Confirmed and Senior, holding expertise in the IAM and PAM areas.
- i) providing a list of 3 Identity Access Management relevant projects executed in the last 3 years (2023-2024-2025) having a value of at least €100.000,00 (one hundred

thousand/00), concerning an organisation/institution/company with over 1.000 (one thousand) staff members in total.

- i. Please specify for each project: sector (private or public), project period, and indicative amount (the EUI reserves the right to ask for a reference person or additional information before signing the contract).

❖ **Evidence to be submitted with the tender as part of Envelope n.1 – Administrative Documents (please, for more details on the submission process, see point 3 of the letter of invitation to tender):**

- a signed and dated Declaration on Honour available in Annex II A.
- a document (e.g. financial statements) attesting that the *tenderer* had a minimum annual turnover in the last 3 (three) financial years for which accounts have been closed of at least €100.000,00 (one hundred thousand/00).
- a copy of a risk indemnity insurance policy.
- evidence that the *tenderer* is included in a trade or professional register and entry in the value added tax register.
- list of 3 Identity Access Management relevant projects executed in the last 3 years (2023-2024-2025) having a value of at least €100.000,00 (one hundred thousand/00), concerning an organisation/institution/company with over 1.000 (one thousand) staff members in total:
 - specifying per each project: sector (private or public), project period, indicative amount.

Each one of the members making up the group and/or consortium must possess the selection criteria from a) to d), g), while all the others must be possessed by the group as a whole.

The *EUI* reserves the right to perform sample checks in order to verify the accuracy of the statements submitted by *tenderers*.

Tenderers that are not compliant with the applicable minimum requirements shall be rejected.

Article 10. Award criteria

Only the *tenders* submitted by *tenderers* meeting the requirements of the exclusion and selection criteria will be evaluated in terms of quality and price. The *contract* shall be awarded according to the “**most economically advantageous tender**” criterion, following the assessment of the best quality/price ratio made by the competent evaluation committee, which will assign a score to each *tender* to a maximum of 100 points, based on the following parameters:

MAXIMUM SCORE	
Technical and quality evaluation	70/100
Financial evaluation (price)	30/100

The total score of the *tender* shall be the sum of the technical and financial score obtained.

The *tenderer* obtaining the highest overall score shall be awarded with the *contract*.

A - Allocation of points for technical and quality evaluation criteria

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

For the technical evaluation, each tenderer will be required to fill in the technical offer form (Annex II B).

Tenders not obtaining the minimum score established for each criteria A, B and C, as indicated in Table 1 below, shall be rejected from this procurement procedure.

TABLE 1 – Technical evaluation					
DESCRIPTION				MINIMUM SCORE	MAXIMUM SCORE
A	Competences and qualifications of the Tenderer			22.5	45
	A1	Identity Access Management		7.5	15
		A1.1	Experience in the field of Identity Access Management, especially about identity governance, privileged access management and business development	N/A	5
		A1.2	Direct support channel - process completed = 5 points - process started = 1 point	N/A	5
		A1.3	One Identity Manager Implementation Certification Process - process completed = 5 points - process started = 1 point	N/A	5
	A2	Implementation of Business Processes		7.5	15
		A2.1	Proposal to establish a catalogue of administrative applications and services to request access providing an estimate of time and resources	N/A	5
		A2.2	Proposal of an approval workflow granting access to a new target (one authoritative source and one target) providing an estimate time and resources (the target within EUI infrastructure)	N/A	5
		A2.3	Proposal of Segregation of Duties Matrix for the financial area mentioning units and roles providing an estimate time and resources	N/A	5
	A3	Privileged Access Management		7.5	15
		A3.1	Proposal to create privileged credentials linked to the users' credentials providing an estimate of time and resources (on-premises and Entra ID)	N/A	5
		A3.2	Proposal for real time risk rating on accumulated access rights providing an estimate time and resources	N/A	5
		A3.3	Proposal for integrating all critical Linux servers with a central identity service (e.g., LDAP/AD/Entra ID/IdM) to ensure secure privileged access management, enforce individual accountability, and implement centralised authentication, authorisation, logging and least-privilege access controls	N/A	5
B	Competences and Qualifications of Tenderer' support personnel: Cybersecurity Technical Analyst - Junior			7.5	15

	○ (please submit only 2 CVs without including name, surname, age and nationality of the person proposed) • Cybersecurity Technical Analyst - Confirmed ○ (please submit only 2 CVs without including name, surname, age and nationality of the person proposed)			
	B1	Knowledge of One Identity product family; Integration with Microsoft Active Directory and AD Azure; Integration with database (Oracle/SQL)	N/A	10
	B2	Possession of technical certifications from the list included in Art. 7.1.1 TS - Cybersecurity Technical Analysts certifications	N/A	5
C	Technical support services proposed by the Tenderer in accordance with Art. 7.2 of these TS		<u>5</u>	<u>10</u>

The maximum score for criteria **A+B+C** is **70 points**, and the **minimum is 35 points**.

