ANNEX I.A

IT hosting services for the Agency for the Cooperation of Energy Regulators

Framework Contract

TECHNICAL SPECIFICATIONS

OPEN CALL FOR TENDERS

ACER/OP/MMD/04/2016

Table of contents

1. Introduction

This document contains detailed technical specifications for the requested "IT hosting services for the Agency for the Cooperation of Energy Regulators" and includes the following:

- a description of the services requested;
- a description of experts' profiles required for the delivery of the services;
- the Service Level Agreement (SLA) framework and the Service Level Requirements.

The purpose of this document is to specify in a clear manner what are the expected deliverables and services, together with the quality expected in relation to both deliverables and services, which may be part of each specific contract.

2. Technical specifications

The purpose of the Framework Contract (hereinafter the 'FWC') is the provision of the following services:

- Secure and highly available dedicated managed hosting services in order to implement, maintain and operate an IT infrastructure needed for testing, development and deployment of software, web applications, databases, services, etc. in multiple environments (e.g. test, stage and production).
- Housing (co-location) of ICT infrastructure (i.e. servers, storage equipment, related networking and any other needed equipment, etc.) owned by the Agency.
- Provision of support services capable to provide maintenance and support of any hosted or housed (co-located) equipment and/or any installed and configured software.
- Dedicated managed hosting services to ensure Business Continuity/Disaster Recovery (hereinafter the 'BC/DR') to the abovementioned hosted IT infrastructure.
- Dedicated managed hosting services to ensure BC/DR to the current Agency's owned and hosted ICT infrastructure.
- Consultancy services to ensure proper evolution of the hosted infrastructure (e.g. log analysis, continuous improvement, expert advice, etc.).

2.1 Description of the requested services

The services listed below shall include the related basic infrastructure (such as cooling, power, space, cabling, etc.) which is needed to provide the fully functional system.

2.1.1 General requirements

All tenderers shall comply with the general Service Level Requirements defined in Section 4 of these Technical Specifications.

Where applicable, all hosted equipment/software/services should be at least VMware vSphere (ESX 5 and higher), Windows 2008 r2 (and higher), Redhat Enterprise Linux 6 (and higher) and Oracle 12c (and higher) certified or equivalent. The provisioned equipment shall support IP v6.

2.1.2 Specific requirements

The requested services shall include related services such as licensing of specific features related to the provided hardware platforms (e.g. iLO licenses, licensed software for the Storage Area Network and for the networking and security equipment/appliances, licensed software for BC/DR purpose), initial set up of the hardware platform, installation and basic configuration of operating systems, installation and basic configuration of databases, security and networking software, maintenance of an adequate security and service level. These related services shall be included in the relevant price of the service requested and shall not be charged separately by the selected Contractor.

The selected Contractor should also provide, for each provided service (i.e. hosting service), permits (if applicable), technical support for all platforms used for hosting (e.g. active technical support with various vendors of various components of the technological platform) without being entitled to any additional compensation for such support.

At the end of each specific contract and/or at the end of the FWC the Agency shall retain the right to remove its own equipment, software, applications, data, etc. The selected Contractor is required to ensure cooperation with a potential new contractor for the possible handover of the Agency's equipment (e.g. test environment with Cisco UCS and EMC storage) upon prior agreement for a Transfer Out of all the platforms.

The Agency's staff and/or consultants shall have physical access to the hosted equipment at any time without any additional cost.

2.1.3 Services related to physical housing and co-location

The selected Contractor should be able to provide <u>at least</u> the following:

A. A dedicated space inside the datacentre facility (primary site) hosting a cage with enough volume to hold 6 standard 42 HU racks and a possibility of extension/addition to reach in total enough volume to hold 12 standard 42 HU racks, to be rented by the Agency as a service. This shall include the exclusively dedicated cage with all the necessary infrastructure to be made available to the Agency.

The cages (or private server rooms, if offered) should be physically secured (locks, doors, access control, CCTV supervising the area or the surrounding areas) and every access should be automatically recorded by the Contractor's monitoring and surveillance system. The Agency may request that it is automatically notified (e.g. by email and/or sms) of any access to the secured area.

B. A dedicated space inside the secondary datacentre facility (remote site) hosting a cage with enough volume to hold 6 standard 42 HU racks and a possibility of extension/addition to reach in total enough volume to hold 12 standard 42 HU racks, to be rented by the Agency as a service. This shall include the exclusively dedicated cage with all the necessary infrastructure to be made available to the Agency.

The cages (or private server rooms, if offered) should be physically secured (locks, doors, access control, CCTV supervising the area or the surrounding areas) and every access should be automatically recorded by the Contractor's monitoring and surveillance system. The Agency may request that it is automatically notified (e.g. by email and/or sms) of any access to the secured area.

C. A dedicated 42 HU standard server rack inside the cage referred to in points A and B above, to be rented by the Agency as a service.

The racks should be physically secured (locks, doors, access control, CCTV supervising the area or the surrounding areas) and every access should be automatically recorded by the Contractor's monitoring and surveillance system. The Agency may request that it is automatically notified (e.g. by email and/or sms) of any access to the secured area.

2.1.4 Hosting hardware services

The selected Contractor should be able to provide <u>at least</u> the following:

D. A dedicated managed physical hardware infrastructure inside the rack referred to in point **2.1.3 – C** above, to be rented by the Agency as a service. This service shall include the provisioning of the following:

D1. Computing capacity
D2. Memory capacity
D3. Storage capacity
D4. Network capacity

The following minimum requirements must be met for this service:

- D1. Computing capacity:
  - 2-way, 4-way and 8-way symmetric multiprocessing for physical CPUs supported
  - 6, 8, 10 and 12 cores per physical CPU supported
  - 2.4 GHz physical CPU clock supported
  - blade and standalone servers supported
  - x86-64 CPU architecture supported

  Allocated computing capacity made available to the Agency shall be measured in CPU cycles (in GHz).

