Executive Summary

Annex I

Call for Tenders

Common Shared Infrastructure

LISA/2016/RP/01

(Restricted Procedure – Article 104 (1) (b) Financial Regulation,

Article 127 (2) paragraph 2 Rules of Application)

Table of Contents

I. VOCABULARY

Abbreviation	Description
BCU	Backup Central Unit
BMS	Biometric Matching System
CBS	Core Business System
CfT	Call for Tender
CMA	Common Management Area
COTS	Commercial Off-The-Shelf
CS	Central System
CSA	Common Services Area
CSI	Common Shared Infrastructure
CU	Central Unit
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
EURODAC	European Asylum Dactyloscopy Database
EUWS	End User Workstation
FwC	Framework Contract
HP	Hewlett Packard
ITSM	Information Technology Service Management
LIS	Large IT Scale Systems
MS	Member State
NOP	Non-Operational Platform
NTP	Network Time Protocol
NS	National States
PPE	Pre-Production Platform
PRD	Production Platform

SIS II	Schengen Information System
SM9	HP Service Manager 9
SMTP	Simple Mail Transfer Protocol
s-TESTA	Secure Trans European Services for Telematics between Administrations
TESTA-ng	Trans European Services for Telematics between Administrations – new generation
VIS	Visa Information System
WAN	Wide Area Network
WP	Work Package(s)

II. CONTEXT OF THE CALL FOR TENDERS

II.1. Background

II.1.1. eu-LISA

The European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is a relatively newly established agency (Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 (OJ L 286, 1.11.2011, p.1) which entered into force on 21 November 2011.

The agency's sites are distributed as follows: the headquarters are based in Tallinn, Estonia, whilst its operational centre is in Strasbourg, France. There is also a business continuity site for the systems under management based in Sankt Johann im Pongau, Austria.

The Agency is set up in the form of an independent European body (Regulatory Agency). Its core mission is to fulfil the operational management tasks for the systems SIS II, VIS and EURODAC. The main operational responsibility is to ensure that these systems are 24/7 available and functioning according to specifications. Other responsibilities include adopting the necessary security measures, ensuring data security and integrity, as well as compliance with data protection rules.

II.1.2. Operational responsibility of IT Systems

According to its legal mandate, eu-LISA is operationally responsible for three (3) Large-Scale IT Systems (LIS), governed by a legal basis which defines, among others: the business, the governance and the security rules.

Each LIS is operated by eu-LISA on behalf of the Member States (MS) and the services are provided by eu-LISA to the MS' National System (NS). End-users of each MS are connected to their NS which relays their requests to the Central System (CS).

These LIS's are:

- SISII: Schengen Information System II, a highly efficient large-scale information system that supports external border control and law enforcement cooperation in the Schengen States
- VIS: Visa Information System, which allows Schengen States to exchange visa data
- EURODAC: Related to asylum seekers, making it easier for EU States to determine responsibility for examining an asylum application by comparing fingerprint datasets.

From a technical point of view these systems are being hosted on a dedicated IT infrastructure ('silo' approach) and are thus considered as Core Business Systems (CBS). A CBS is a logical unit that provides a service to the MS (i.e. SIS, VIS, EURODAC) or to another CBS (i.e. Biometric Matching System (BMS)).

In this context, a fourth CBS, namely BMS is supporting VIS by offering verification and identification searches.

Related to the topology, SISII, VIS and EURODAC are delivering services to Member States (MS) and thus are connected to them via a dedicated WAN (Wide Area Network) operated by an external provider, while BMS is delivering its services to VIS and thus locally interconnected with VIS.

It is likely that a number of other systems will be entrusted to the management of the agency in the years to come (subject to the adoption of the relevant legal bases). In addition, the agency is also operationally responsible for the communication networks that support the above systems. In terms of networks, eu-LISA is technically responsible for the communication infrastructure for SIS II, Eurodac and VIS (the Secure Trans European Services for Telematics between Administrations network (s-TESTA) — to be migrated to a new Secure Trans European Services for Telematics between Administrations – new generation network (TESTA-NG) in 2016), as well as their respective consultation mechanisms.

II.1.1. Operational sites

eu-LISA is hosting its core business services in an active-passive datacentre approach. The main datacentre is located in Strasbourg, France and is referenced to as the CU (Central Unit). The datacentre in Sankt Johann im Pongau, Austria is a dedicated passive datacentre (hot standby), further referenced to as the BCU (Backup Central Unit). The BCU is a copy of the CU and business data is replicated between the two environments. IT staff and contractors are located in Strasbourg.