As far as sub-criteria A1.1, A2.1, A2.2, A2.3, A3.1, A3.2, A3.3, B1 and B2 are concerned, the following judgements and corresponding coefficients included in Table 2 below shall be used for assigning the scores.

TABLE 2 Quality coefficients to be assigned to sub-criteria A1.1, A2.1, A2.2, A2.3, A3.1, A3.2, A3.3, B1 and B2		
JUDGEMENT	DESCRIPTION	COEFFICIENT
EXCELLENT	<i>The tender exceeds the requirements set up by the tender specifications</i>	1.00
GOOD	<i>The tender partly exceeds the requirements set up by the tender specifications</i>	0.75
SUFFICIENT	<i>The tender meets the requirements set up by the tender specifications</i>	0.50
POOR	<i>The tender partly meets the requirements set up by the tender specifications</i>	0.25
INSUFFICIENT	<i>The tender does not meet the requirements set up by the tender specifications</i>	0.00

As far as criterion C is concerned, the following judgements and correspondent coefficients included in Table 3 below shall be used for assigning the scores.

TABLE 3 Quality coefficients to be assigned to criterion C		
JUDGEMENT	DESCRIPTION	COEFFICIENT
EXCELLENT	<i>The tenderer proposes:</i> – a response time (blocking) within 1 hour. – a response time (not blocking) within 2 hours. – 2 daily checks + proactive monitoring.	1.00

GOOD	<i>The tenderer proposes:</i> – a response time (blocking) within 2 hours. – a response time (not blocking) within 4 hours. – 2 daily checks.	0.75
SUFFICIENT	<i>The tenderer proposes:</i> – a response time (blocking) within 4 hours. – a response time (not blocking) within next business day. – 1 daily checks.	0.50
INSUFFICIENT	<i>The tenderer proposes:</i> – a response time (blocking) exceeding 4 hours. – a response time (not blocking) exceeding next business day. – Less than daily checks.	0.00

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

B - Allocation of points for financial evaluation criteria

For the financial evaluation, each tenderer will be required to complete the financial offer form (Annex II C).

In evaluating the financial aspects of the tender submitted, the Evaluation Committee shall use the scores shown below in **Table 4**, with a maximum total (**D criterion**) of **30 points**.

D = (D1+D2+D3+D4+D5+D6) = 30 points.

Table 4 – Financial evaluation				
Description of the services to be quoted				MAX Points 30
D1	Cybersecurity Technical Analyst – Junior			5
	D1.1	On Site (Standard operation - 8 hours a day)	3	
	D1.2	Remote	2	
D2	Cybersecurity Technical Analyst – Confirmed			5
	D2.1	On Site (Standard operation - 8 hours a day)	3	
	D2.2	Remote	2	
D3	The implementation of Business processes			5
D4	Privileged Access management			5
D5	Cybersecurity Technical Analyst – Junior - Full Time Equivalent This role should address second level support requests and exceptions interacting with internal stakeholders and ensuring provisioning and timely removal of access.			5

D6	Technical support services - REMOTE (availability from Monday to Friday 09 am to 06pm) (refers to Art. 7.2 of these TS)	5
-----------	---	----------

The **maximum score** achievable for price will be awarded to the tenderer who offers the **best price for the provision of consultancy service or service** (lowest price). The following formula will be applied to each criterion included in Table 4 reported above:

$Dx = Y \times \frac{\text{Best (Lowest) price offered}}{\text{Price offered}}$

Dx = any D criteria established in Table 4.

Y = any breakdown score of the maximum score established in Table 4.

The other tenderers 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.

CHAPTER IV - FINAL PROVISIONS

Article 12. Requirements for the signature of the contract

The successful tenderer, within the date to be communicated by the EUI, must submit the following documents before the signature of the contract:

- a copy of the full criminal record of the legal representative of the successful tenderer.
- the non-disclosure agreement related to the protection of personal data as provided for by the applicable rules of the [EUI Data Protection Policy](#), that will be provided in due time by the EUI to the successful tenderer.

Please be aware that any employee of the successful tenderer who is involved in the implementation of the contract with the EUI must return to the contracting authority such agreement duly filled and signed.

- Declaration of compliance with Annex II D – AI Tools, Supply Chain and IAM Clause.

Please note that should the successful tenderer fail to submit the documents outlined above in due time or, upon testing, is found not to be in compliance with the declarations submitted in the tender, the EUI reserves the right to award the contract to the following tenderer in the ranking or to launch a new call for tender.

Article 13. Contract management

For the *EUI*, the reference person(s) for the *contract* management is/are the following:

- the Director of the Information and Communication Technology Service.

Article 14. List of tender documents

The tender documents of the present procurement procedure are composed of the draft contract, the invitation letter, these *tender specifications* - TS (Annex I) and the contractor's *tender* (Annex II), including the following annexes:

- Annex II A – Declaration on honour;
- Annex II B – Technical *offer*;
- Annex II C – Financial *offer*;
- Annex II D – AI Tools, Supply Chain and IAM Clause.
 - Annex II D is included in the tender documents for transparency purposes as it shall be submitted to the signature of the contractor before proceeding with the signature of the contract to be awarded.