- D2. Memory capacity:
  - 128 GB of RAM per physical CPU supported

  Allocated memory capacity made available to the Agency shall be measured in GB.

- D3. Storage Capacity:
  - delivered on SAS, SATA, and SSD disk drives
  - delivered by redundant SAN storage controller pairs
  - 20000 IOPS per SAN storage controller pair supported
  - using SSD drives as additional SAN storage controller cache supported
  - FC and FCoE connectivity
  - 40 TB capacity per SAN storage controller pair supported
  - 100 disk drives per SAN storage controller pair supported
  - RAID options 0/1/10/5/6 supported

For the purpose of unique evaluation it is assumed that SSD drive provides 2000 IOPS, 15 K SAS drive provides 180 IOPS, 10K SAS drive provides 140 IOPS and 7.2 K SATA drive provides 100 IOPS of storage performance. The offered performance should apply to continuous read/write (~70/30) IOPS using 4KB blocks under the load from standard web applications and DB operations. In case a specific solution with dedicated SSD appliances is offered the actual delivered performance of the appliance is considered.

Allocated storage capacity made available to the Agency shall be measured in TB.

- D4. Network capacity:
  - 10 Gbps total bandwidth per each delivered physical CPU supported
  - delivered by copper and/or fibre connections of standard bandwidths (10 Gbps, 1 Gbps and 100 Mbps for Ethernet connections and 4, 8 and 16 Gbps FC connections)
  - FC, FCoE and iSCSI supported
  - physical redundancy of all connections supported
  - logical aggregation of connections supported
  - efficient network traffic management to fully utilize the delivered connections regardless of the used network protocol (switch, router, fibre switch, proxy, load balancer, etc.)
  - VLANs supported
  - network traffic filtering/routing and inspection supported
  - rule based network access management supported
  - physical redundancy of all network devices supported
  - secure network segmentation supported (DMZs, LAN, etc.)
  - secure VPN tunnels supported (IPSec, SSL)
  - Centralised management console
  - Management of network security processes, data and policies
  - efficient network traffic management to fully utilize and secure the delivered connections regardless of the used network protocol (firewall, IPS, IDS, malware protection, mail security, web security, DLP, syslog, etc.)

Any implemented network topology must as a minimum include external and internal firewalls, IPS/IDS service, external and internal load balancers, malware protection on network level and a logging service, all in redundant configuration at least on the primary site. The Contractor shall provide a detailed description of the network security measures in the Technical tender. The solutions offered by the Contractors shall be in line with best practices and standards and shall provide the comprehensive protection of the hosted information system against network based threats.

Allocated network capacity shall be measured by an average total bandwidth, delivered to a single physical CPU (in Gbps), of all connections that are actually active and able to transmit traffic according to the connection's bandwidth. The connections used to inter-connect components of network equipment (e.g. a redundant pair of equipment, firewall and switch, etc.) shall be excluded.

For redundant pairs of connections, the network capacity shall be measured according to implemented/supported redundancy mode (active/active[1] – double capacity, active/passive – single capacity).

The provision of hosting hardware services shall include at least the following:

- maintenance of hardware inventory for all hosted equipment;
- physical installation in the racks (i.e. server or any other rack mountable device);
- testing of hosted equipment after installation;
- checking and installing cable connections and cable management;
- device labelling.

2.1.5 Housing hardware services

The selected Contractor shall be able to co-locate and keep functioning, in the selected Contractor's data centre inside the racks or the space rented as described in point **2.1.3.**, the equipment owned and pre-configured by the Agency.

E. The selected Contractor shall provide <u>at least</u> the following housing services:

E1. Housing of a Server;
E2. Housing of a SAN Unit;
E3. Housing of a Network Connectivity Device (i.e. switch, router, fibre switch, proxy, load balancer, etc.);
E4. Housing of a Network Security Device (i.e. firewall, IPS, IDS, malware protection, mail security, web security, DLP, syslog, etc.);
E5. Housing Backup Device (i.e. tape drive, tape library, disk backup device and the connected Backup System)

In case a single physical hardware platform (i.e. Server, SAN Unit, etc.) occupies more than one rack or consumes more than 1 kW of power, it shall be considered that additional physical hardware platform is being co-located for each full rack of equipment for that platform or each kW of power consumed.

The procedures and requirements for the transport of the equipment to/from the data centre are described in point **2.1.11** of these Technical Specifications.

2.1.6 Connectivity services

The selected Contractor should be able to provide <u>at least</u> the following:

F. A dedicated managed physical network connections, to be rented as a service by the Agency, for the purpose of connecting the physical hardware infrastructure referred to in points **2.1.4** and **2.1.5** above to the following targets:

F1. Agency's premises – 10 Mbps
F2. Agency's premises – 100 Mbps
F3. Agency's premises – 1 Gbps
F4. Agency's premises - 10 Gbps

[1] Active/active redundancy mode for the purpose of this paragraph means that full capacity/performance of both nodes forming a redundant pair is available for use without any limitations and the total bandwidth is twice the bandwidth of the single node.

F5. Internet – 10 Mbps
F6. Internet – 100 Mbps
F7. Internet – 1 Gbps
F8. Internet - 10 Gbps
F9. Remote site – 10 Mbps
F10. Remote site – 100 Mbps
F11. Remote site – 1 Gbps
F12. Remote site – 10 Gbps

This service shall be measured by number of connections made available to the Agency for a particular connection bandwidth. Only raw physical connectivity shall be considered, regardless of the actual traffic transmitted (flat-rate).