II.1.2. Description of current technical infrastructure and existing architecture

eu-LISA is responsible for the operation of the CBS but also for their maintenance (evolutive, corrective and adaptive). In this context, two distinct and physically separated IT infrastructures (also called platforms) are used:

- Operational platform (OP)
    - **Production environment (PRD)**
        - Present in CU and BCU
        - Application data and application logs inside the database are replicated between both sites
        - Only accessed by eu-LISA staff
- Non Operational Platform (NOP)
    - **Pre-production environment (PPE)**
        - Clone of the production environment
        - Does not contain production data
        - Present in the CU and BCU
        - Only application data and application logs inside the database are replicated between both sites
        - Accessed by eu-LISA & contractor staff (only on-site) and Member States
    - **Other environments**
        - Multiple environments (test, training, playgrounds …)
        - Present only in CU
        - Accessed by eu-LISA & contractor staff (only on-site) and Member States

The development environment located at the contractors premises during the design phase may be considered as a fourth environment. However, eu-LISA has no access to these environments.

More information on eu-LISA can be found at the following link: http://www.eulisa.europa.eu/

III. CALL FOR TENDERS PRESENTATION

III.1. Scope of the Call for tenders

To ease the administration and operation of the shared technical services, eu-LISA is aiming to centralize and simplify all technical services, and to create a new Common Shared Infrastructure (CSI) to be used by the Core Business Systems (CBSs) or other Shared Applications.

The purpose of the Call for Tender (CfT) is to conclude a Framework Contract (FwC) with the future contractor for the provision of IT services, to implement a Common Shared Infrastructure covering the work packages list as described in the section "III.3 – List of Work Packages" and according to technical specification described in detail in Tender Technical Specifications (TTS) document.

III.2. Types of Work Packages

The Framework Contract (FwC) will cover three main types of work packages:

- Maintenance
- Shared Services Implementation
  - Hardware delivery and installation
  - Virtual Environment Configuration
  - Software delivery and integration
  - Evolutionary work packages
- Hand-over

III.3. List of Work Packages

Work Packages (WP) are covering:

a) Specific maintenance activities

b) Implementation of known, specified technical services

c) Implementation of identified and foreseen but not yet specified technical services

d) Hand-over related activities.

This is not a mandatory list and not all services might be implemented; other work packages might be identified and requested to be implemented by the Contractor during the contract.

For the known, specified work packages, Contractor will provide specific offers and estimations, as for the foreseen but not yet specified or unforeseen work packages, the Contractor will estimate the effort based on man-day and hardware & software quotations.

Hereafter is a non-exhaustive list of work packages to be implemented under the framework contract.

- WP of type "Maintenance"
  - Existing End User WorkStation (EUWS)
  - Existing HP SM9 Service Manager
  - Existing Backup Infrastructure
- WP of type "Shared Services Implementation"
  - WP of sub-type "Hardware delivery and installation"

- Hardware Installation related to shared infrastructure

- WP of sub-type "Virtual Environment Configuration"
  - Backup of Common Shared Area
  - Monitoring of Common Shared Area
  - Creation of Virtual Farm environment
- WP of sub-type "Software delivery and integration"
  - Mail Services
  - Data warehouse
  - Reporting facilities – Application & Business reporting
  - Technical documentation management
  - Time synchronization
  - Access Management – Personal Access Management
  - Access Management – Privileged Identity Management
  - Identity & Access management
  - Backup Management
  - Unified Threat Management
  - Vulnerability management
  - Key & Certificate Lifecycle Management
  - Endpoint Anti-Malware services
  - Name resolving services
  - IP Address & DNS Management
  - Hardware Management
  - Integrity monitoring
  - Compliance verification
  - Database management
  - Log Management
  - Security Information Management Services
  - Technical Monitoring
- WP of type Hand-Over

III.4. Detailed description of the work packages

III.4.1. Maintenance work packages

The maintenance work packages aim at allowing existing shared infrastructure and services to provide the expected level of quality as defined in the Technical Specifications.

Maintenance will be provided by the Contractor on existing environments/infrastructures defined and located on the premises of the Operations Centre of the Agency in Strasbourg (CU) and of the Backup site of the Agency (BCU - Sankt Johann im Pongau, Salzburg). Remote access for maintenance of the Central Unit (CU) or Backup Central Unit (BCU) will not be accepted under this contract.

The major aim of these services is to correct and adapt as necessary the existing shared infrastructure and services.

- **Corrective and adaptive maintenance**

The maintenance services requested cover mainly the activities of corrective and adaptive maintenance defined as following:

- Corrective maintenance consists of reacting to the anomalies noticed during the operation of the system, by implementing their correction or temporary bypass measures (to be followed by a final correction). The technical follow-up of an anomaly is ensured by an anomaly report;
- Adaptive maintenance consists of updating the configuration of the hardware equipment and the software products of the system in order to keep them in line with the technical support guaranteed by their suppliers.

More precisely, the adaptive maintenance aims to:

- Adapt the technical environment and systems, in order to maintain them in a "state of guaranteed availability";
- Maintain the quality of the services delivered by this system, by anticipating the end of the support of the hardware, firm-wares, operating system, software products (COTS, including Open Source software) and applications, as well as the problems arising from the obsolescence of certain components of the system.

"State of guaranteed availability" indicates:

- That the system in production, and other environments, must be constantly maintained in good working order, according to the specifications;
- That this system must work according to the high availability criteria defined in the SLA and relevant Quality Indicators;
- That for the duration of the contract, all the hardware and software which are under the responsibility of the Contractor, must be subject to maintenance in conformity with the conditions of the Tender Technical Specifications (TTS).

"To maintain the quality of services delivered by the system" means:

- That the Contractor must be able to demonstrate at any time that his services and deliverables enable the system to provide a quality of service at least equal to the requirements made in the TTS;
- That the Contractor alone is the only party responsible for any malfunction or degradation in the quality of service arising from a modification made by him to the system, and in any such case will be responsible for any complementary maintenance (including the software or equipment updates not planned otherwise) needed to remedy any malfunction or degradation; exception made of modifications solely decided by eu-LISA.

III.4.2. Shared Services Implementation

Implementation of technical shared services is covered by four main activities:

- Hardware delivery and Installation
- Virtual environment Configuration
- Shared Services Delivery and Integration
- Evolutionary Work Packages

III.4.2.1. Hardware delivery and Installation

Installation and configuration of needed equipment will need to take place in the premises of the Operations Centre of the Agency (Strasbourg) (CU), and also in the Backup site of the Agency (Sankt-Johann im Pongau, Salzburg) (BCU) .

As an enabler of building the shared technical infrastructure, the physical layer of the infrastructure must be put in place in the beginning.

The Contractor will need to deliver, install and configure the specific hardware equipment needed to build the shared technical infrastructure, in conformity with specific architectural, functional and technical requirements foreseen and expressed in the Tender Technical Specifications (TTS) document.

III.4.2.2. Virtual environment configuration

The Contractor, making use of the infrastructure described in Chapter "III.4.2.1 – Hardware delivery and Installation" will fully install and configure the virtual environment and all associated services in order to enable the full deployment of future work packages, as they were mentioned above in Chapter "III.3 - List of Work Packages", without being an exhaustive or mandatory list.

III.4.2.3. Shared Services delivery and Integration

Under the coverage of the Framework Contract, the Agency will be able to demand the Contractor to implement the technical shared services through different work packages as are listed in the Chapter "III.3– List of Work Packages".

The order of implementation cannot and shall not be considered the one in which the Work Packages are previously listed, and is subject of technical constraints, as described in the Tender Technical Specifications document.

Implementation of the services must comply at least with the minimum, specific requirements as are expressed in the Tender Technical Specifications and its annexes in terms of architecture requirements and performance.

All the platforms and technical environments which are covered by the FwC needs to be implemented in both operational locations of the Agency - CU and BCU, the ones in BCU being a 1:1 copy of the ones existing in CU.

III.4.2.4. Evolutionary work packages

Evolutionary work packages will be used by the Agency during the FwC to request the Contractor to implement either unforeseen services, or foreseen, but not yet specified services.

For these specific work packages, the Contractor will use the fixed priced or QTM estimation methodology to estimate the effort for implementation.

III.4.3. Hand-Over

Hand-over corresponds to the transfer or the preparation of the transfer of a system to another organization that will take the work over.

At the end of the contractual period, or earlier on request from the Agency, the Contractor will handover to eu-LISA, or any specified third parties on its behalf, in accordance with instructions to be given by the Agency.

The Contractor has to provide a handover report to eu-LISA for review and acceptance at the end of the handover activity.

III.4.4. Description of Work Packages and Shared Services

III.4.4.1. End User Work Stations (EUWS)

EUWS is a common management security zone which is under eu-LISA responsibility and is used to:

- Connect all the workstations necessary for eu-LISA to access, for management purposes, the core business systems.
- Share some common services

There is one dedicated EUWS infrastructure for production platform and one dedicated EUWS infrastructure for pre-production platform.

III.4.4.2. HP SM9 Service Manager

HP SM9 is the ITSM tool used by eu-LISA to quickly and efficiently handle incident, problem and change management while bringing together a broad range of ITSM capabilities. It allows eu-LISA to have an improved interface for MS users and represents also a stable basis for reporting and process measurements.