All the provided connections must be fully redundant. For Internet connections (F5, F6, F7.) the redundancy must be at the level of network operators. All connections must be configured in a way to ensure seamless and automated failover in case of connection failure. For connections F1., F2., F3. and F4 the service shall include the physical set-up of the connections at the Agency's premises together with necessary network equipment to properly terminate and secure the connection on the Agency's side. The provision of a redundant connection shall be considered as part of the single physical network connection and should not be counted as another connection.

All connections should support the use of VPN tunnelling.

All the connections shall be fully symmetrical regarding the traffic direction (download/upload). The option for logical aggregation of multiple physical connections shall be included as part of the service. The network capacity requirements and measures from point **2.1.4 – D5** shall not apply to these connections.

2.1.7 Software related services

The selected Contractor should be able to provide at least the following:

G. A dedicated managed software infrastructure made available within the physical hardware infrastructure from points **2.1.4** and **2.1.5** above, to be rented as a service by the Agency. This includes:

- The provision and managing of a Virtual machine (without the OS installed):
  - RHEL & Windows Server & Windows desktop OS supported
  - 16 virtual CPUs supported
  - 64 GB RAM supported

- The provision and managing of a Web & FTP server:
  - Apache and IIS supported
  - SFTP, FTPS and FTP supported
  - Delivered on RHEL & Windows Server operating system
  - 32 GB RAM supported per instance
  - Virtualisation supported

- The provision and managing of an Application server:
  - JBOSS and Liferay supported
  - Delivered on RHEL operating system
  - 32 GB RAM supported per instance
  - Virtualisation supported

- The provision and managing of a DB server:
  - Oracle and MS SQL supported
  - Delivered on RHEL server operating system
  - 64 GB RAM supported per instance
  - Virtualisation supported

- The provisioning and managing of a Mail server:
  - Postfix (or equivalent) and MS Exchange supported
  - Delivered on RHEL & Windows Server operating system
  - 32 GB RAM supported per instance
  - Virtualisation supported

- The provisioning and managing of an Infrastructure server (DNS, DHCP, AD, LDAP, CAS, etc.):
  - Delivered on RHEL & Windows Server operating system
  - 4 GB RAM supported per instance
  - Virtualisation supported

- The provisioning and managing of a Terminal server:
  - Delivered on Windows Server operating system
  - 64 GB RAM supported per instance
  - Virtualisation supported
  - Compatible with Windows 7 and Windows 8 end-user operating system

- The provisioning and managing of a File server:
  - Delivered on RHEL & Windows Server operating system
  - 16 GB RAM supported per instance
  - NFS and SMB protocols supported
  - Virtualisation supported

- The provisioning and managing of a General purpose server:
  - Fully operational RHEL & Windows operating system
  - 64 GB RAM supported per instance
  - Virtualisation supported

- The provisioning and managing of an End-user workstation:
  - Fully operational Windows 7 or Windows 8 desktop operating system
  - 8 GB RAM supported per instance
  - Virtualisation supported

This service shall be measured by a number of man-days necessary to implement, maintain and operate the software infrastructure according to Agency's requirements.

H. A comprehensive licensing model that will allow the Agency to properly license third-party software for a specific period of time as a service rented by the Agency. This includes:

H1. Hypervisor and Virtualisation Software
H2. Operating system

The following minimum requirements must be met for this service:

- H1. Hypervisor and Virtualisation Software
  - support for clustering, DRS and HA
  - centralized management console
  - support for RHEL and Windows virtual machines
  - virtual machine and storage migrations
  - virtual machines resource management
  - integrated backup solution
  - performance and capacity monitoring
  - can be used to replicate the Agency’s current environment

- H2. Operating system
  - Linux Red Hat, Windows Server and Windows (desktop) license.
  - Capable to replicate the Agency's current environment.

This service listed under H above shall be measured by a cost of a license per physical CPU running the licensed product.

All the software related services listed under G and H above must be provided with complete software installation on the hardware (applies to hosting or/and housing) for the quantity indicated in the specific contract and basic configuration has to be done so the software is ready for use.

Basic configuration means all the actions needed to implement all the minimum requirements for proper functioning of the software according to the manufacturer's instructions.

Virtualisation may be offered by the Contractor or explicitly requested by the Agency in the specific contract. The support for virtualisation is mandatory and is part of the software infrastructure made available to the Agency.

2.1.8 Security related services

The selected Contractor should be able to provide at least the following:

I. A dedicated managed security service made available to the Agency for all services delivered according to these Tender Specifications. This includes:

I1. Backup
I2. BC/DR (Business Continuity/Disaster Recovery for the hosted services)
I3. Agency's BC/DR (for existing infrastructure at Agency's premises)
I4. Anti-malware
I5. Monitoring and Surveillance
I6. Public Key Infrastructure service
I7. Archiving and long term data retention service

The following minimum requirements must be met for this service:

- I1. Backup:
  - RHEL and Windows virtual and physical machines supported
  - De-duplication/compression of data supported
  - Automatic scheduled backups supported
  - Centralised management console
  - Management of backup processes, data and policies
  - Periodic restore of data from backup and test of the quality of backed up data
  - Hypervisor based backup
  - Agent based backup (within the OS)
  - Delivered by backup device (tape drive, tape library, disk backup device)
  - 150 TB capacity per backup device supported
  - 1 TB/h data transfer per backup device supported

  Backup services shall be measured by total backup capacity (in TB) made available to the Agency. The Contractor shall provide a detailed description of the Backup service in the Technical tender.