III.4.4.3. Backup Infrastructure

It is represented by the existing physical infrastructure which is used for backing-up systems and Common Shared Services Area.

III.4.4.4. Hardware delivery and installation

It is the process of installation and configuration of physical infrastructure according to the requirements defined in the TTS. This infrastructure needs to be put in place in order to be able to install and configure the Virtual Environment.

III.4.4.5. Virtual Environment Configuration

It is the process of installation and configuration of Virtual Environment on top of the hardware equipment previously installed.

The Virtual Environment will be the environment used later to implement the shared services in the scope of the current CfT.

It will comprise the installation, migration and configuration of following:

- Backup of Common Shared Area
- Monitoring of Common Shared Area
- Creation of Virtual Farm environment

III.4.4.6. Mail Services

The implemented mail services allow messages to be passed both between Member States and between eu-LISA and Member states.

Mail Transfer Agent is software used to transfer email messages from one computer to another. The most common protocol used is Simple Mail Transfer Protocol (SMTP).

III.4.4.7. Data Warehouse, Reporting facilities - Application & Business reporting

Data warehousing encompasses the aggregation of data from multiple sources in a single, homogenized structure allowing creation of business meaningful reports and overviews targeted at piloting the business evolution and resource arbitration. Data warehousing comes with the challenges of controlling the aggregation in order to allow data incoming from sources with heterogeneous security constraints to produce useful strategic or tactic data while respecting their own security constraints.

The data warehouse is used to centralize all data from the different Core Business Systems.

III.4.4.8. Technical Documentation Management

Technical documentation focusses on the system specific configuration documentation. How it is maintained, where it is stored and who has access to it.

On the market, Documentation Management Systems are typically referred to as enterprise content management systems (ECM).

III.4.4.9. Time synchronization

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems. Within the structure of the CBS's and the split between CU and BCU it is of utmost importance that the local time on the servers is the same.

III.4.4.10. Access Management - Personal Access Management

Access management is the combination of the processes, the tooling and the governance required to allow users and systems to make use of IT Services, data or other assets in a manner that is in line with an entity security policies and rules.

III.4.4.11. Access Management - Privileged Identity Management

Privileged identity management is focused on managing generic privileged account credentials. Typically these solutions provide the following functionalities – automated management of password and keys, managing and monitoring privileged sessions, workflows, etc.

III.4.4.12. Identity & Access management

The purpose of the Access Management process is to define the activities as well as the relevant responsibilities and provide a structured way of managing the logical accounts creation, revocation, modification and the periodic review and maintenance of the Systems' accounts. It also provides guidance regarding the password handling and password sharing.

III.4.4.13. Backup Management

Backup, or the process of backing up, refers to the structured copying and archiving of computer data in order to be able to use it to restore the original data after a data loss, data corruption or human error.

Backups have two distinct purposes. The primary purpose is to recover data after its loss, be it by data deletion or corruption. The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy.

III.4.4.14. Unified Threat Management

Unified Threat Managements (UTM) refers to a single device consolidating a large catalogue of security services. This reduces the number of devices needed, while increasing flexibility and ease of deployment: security services can be activated and tweaked from the same management console. Typical security services an UTM provide are: firewalling, proxy-services, IDS/IPS, URL filtering, Data Loss Prevention, VPN, Botnet scanning, and Identity Awareness.

III.4.4.15. Vulnerability management

Vulnerability management focusses on the tools and processes used in order to have an overview of the vulnerabilities existing within a CBS. Vulnerability management is common for all CBS's.

III.4.4.16. Key & Certificate Lifecycle Management

Typically a key management service ensures all keys are identified, documented and managed.

To allow certificates and keys to be monitored, they must be known. This solution supports synchronization with a Certificate authority, to allow the issued certificates to be monitored on the individual systems.

III.4.4.17. Endpoint Anti-Malware services

Anti-malware is the service that delivers malware prevention, detection and handling capabilities. The goal of using such a service within the network is to limit the possibility of executing malicious software on the systems.

III.4.4.18. Name resolving services

Name resolving services also known as Domain Name Service (DNS) allows the translation of the fully qualified domain names into IP addresses and vice versa.

III.4.4.19. IP Address & DNS Management

IP address management is the management of the internet protocol addresses used in the entire network. This service will communicate with the DHCP servers.

III.4.4.20. Hardware Management

Hardware management is about having a universal view on the hardware specifications of all hardware components involved in a CBS. HP SM9 uCMDB solution is in use within eu-LISA.

III.4.4.21. Integrity monitoring

The goal of integrity monitoring is to have an overview of unauthorized changes affecting the IT systems and the hosted data.

III.4.4.22. Compliance verification

Compliance verification is the process, undertaken on a recurrent basis, to analyses the different systems within a network and their settings. A comparison is made between the agreed upon

configurationally values and their actual implementation in order to discover if the system settings strays from configurationally values agreed upon during the design phase.

III.4.4.23. Database management

Database management is all about how administrators are able to connect to and manage the business supporting Oracle databases and the infrastructure and management supporting ones.

Non business supporting databases are not actively supported by eu-LISA staff as they do not require maintenance.

III.4.4.24. Log Management

Log management comprises an approach to dealing with large volumes of log messages (also known as audit records, audit trails, event-logs, etc.) and covers log collection, centralized aggregation, log analysis, etc.

III.4.4.25. Security Information Management Services

The current monitoring and log management implementations are de-centralized and do not provide correlation of events. Consequently, it is up to the security administrator to find the events which fit together to identify a security incident. The SIEM service should

- Provide an overlay of the log management to correlate the necessary security events together to identify incidents.
- Provide the ability to store events and incidents on the long term
- Provide the ability to correlate events to a pre-identified threat scenario

III.4.4.26. Technical Monitoring

Technical Monitoring evaluates all systems and applications in place in order to have a real time overview of all technical and application events generated within the IT environment.

III.5. Other Generalities

III.5.1. Service Desk

The Contractor has to provide a single point of contact (SPOC) for all incident and problem management and for the support of the Agency. Incident and problem management processes will be put in place by the Contractor and must be aligned with the processes implemented at eu-LISA. The Service desk needs to be set up in a way that it can fulfil the requirement of a 24/7 availability and providing the adequate level of response.

III.5.2. Communication

The spoken and written language of all communication will be UK English. All deliverables, reports, drafts etc. must be delivered in English unless otherwise agreed. All meetings will be conducted in English.

III.5.3. Monthly Status Reports

At the beginning of each month, a monthly status report must be sent to the Agency with details of the work carried out in the previous month. The report must also contain a description of the work to be performed in the next month, clearly mentioning the milestones. The monthly report shall also cover team structure, KPI values, hardware and software, value of tangible and intangible assets delivered in the reporting period, problems and issues, risks, budget consumption, planning, action list. A detailed list of the items to be covered in the monthly report status will be defined in the TTS.

III.5.4. Regular meetings

Follow-up, regular and ad-hoc meetings will be setup and organized, in order to report, follow-up or facilitate the implementation of maintenance, project, program and contractual work.

A Steering Committee with the representatives of the Agency and the future contractor will be held quarterly, upon receipt of a Quarterly Status Report from the Contractor.

III.5.5. Quality indicators

The Contractor must respect the quality indicators defined by the Agency. These quality indicators will be defined in detail in the TTS and its specific annexes (i.e. SLA).

All technical services are needed to support 24/7 Core Business Services (SIS, VIS, EURODAC, future business services that may arrive). Taking this into consideration, the general levels of service importance and availability are high, medium and low.

III.5.6. Technical and User Documentation

The Contractor is responsible for the consistency, maintenance and update of the operational, technical and user documentation of shared technical services and all environments within the scope of the call for tender. These documents must be kept updated, respecting the established organization of information and the rules and conventions in place, in order to guarantee the homogeneity of the documentation.

III.5.7. Transversal services

For all the items that will be defined in the TTS, the contractor must foresee at least the following transversal services (non-exhaustive list):

- Program Management
- Project Management
- Quality Management
- Incident Management
- Service Desk/Helpdesk
- Problem Management
- Change Management
- Request Fulfilment Management
- Test Management
- Service Asset and Configuration Management
- Release and Deployment Management
- Service Level Management
- IT Service Continuity Management
- Availability Management
- Capacity Management
- Access Management
- Continuous Service Improvement
- Risk Management;
- Security Management
- Business Continuity
- Contract Management
- Financial Management
- Audibility /Traceability Management
- Hand-over
- Hardware and Software Supplier Contract Management.

The future contractor will be required to fit its own processes to the Agency's operational model, as will be further detailed in phase 2 of the Restricted Procedure.

The future contractor will be required to comply with the rules on data protection and security applicable to the Agency, as will be further detailed in phase 2 of the Restricted Procedure.

It is expected that the Contractor follows-up closely the quality and efficiency of the services delivered by its personnel (independently of the type of service requested) and always anticipate business risks associated to service delivered.

Annex 1 to the Executive Summary – List of Profiles

15 Profiles are defined; each profile corresponds to a minimum level of qualification made up of:

- Minimum level of qualifications and required education degreed relevant for specified profile
- The minimum number of years of professional experience within the previous total.