- I2. BC/DR:
  - RHEL and Windows virtual and physical machines supported
  - nearly synchronous replication to secondary site supported
  - high availability application clusters supported (e.g. Oracle RAC, server farms, etc.)
  - hypervisor based replication
  - storage based replication
  - DB replication
  - centralised management console
  - execution of BC/DR tests
  - Management of BC/DR processes, applications and policies

  This service shall be measured by the number of man-days necessary to implement, maintain and operate the BC/DR processes and activities. The Contractor shall provide a detailed description of the BC/DR service in the Technical tender. The solutions offered by the Contractors shall be in line with best practices and standards and shall provide the comprehensive protection of the hosted information system regarding availability, business continuity and disaster recovery. Any potential licensing cost to use specific BC/DR software or hardware solutions should be included in the cost for hosting hardware services from point **2.1.4** above.

- I3. Agency's BC/DR:

  The selected Contractor shall be able to provide the Agency with a BC/DR environment for its existing infrastructure that is hosted within the Agency's premises. The provision of these services will be expressly requested in a specific contract. The Agency will present a BC/DR plan which will serve as the basis for building a BC/DR solution capable to:

  - Execution of BC/DR tests.
  - Support for VMWare ESX 5.5 and superior.
  - Support for EMC Clariion CX-4 and VNX Series.
  - Host up to 20 physical CPUs and 160 CPU cores.
  - Interact with CISCO switches and routers.
  - Interact with the following software/hardware security vendors: CISCO, JUNIPER, BLUECOAT.
  - Guarantee a smooth integration of all proposed services and all service described in this section.
  - Have a centralised management console.

  This service will connect the DR Data Centre to the Agency's premises with the aim to assure Business Continuity in case of serious disaster at the Agency's premises.

  This service shall be measured by the number of man-days necessary to implement, maintain and operate the Agency's BC/DR processes and activities. The Contractor shall provide a detailed description of the Agency's BC/DR service in the Technical tender. The solutions offered by the Contractors shall be in line with best practices and standards and shall provide the comprehensive protection of the Agency's information system regarding availability, business continuity and disaster recovery. Any potential licensing cost to use specific BC/DR software or hardware solutions should be included in the cost for hosting hardware services from point **2.1.4** above.

- I4. Anti-malware:
  - protection for RHEL and Windows virtual and physical machines
  - hypervisor based protection
  - support for up-to-date real-time protection
  - support for automatic scheduled scans
  - centralised management console#
  - continuous update of malware databases used by the provided Anti-Malware solutions;
  - Management of Anti-malware protection processes, applications and policies

  Anti-malware protection shall be measured by the number of OS instances that are being protected. The Contractor shall provide a detailed description of the Anti-malware service in the Technical tender. The solutions offered by the Contractors shall be in line with best practices and standards and shall provide the comprehensive protection of the hosted information system against malware threats.

- I5. Monitoring and Surveillance:
  - Monitoring for RHEL and Windows virtual and physical machines
  - Monitoring of hardware infrastructure (e.g. Syslog, SNMP)
  - Automatic alerting and reporting
  - Centralised management console
  - Management of Monitoring and Surveillance processes, applications and policies

  Monitoring and surveillance shall be measured by the number of OS instances that are being monitored. The Contractor shall provide a detailed description of the Monitoring and Surveillance service in the Technical tender. The solutions offered by the Contractors shall be in line with best practices and standards and shall provide the continuous monitoring and surveillance of the hosted information system to detect and automatically report any malfunction, capacity or performance bottlenecks and potential security breaches of the hosted information system. In addition, it shall also include periodical reporting on the status of hosted equipment/services. For this purpose, the selected Contractor shall collect and analyse, on a regular basis, security threats and incident related data, data concerning operational reliability of hosted services/equipment and data related to the capacity/performance of hosted services/equipment.

- I6. Public Key Infrastructure service:

  Public Key Infrastructure services shall be measured by number of PKI certificates issued. The PKI service shall ensure the provision of digital certificates issued by a trusted accredited CA within the EU to the end-users (physical and legal entities/systems) using only web browser. The Agency shall have the possibility to approve each certificate request and review the status of issued certificates using only web browser.

- I7. Archiving and long term data retention service:

  These services shall be measured by total archiving capacity (in TB) made available to the Agency. The Contractor shall provide a detailed description of this service in the Technical tender.

2.1.9 Support services

The selected Contractor should be able to provide at least the following:

J. Support services made available to the Agency and/or the Agency's contractors, including the following:

J1. 24x7 Service Desk
J2. System Administration
J3. Custom Support Services
J4. Project Management Services

The following minimum requirements must be met for these services:

- J1. 24x7 Service Desk:
  - the ability to answer the phone call or email inquiry on any issues related to hosting or housed (co-located) service,
  - to log the issue in an appropriate tool, provided by the selected Contractor and
  - to act as a central point of all communications related to operating the hosted or housed (co-located) service environment,
  - services should be provided at least in the three (3) working languages of the EU (English, French and German), if requested by the Agency.

  Service Desk services shall be measured by the number of requests. The Contractor shall provide a detailed description of the Service Desk service in the Technical tender.

- J2. System Administration:
  - Execute any system administration procedure required and/or supplied by the Agency excluding the installation or maintenance of Agency's proprietary software (or the third-party software directly related to it);
  - support for networking connectivity (creation/modification of VPNs, VLANs, DNS entries, etc.)
  - execute configuration change requests
  - execute security-related tasks (authentication and authorization mechanisms, proactive mitigation of existing and emerging security threats, anti-malware operations, system patching and updating, etc.)
  - troubleshooting and provision of relevant information about the hosted infrastructure and applications (e.g. log extraction, investigation of incidents, etc.)