The minimum level of qualification has to be fulfilled by each person proposed for a given profile. It corresponds to a profile with normal expertise, independently of the technological, languages or other requirements needed for particular tasks.

In complement to the profiles with normal expertise, profiles with specific expertise are defined. They correspond to normal expertise with in addition a minimum number of years of experience in a particular domain indicated in the request (e.g. a technology, a methodology, a tool or a function). This experience must be gained during the years of professional experience (excluding the studies themselves). The total number of years of experience and studies necessary after the secondary school is higher for a profile with specific expertise than for a profile with normal expertise. One single level of specific expertise is defined by profile.

For the implementation of the specific contracts under this Framework Contract, some or all of the following roles may be required:

1. Program Manager
2. Project Manager
3. Senior Enterprise Architect
4. Quality Manager
5. Security Architect
6. Security Manager
7. IT Security Expert
8. Network Architect
9. Network Engineer
10. System and Storage Engineer
11. Test Manager
12. Test Engineer
13. Database Administrator
14. Helpdesk/Service desk staff
15. Training and User Documentation Manager

The minimum requirements set for each profile must be met by the future contractor during the entire duration of the framework contract.

With respect to the below required education qualifications, one year of experience in the relevant domain is considered as equivalent to one year of higher education. However, these years cannot be taken then into account in the experience.

1. Program Manager

Nature of the tasks	• Maintain overall responsibility for the execution of the framework contract; • Report and present to the Steering Committee; • Create and ensure maintenance the Project Quality Plan for the framework contract; • Act as escalation actor for each specific contract; • Provide an answer to eu-LISA Request for Offers, using the commonly agreed template.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 10 years of professional experience in ICT; minimum of 5 years of experience relevant to the requested role; Excellent and established performance managing larger or similar programs.

2. Project Manager

Nature of the tasks	• Report and present to Program Board and participate to the Steering Committee; • Create and ensure maintenance the Project Quality Plan ; • Act as escalation actor for each specific contract; • Provide an answer to eu-LISA Request for Offers, using the commonly agreed template; • Be the Single Point of Contact (SPOC) between all stakeholders of the project for topics related to the framework and each specific contract; • Maintain the Project Quality for the framework contract and ensure alignment with the evolutions of the contract; • Create, maintain and report, following the eu-LISA PM Methodology, the necessary logs of the project: risk log, action log, issue log, lesson learned log. The templates used for this reporting will be provided by eu-LISA's PMO team • Staff the different framework contracts will resources

	that fulfil the requirements laid down by eu-LISA; • Take all the necessary actions to ensure the business continuity of VIS and BMS and the improvement of the delivered services; • Deliver the Monthly Status Reports; • Follow-up and manage the daily activities of the project; • Ensure that all the deliverables will undergo an internal review process prior to submitting to the quality management team of eu-LISA; • Facilitate the specific contract status meetings; • Escalate, when appropriate the issues of a specific contract to the Contractor Project Director. • Ensure that all deliverables from a specific contract are published on the Contractor Knowledge base. • Ensure that the security policies and ITSM processes, aligned with eu-LISA processes, are followed by its team.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 10 years of IT professional experience of which 6 years of experience with a project management methodology (e.g. Prince2). Prince2 Practitioner Certification is as asset. Proven experience with quality procedures.

3. Senior Enterprise Architect

Nature of the tasks	• High-level qualified person able to develop enterprise architecture in line with defined strategy • Define, assess and coordinate architecture projects, design architecture building blocks; • Design and coordinate architecture implementation; • Align and integrate multiple architectures, layers and perspectives; • Advice on architecture frameworks and methods; • Define and measure architecture indicators (maturity, implementation, etc.); • Ensure interoperability; identify potential reuse; perform cost-benefit analyses; design Service Oriented Architecture;

	• Design and assess Identity and Access Management and Master Data Management solutions; • Coordinate the technical implementation; • Perform Business Analysis and contribute to the Functional, Technical, Security and Testing Specifications
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 10 years of IT professional experience; minimum of 5 years of experience relevant to the requested role; certified enterprise architect or equivalent. Experience in business processes modelling. Proven experience with quality procedures.

4. Quality Manager

Nature of the tasks	• Ensure that all processes related to Quality management are set up and maintained; • Maintain all documentation related to quality management; • Support the project team and the customer on all issues related to quality management; • Carrying out quality audits and IT processes quality assessments.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 7 years in the ICT business including 2 years in Quality management, experience in Quality management, quality models, quality assurance (ISO standards or equivalent).

5. Security Architect

Nature of the tasks	• Create and manage design patterns, and reference architectures for the solutions in the scope of this engagement. • Analyse and define security requirements for the solutions in the scope of this engagement • Ensure that the solutions implemented comply with Agency security policies and standards, regulatory requirements and contractual requirements • Work with the Security Officer and IT teams to ensure that implemented security technologies are

	integrated and fully utilized as intended in the protection of agency information systems. • Develop strategic and detailed technical roadmaps of the enterprise security environments and the associated technologies required to deliver these solutions on a global basis. • Develop the business, information and technical artefacts that constitute the enterprise information security architecture and solutions.
Education	University degree (master or equivalent) in a relevant field;
Work Experience	Minimum 6 years of relevant professional experience in IT security or a minimum of 4 years of experience in a Security Architect role. Strong professional knowledge of TOGAF and SABSA. Certified Information Systems Security Professional with Information Systems Security Architecture Professional concentration (CISSP-ISSAP) and Certifications of Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), TOGAF certification is an asset.

6. Security Manager

Nature of the tasks	• Ensure that all processes related to security are set up and maintained; • Support the project team and the customer in areas such as risk analysis, contingency planning, IT security audit, security logs analysis, security development, protection profiles; • Management of the security framework, using standards like ISO 2700x or equivalent.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 7 years of professional in IT, including 5 years in dealing with ICT security issues, experience in carrying out complete security studies of ICT Projects/systems, using standards ISO 2700x, ISO22301 or equivalent;

7. IT Security Expert

Nature of the tasks	• Defining security configuration and operations standards for the solutions in the scope of this engagement. • Develop and validate baseline security configurations for the solutions in the scope of this engagement. • Perform internal and external technical control and vulnerability assessments to identify control weaknesses and assess the effectiveness of existing controls. • Perform source code reviews. • Perform network and application penetration testing (Black box, Grey box and White box). • Defining detailed security architecture for the solutions in the scope of this engagement. • Performing technical security audits. • Perform log analysis and security monitoring. • Perform IT infrastructure/ Application Security configuration reviews. • Design and implement technical security mechanisms and technologies. • Design and develop technical security standards and procedures.
Education	University degree (master or equivalent) in a relevant field;
Work Experience	Minimum 6 years of relevant professional experience in IT Security, of which 4 years of experience in relevant field. Solid professional experience in implementing, managing and maintaining the security solutions covered in the scope of this engagement. Experience with security risk management and tools (e.g. ISO 27000, CRAMM, EBIOS). This profile is expected to possess advanced knowledge of/in: Security best practice guidelines (ISO 27001, NIST, SANS Top 20 OWASP Certified Information Security Manager (CISM) and/or Certified Information Systems Auditor (CISA) is an asset.

8. Network Architect

Nature of the tasks	• Perform network modelling, analysis and planning;

	• Design, test and inspect data communications systems; • Write functional requirements/specifications documents; • Create and document configuration and provisioning parameters, writing technical service specifications for network elements. • Ability to apply complex design principles and methodology to ensure cost-effective and optimal use of resources and technology without jeopardizing network integrity.
Education	University degree (master or equivalent) in a relevant field; CCNA certification or equivalent with other vendors such as Juniper/Brocade
Work Experience	Minimum 8 years of experience but not limited to networking architecture, IP/MPLS, optical transport, DNS, IPv6. LAN protocols (Spanning Tree Protocol and/or VLAN trunking) TCP/IP, RIP, OSPF, BGP and/or EIGRP WAN network topologies and hardware (CSU/DSU, Private Line, DSL) Network Management tools Network (Cisco Certified Network Professional/CCNP or equivalent) and IT Service Management/ITSM qualifications (IT Infrastructure Library/ITIL-ITILV3ISO/IEC 20000 or equivalent) is an asset.

9. Network Engineer

Nature of the tasks	• Construct and maintain configurations for data networks. • Design, test and install network software and hardware. • Configure and install various network devices and services (e.g., routers, switches, firewalls, load balancers, VPN, QoS) • Perform troubleshooting of network problems utilizing network analysers and/or sniffers and other troubleshooting tools. • Deal with network related documentation (develop/update/review) and technical specifications.

	• Configure and implement network monitoring and management systems. • Implement and monitor network security. • Plan network capacity/estimate network utilization. • Analyse current network software and propose modifications and new software according to best practice standards and procedures. • Engage with vendors offering network related services and equipment.
Education	University degree (master or equivalent) in Computer Science or a relevant subject; Minimum 4 years of relevant education (master or equivalent) after the secondary school Network (Cisco Certified Network Professional/CCNP or equivalent) and IT Service Management/ITSM qualifications (IT Infrastructure Library/ITIL-ITILV3ISO/IEC 20000 or equivalent) is an asset.
Work Experience	Minimum 9 years of relevant professional experience in the following fields: • DNS and IP administration • LAN protocols (Spanning Tree Protocol and/or VLAN trunking) • TCP/IP, RIP, OSPF, BGP and/or EIGRP • WAN network topologies and hardware (CSU/DSU, Private Line, DSL) • Network Management tools Advanced/In depth knowledge of the principles, practices and procedures related to Local and Wide Area Networks (LAN/WAN) Advanced/In depth knowledge of Firewall/VPN/load balancer configuration and troubleshooting (Cisco, Stonegate, F5 products are a plus) Very good knowledge of encryption at network layer and encryption protocols (SSL/TLS, IPSEC, etc.)