  System Administration services shall be measured by the number of man-days necessary to fully support the operation of the hosted infrastructure and applications. The Contractor shall provide a detailed description of the System Administration service in the Technical tender.

- J3. Custom support services:
  - installation and maintenance of Agency's proprietary software (or the third-party software directly related to it) according to the detailed written procedures provided by the Agency
  - operational support related to fulfilment of specific service requests and participation in various software deployment activities (e.g. trainings, testing, benchmarking, etc.)

    Custom support services shall be measured by the number of man-days necessary to fully support the deployment and operation of the Agency's

proprietary software. The Contractor shall provide a detailed description of the Custom support services in the Technical tender.

- J4. Project Management Services:
  - preparation of relevant documentation, plans and specifications
  - attendance to meetings
  - management of projects

  Project Management services shall be measured by the number of man-days necessary to manage and coordinate the activities related to delivery of services in scope of this tender. The Contractor shall provide a detailed description of the Project Management services in the Technical tender.

All other support services shall be included in the scope of a particular specific service from points J1. - J4. above. These other support services shall be provided by the Contractor at no additional charge to the Agency and they mainly but not exclusively include:

- Performing and keeping up to date hardware inventory of hosted equipment;
- Testing hosted equipment;
- Power cycling;
- Loading/changing pre-labelled removable media;
- Reporting the status of indicator lights;
- Resetting circuit breakers;
- Checking cable connections;
- Reporting physical conditions within the data centre;
- Cable management;
- Physically installing or removing equipment;
- Device labelling;
  - Logging on to the Agency's servers;
  - Performing hardware related software installations according to published installation processes;
  - Basic server administration tasks such as creating new virtual hosts, activating authentications etc.;
  - Kernel updates and recompilation;
  - Software updates and recompilation;
  - Soft reboots (reboot done after logging in to a server);
  - File system checking;
  - Basic system troubleshooting;
  - LAN network device administration (switches, routers, load balancers, proxies, etc.);
  - Security administration such as firewall rule base administration;
  - Creating scripts;
  - Responding to client monitoring events;
  - Problem management activities.

Unless otherwise specified when requesting specific support service, the Contractor shall start executing the request within one (1) working day from the time the request was communicated to the Contractor's service desk. In urgent cases and when expressly requested in writing the Contractor shall start executing the request within six (6) hours from the time the request was communicated to the Contractor.

2.1.10 Other services

The selected Contractor should be able to provide <u>at least</u> the following:

K. Internet services made available to the Agency, including the following:
K1. Public IP addresses

K2. Public domain names
K3. Public DNS entry
The following minimum requirements must be met for these services:

- K1. Public IP addresses:
  - Ability to provide up to 48 public IP addresses
  - Use of public IP addresses on provided Internet Connections

  Public IP addresses service shall be measured by the number of provided IP addresses.

- K2. Public domain names:
  - Ability to associate Public IP addresses with the Agency's Domain Name and Service Names.

  Public domain names service shall be measured by the number of registered domain names.

- K3. Public DNS entries:
  - Ability to propagate the information under K.1 and K.2 over the Internet
  - Secondary DNS server provided by the Contractor or Internet Service Provider

  Public DNS entries service shall be measured by the number of DNS entries.

L. Consultancy services, including the following:
- optimisation and further development of deployed infrastructure and applications;
- assisting the Agency with application management, including management of user accounts and implementation of specific configurations and settings;
- analysis and assessment of specific data/information available on the hosted infrastructure.

Consultancy services shall be measured by the number of man-days necessary to perform the required activities.

2.1.11 Transfer in/out services

The selected Contractor shall be able to relocate existing IT equipment (including HW, SW, system configuration, data) which belongs to the Agency and which the Agency intends to host in the datacentre of the selected Contractor or which the Agency intends to transfer from the Hosting site to another location.

For transfer in/out services, the following planned delivery lead time shall apply: 12 weeks.

The services to be provided shall include in particular:

- The removal of the IT equipment, owned by the Agency, from the Agency's headquarters in Ljubljana, Slovenia to the Hosting Data Centre of the selected Contractor;

- The removal of the IT equipment, owned by the Agency, from the existing data centres in Ljubljana and Maribor, Slovenia to the hosting data centre of the selected Contractor;

- The removal of the IT equipment owned by the Agency and located in the Hosting Data Centre of the selected Contractor, to the Agency's Headquarters or to a third-party location.

The transfer in/out services in this section shall be charged according to **Section 9.2. Ordering Procedure** of the Annex I – Tender specifications as Out of price list services, if and when requested by the Agency.
For the services mentioned above the selected Contractor shall be able to provide the following activities:

- Inventory of hardware, software, services and related configuration(s) that the Agency intends to relocate to the selected Contractor's Hosting Data Centre. In order to define the scope of the transfer, the Agency will include in its request for services a description of the scope with a draft list of hardware (i.e. physical and virtual servers, roles of the servers, software installed and dependencies from other services).

- Creation of a migration plan which should include, as a minimum, the following documents:
  a. A detailed time schedule listing the planned activities.
  b. A list of dependencies with the suggested resolution of the dependencies. The resolution should use as much as possible any equipment in the Hosting Data Centre which belongs to the Agency.
  c. A document containing a high-level analysis of the function of each component of a platform and a low-level analysis containing a description of how the platform works, together with the security measures needed.
  d. A deviation plan which must be provided only in case that one or more components of the entire working system will not be relocated. In this event the selected Contractor will need to assure that the migrated equipment can work in the absence of one or more components which can be replaced with the Agency's existing component or with a similar component which can be ordered by the selected Contractor.
  e. Technical Manuals and instructions on how to re-establish the full functionality of the migrated hardware and software, to re-establish connections with all software dependencies (local or remote), how to start up the full migrated system, and eventually how to publish the system to a public network infrastructure (e.g. on the Internet) or on a private network infrastructure. These manuals need to be provided to the Agency.
  f. Test case manuals with the purpose to test that all functionalities with the same hardware and different configuration will work in the new migrated location. The test case will be used as an acceptance test.