10. System and Storage Engineer

Nature of the tasks	• Manage and monitor all installed systems and infrastructure; • Monitor and test application performance for

	potential bottlenecks, identify possible solutions, and work with developers to implement those fixes • Participate in the design of information and operational support systems • Proactively ensure the highest levels of systems and infrastructure availability • Server management, Operating System (OS) knowledge (UNIX, Linux, Windows) • Administration of Backup & Storage systems (knowledge of HP backup & storage systems required) • Active Directory (AD) / LDAP Management • Email and antispam systems • Network Access Server (NAS) and Distributed file systems • Public Key Infrastructure (PKI) systems • Replication & Disaster recovery • Document management systems • Centralized deployment of software and updates • HW/SW inventory management • Provide 2nd and 3rd level support • Support of mail servers and mail relays • IT support, ranging from simple desktop and peripheral support to complex server and network issues
Education	University degree (minimum 4 years master or equivalent) in a relevant subject; Familiar with ITIL/ITIL V3 concepts / ITIL Foundation Certified Professional is a plus.
Work Experience	Minimum 9 years of relevant professional experience

11. Test Manager

Nature of the tasks	• Plan and control that any changes to the system are validated in accordance with specifications and requirements; • Support user needs for testing; • Manage all related test environments and plan the usage

	of these; • Document test plans, tests and tests results.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 6 years of professional experience in IT; minimum 4 years relevant to the requested subject; proven ability to work with standard test methods and test tools;

12. Test Engineer

Nature of the tasks	• Develop test strategies • Produce and maintain the required test design specifications – test cases. These can be paper-based (legacy or test cases which cannot be automated) or be integrated in a given tool. The latter determines the format and language applicable to the test cases: XML, Excel format, etc. • Develop test processes, procedures and documentation • Develop test acceptance criteria • Perform testing activities on technical products and analyse the result(s). • Report problems or failures leading to suggestions to improve or perfect the technical products • Interact with project teams and other stakeholders in the framework of the tests organization and activities • Report on the test result(s)
Education	University degree (bachelor or equivalent) in a relevant subject;
Work Experience	Minimum 6 years of relevant IT experience and minimum 4 years of testing experience.

13. Database Administrator

Nature of the tasks	• Maintain the databases and application server products in terms of capacity management, trouble shooting, new releases, documentation, access control, back-up/recovery and other tasks related to the role as DBA; • Make studies/analyses on proposed changes, assess impact and propose database adaptations/application

	server adaptations to fulfil specifications and requirements; • Report and communicate with providers of products as regards errors, incidents and problems.
Education	University degree (bachelor or equivalent) in a relevant subject;
Work Experience	Minimum 6 years of professional experience in IT, including 3 years in database administration; experience in database administration, and in particular Oracle products (e. g. Oracle DB, Oracle Text, Oracle RAC, Oracle Data Guard, Oracle VPD, ASM, Oracle Enterprise Manager, Oracle Recovery Manager, Oracle WebLogic server, etc.) of recent versions.

14. Helpdesk/Service Desk Staff

Nature of the tasks	This profile indicates the general need for operational staff and management for the Helpdesk, the related incident management, and other relevant tasks included in this function (i.e. as can be found in the ITIL definitions of a Service Desk or in similar standards).
Education	
Work Experience	Minimum of 4 years of professional experience in the ICT business, including 2 years with work in a relevant Helpdesk/Service desk in environments similar to the system of this call for tender.

15. Training and User Documentation Consultant

Nature of the tasks	• Person who is able to produce the user manuals of implemented services for end-users. • Produce and maintain the manuals and technical documentation. These can be paper-based or be integrated in a given tool. The latter determines the format and language applicable to the documents: Word, PDF, XML, Excel format, etc. • Writing IS on-line help • Writing web documentation • Prepare and provide training courses on information systems.
Education	University degree (bachelor or equivalent) in a relevant subject;
Work Experience	Minimum 3 years of relevant IT experience and minimum 2

	years of experience with one or more of the following: documentation writing or training, office automation or presentation tools (e.g. Word, PowerPoint).