- Proper packing of all equipment prior to transportation. Packing shall be specific for IT equipment with the use of air bubbles or specific foams and specific boxes (generally made of wood and/or cartoon). The selected Contractor shall assure the working of the platform; prior to the removal of the equipment, i.e. all cables need to be labelled, each input/output port shall be identified on each piece of equipment and clearly marked in order to allow smooth re-installation of all parts as well as connection to the remaining components of the system.

- Provision of transportation services and means from the Agency's location to the location of the selected Contractor. The transportation service must include the door to door service and the transportation in and out of the buildings involved. In case no goods lift is present in the building and no transportation path is available, the selected Contractor shall provide specific means of transport which shall reduce the risk on any damage to the transported equipment or the premises (e.g. through the use of specific remote handling devices for IT equipment).

- Inventory of all parts prior to the final re-installation is necessary. The inventory must be consistent with the inventory mentioned at Chapter 2.1.11, and shall specify a list of additional items that might be needed for the final re-installation.

- Re co-location of the transported assets in the new final location and in particular in a rented rack;

- Establishment of all cables based on the labels applied during the inventory, and checks on connectivity of all the components which need to be connected to the internal and external pre-existing components;

- Reconfigurations of the equipment (mainly of hardware and software) in order to re-establish all the dependencies and needed links to the internal and external components.
- Start-up of the moved system in the new working environment and test electrical, network and storage connectivity.

- Test of removed items following the acceptance tests as described in point **f.** above.

- Final deployment of removed items in production and publication of the services for normal use (in case a migration of data will be needed, this will be done by the selected Contractor as the last stage).

3. Service level requirements

The minimum service level requirements (hereinafter the 'SLR') defined below are mandatory for the selected Contractor. Any additional service level requirements shall be set in the service level agreements (hereinafter the 'SLAs') annexed to the FWC and/or specific contract(s).

The tenderers are encouraged to commit to deliver additional services, in addition to the minimum services described in the service level requirements.

The tenderers who wish to offer such additions and improvements shall describe them in the relevant section of their technical offer.

The additional services and improved service levels will be taken into account in the technical evaluation of the tender. These additions and improvements, if offered by the tenderer, shall be binding.

The service level requirements will provide the basis for the SLA for the FWC and specific contract(s).

The minimum service levels requirements which will be included in the SLA (indicative, but non exhaustive) are:

- **Hardware availability**: The dedicated hardware operated and maintained on behalf of the Agency will be operational at least 99.95% of the time in each calendar month;
- **Air conditioning** shall guarantee that the temperature of the open space in the Agency's Data Centre Services area will remain between 17° C and 25° C and relative humidity will remain between 30% and 70%**;**
- **Physical security:** The Contractor should ensure that access to the Agency's Data Centre Services facility(s) will be monitored and restricted at all times. Security of the facility shall be maintained via a security card, video surveillance, biometric hand scan and security vestibule. Tenderers should describe a process for ensuring that only those

with the authority are given access to the Agency's ICT infrastructure and that all accesses are logged and records kept for at least twelve (12) months.;

- **Network availability:** The Contractor's IP network should be guaranteed to be available and capable of forwarding IP packets 99.95% of the time, as averaged over a calendar month. The Contractor network shall include the Agency's access port (the port on the Contractor's aggregation router upon which the Agency's circuit terminates) and the Contractor's IP backbone network, which should include Contractor's owned and controlled routers and circuits (including any transit connections);
- **Internet availability:** Internet connections provided by the Contractor for the Agency's needs should be guaranteed to be available and capable of forwarding IP packets 99.95% of the time, as averaged over a calendar month;
- **Internet latency:** An average monthly transmission rate of 65 milliseconds or less to at least one of the Contractor's upstream Internet providers' or peers' BGP interfaces. Internet latency should be measured to Contractor's upstream Internet providers' or peers' BGP interfaces at approximately five (5) minute intervals and should calculate the average at the end of each calendar month;
- **Packet loss:** The Contractor shall guarantee that packet loss shall not be more than one per cent (1%) on their data centre network or Backbone Network during any calendar month. Packet loss should be measured on the Contractor's Backbone Network at approximately five (5) minute intervals and should calculate the average at the end of each calendar month**;**
- **Denial of service (DoS):** The Contractor shall respond to the Agency's request for assistance with a Denial of Service (DoS) attack and begin the appropriate diagnostic procedures as soon as reasonably possible and, in any event, in less than 30 minutes from the submission of a report of DoS activity.
- **Outage notification:** The Contractor shall guarantee that they shall contact the Agency's technical contact, either by telephone or by email to the telephone number or email address, respectively, within 30 minutes after the occurrence of any unavailability affecting the Agency's infrastructure.
- **Disaster Recovery / Business Continuity:** The Contractor shall be able to ensure the continuous provisioning of the managed hosting infrastructure and services by establishing and managing a Disaster Recovery site through which services are delivered to users in the event of a disaster at primary site, ensuring the provision and management of all hardware and software resources and connectivity. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) together will other details of the solution will be defined in the SLA.

3.1 Benchmark cards for Service Level Agreement

With the aim to define a modular and customer-oriented SLA framework the Agency will set a list of benchmarks which will be used during the implementation of a specific contract to continuously monitor that the selected Contractor, when performing the specific services, is performing at commonly-agreed quality standards. Service levels requirements described above could eventually have the form of these benchmarks.

The selected Contractor may propose additional benchmarks, prior to the signature of a specific contract. The proposed benchmarks shall be approved in writing by the Agency and should follow the following basic rules:

- cannot override or modify any part of the benchmarks defined by the Agency,
- cannot be expressed in a way that makes the benchmarks defined by the Agency unusable for the purpose of the contract implementation,
- must be supported by relevant literature and with a descriptive paper describing the use of the proposed benchmark.

An example of a benchmark card:

Benchmark E2.1 – Infrastructure availability and uptime	
Service quality indicators	Continuity of operation of the overall Agency's hosted managed infrastructure (including hardware and related software, connectivity, networking components, storage, etc.)
Unit of measure	Minutes
Source of measurement data	Report of the level of the services offered
Observation period	Quarterly
Frequency of measure	Monthly
Data to measure	– Actual availability: minutes of the month when there is availability of infrastructure. The infrastructure is considered unavailable even in case of problems of application which cause the complete closure of the system. – Planned unavailability of the infrastructure: minutes for the month of unavailability of infrastructure agreed in advance with the Agency – Theoretical availability: minutes of the month
Rules for measuring	None
Formula (if any)	Value = (Actual availability) x 100 / (Theoretical availability - Planned unavailability of the infrastructure)
Thresholds	Value ≥ 99.5% for each month of the quarter Improvements of the threshold value indicated by the Contractor in offering technical improvements can also be provided separately for each service area. In this case the determination of the score will take as a reference the average of the values individually applicable to the different service areas.
Contractual actions	In case of non-compliance with the threshold value the Agency shall apply a penalty equal to: – 3% of the monthly fee for each month that the Contractor registers oneservice area with non-standard up-time; – 10% of the monthly fee for each month that the Contractor registers two areas of service with up-time with non-standard; – 20% of the monthly fee for each month that the Contractor registers three or more areas of services with up-time with non-standard.
Exceptions	Force majeure adequately documented by the Contractor and accepted by the Agency.

4. Professional profiles

4.1 A-level profiles

- Project Manager (PM)
- IT Infrastructure Architect

Project Manager (PM)	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Economics or similar
Tasks	– Manage project development; – Define project scope, goals and deliverables that support business goals in collaboration with senior management and stakeholders; – Communicate the project scopes, goals and deliverable to the implementation team; – Develop full-scale project plans and associated communications documents; – Effectively communicate project expectations to team members and stakeholders in a timely and clear fashion; – Liaise with project stakeholders on an on-going basis; – Estimate the resources and participants needed to achieve project goals; – Draft and submit budget proposals, and recommend subsequent budget changes where necessary; – Determine and assess the need for additional staff and/or consultants and make the appropriate recruitments if necessary during project cycle. – Set and continually manage project expectations with team members and other stakeholders; – Delegate tasks and responsibilities to appropriate personnel; – Identify and resolve issues and conflicts within the project team; – Identify and manage project dependencies and critical paths; – Plan and schedule project timelines and milestones using appropriate tools; – Track project milestones and deliverables; – Develop and deliver progress reports, proposals, requirements documentation and presentations; – Determine the frequency and content of status reports from the project team analyse results and troubleshoot problem areas; – Proactively manage changes in project scope, identify potential crises, and devise contingency plans; – Define project success criteria and disseminate them to involved parties throughout project life cycle. – Coach, mentor, motivate and supervise project team members and contractors, and influence them to take positive action and accountability for their assigned work; – Build, develop and grow any business relationships vital to the success of the project; – Identify and communicate risks in due time to the contractor and be responsible for the risk register; – Check project implementation and assure delivery in time; – Act as interface between the contractor and the development team; – Draft executive and medium level project documents; – Lead and coordinate any relationship and needed cooperation with the Agency’s contractor for software development products.
Knowledge and skills	– In-depth knowledge of project management frameworks (i.e. PRINCE2 and/or PMBOK)

	– Knowledge of project management tools (e.g. Primavera or MS Project, Microsoft Excel); – Excellent command of English language which should allow him to participate to meetings and to draft efficiently minutes and notes to the internal team meetings and external meetings with the contractor and stakeholders.
Experience	– Minimum 7 years' experience in IT covering a similar position for at least 5 years (the minimum experiences had to be gained after obtaining the qualification mentioned in 'Minimum education'). – Experience in quality assurance procedures; – Must have successfully completed the project management for at least 2 international projects.

IT Infrastructure Architect	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Mathematics or similar
Tasks	– Decide and develop implementation plan for infrastructure architecture on the basis of IT strategies and business requirements. – Enforce infrastructure architecture execution as well as on going refinement tasks. – Stimulate evaluation and selection of entire infrastructure architecture standards commensurate with IT business partners. – Consult project teams to fit infrastructure architecture assignments and identify needs to modify infrastructure architecture to attain project requirements. – Identify needs to change technical architecture to incorporate infrastructure needs. – Ensure documentation of entire architecture design and evaluation work.
Knowledge and skills	– Detailed understanding of infrastructure technologies and solutions. – Knowledge of IT governance and operations. – Comprehensive knowledge of hardware, software, application and systems engineering. – Familiar with best practice methodologies pertaining to design and development, systems engineering and integration and service management (such as ITIL). – Analysis skills using analysis methodologies. – Ability to interact with stakeholders, by means of facilitating scoping workshops, in order to drive out requirements. – Grasp of tools and techniques used to capture and prioritise requirements in order to produce designs that deliver business value.
Experience	– At least 5 years' experience in the relevant field (the minimum experiences had to be gained after obtaining the qualification mentioned in 'Minimum education'). – Excellent experience in Data Centre design, relocation and transformation projects, – Wide experience of current infrastructure technologies and with major IT companies including Oracle, Sun, Microsoft, IBM, HDS, RedHat, and VMware, EMC, Cisco, HP. – Good experience in network systems design, implementation and management. – Excellent experience in virtualisation technologies and best practices – Excellent experience in designing large highly available resilient IT systems

	– Familiar with best practice methodologies pertaining to design and development, systems engineering and integration and service management (such as ITIL) utilised in the IT industry in general. – Ability to conceptualise, energise, mobilise and ensure delivery on time, budget and according to customer expectations and company directives

4.2 B-level profiles

- Storage Area Network Engineer
- Network Engineer
- Virtualisation Engineer

Storage Area Network Engineer	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Mathematics or similar
Tasks	– Ensure all storage allocation tasks are completed per approval/guidance of site leadership. – Ensure full capability of the Storage Area Networks on all mission critical networks. – Provide input to technical briefs used to coordinate storage space increases and new system integrations. – Ensure the SAN is balanced and configured for the most efficient operations. – Perform routine system updates and maintenance while maintaining SAN up-time-
Knowledge and skills	– Knowledge of storage clustering, virtualisation, SAN and networking functionality. – Ability to monitor system performance and utilization. – Ability to create documentation based on functions and tasks performed.
Experience	– At least 5 years' experience in the relevant field (the minimum experiences had to be gained after obtaining the qualification mentioned in 'Minimum education'). – Minimum 3 years' experience in storage (SAN and NAS) administration and other related experience – Extensive experience in working on multiple vendor platforms including but not limited to EMC, HP, NetApp, Hitachi, and IBM and their associated file system structures. – Experience in supporting Fibre Channel switches (Brocade, Cisco etc.) HBAs and zoning and an understanding of SAN design in a heterogeneous environment. – Certifications: at least 1 certification for each proposed storage component.

Network Engineer	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Mathematics or similar
Tasks	– Design, plan, implement and administer LANs and WANs internet/intranet. – Analyse and develop key components, using methodology prescribed techniques. – Responsible for communication protocols, configuration, integration and security. – Responsible for network evaluations, troubleshooting a variety of network problems and implementing various software and hardware upgrades. – Investigate, diagnose and resolve all network problems.

	– LAN/WAN daily operations: router, switch, firewall configurations/access lists, firewall. – LAN/WAN monitoring / vendor contact - continuously monitor all network circuits.
Knowledge and skills	– Extensive knowledge of network system engineering methods, configuration and management of networking components and various networking services. – Extensive knowledge of network operations. – Good leadership skills and the ability to guide and provide technical direction and supervision for a given project.
Experience	– At least 5 years' experience in the relevant field (the minimum experiences had to be gained after obtaining the qualification mentioned in 'Minimum education'). – At least 2 certifications on proposed LAN component (router – switching, etc.). – Working knowledge of major networking components and hardware components.

Virtualisation Engineer	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Mathematics or similar
Tasks	– Decide, plan and implement the virtualisation infrastructure. – Administer virtualisation clusters, including managing updates, deploying high-availability, load-balanced systems, monitoring of the infrastructure. – Design and documentation of all server infrastructure and operating system standards according to best practice IT standards guidelines. – Ensure correct components are accounted for and accurately constructed according to specifications. – Work closely with management to prioritise virtualisation efforts and prepare progress reports (both formal and ad-hoc) regarding project status and deliverables.
Knowledge and skills	– Transforming business requirements and specifications into efficient virtualisation infrastructure- – Designing robust systems for the expanding and maturing the virtualisation environment, designing complex virtual infrastructure solutions in a mid-to-large scale data centre environment – Excellent knowledge of server and desktop virtualisation technologies. – Understanding of storage, network and hardware technologies. – Lead or work on a variety of teams with members of multiple groups to proactively address support issues. – Liaison with other IT teams to gain consensus, provide status updates and present remediation solutions.
Experience	– At least 4 years' experience in the relevant field ((the minimum experiences had to be gained after obtaining the qualification mentioned in 'Minimum education'). – At least 1 certification on the proposed virtualisation component. – Excellent experience in designing virtualisation infrastructure that meets customer requirements.

4.3 C-level profiles

- Infrastructure Server Engineer

Infrastructure Server Engineer	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Mathematics or similar OR secondary education attested by a diploma giving access to post-secondary education and appropriate professional experience of three years
Tasks	– Responsible for installing, troubleshooting and providing support on the server proposed brand systems. – Handle the tasks of calibrating server systems after completion of installation and testing of functionalities. – Identify and repair system instruments by applying best practices, act as an escalating point for server related incidents. – Responsible for installation as well as configuration of hardware and software products. – Performing system administration procedure based on provided documentation/manuals
Knowledge and skills	– Investigating, reporting and resolving problems, including documenting of solutions. – Understanding of VLANs, TCP/IP networks and routing. – Be proactive when dealing with customer incidents and service requests. – Excellent knowledge of the hardware of the proposed server brand. – Understanding backup, monitoring/surveillance and anti-malware solutions
Experience	– At least 3 years' experience in the relevant field (in case of secondary educations this means additional 3 years of experience) (the minimum experiences had to be gained after obtaining the qualification mentioned in 'Minimum education'). – At least 1 certification on the proposed server brand. – Experience in building, changing and decommissioning server hardware. – Experience in testing and managing hot fixes, patches and upgrades.