

Call for tenders

Managed IT Services

Annex A.1 - Service Requirements

TABLE OF CONTENTS

1.	OVERVIEW OF CURRENT SITUATION	3
1.1.	Infrastructure.....	3
1.2.	Hardware	7
1.3.	Applications.....	8
1.4.	Telephony	10
1.5.	Security	11
2.	OVERVIEW OF REQUIRED MANAGEMENT AND SUPPORT SERVICES.....	12
2.1.	Servicedesk - Provisioning of end-user support.....	12
2.2.	Network infrastructure Management.....	13
2.3.	Hardware Management & Support.....	13
2.4.	Application Services Management	14
2.5.	Voice and Telecom / PABX end-user support	14
2.6.	Microsoft Cloud Support Services	14
3.	DETAILED REQUIREMENTS FOR THE MANAGEMENT AND SUPPORT SERVICES...	15
3.1.	Servicedesk – Provisioning of end user support	15
3.2.	Network Infrastructure Management.....	16
3.3.	Hardware Management & Support.....	17
3.4.	Application Services Management	19
3.5.	Voice and Telecom / PABX end-user support	20
3.6.	Microsoft Cloud support services	21
3.7.	Description of Future needs – Extended infrastructure projects.....	23
4.	DETAILED PROFILE DESCRIPTION	24
4.1.	Service Manager.....	25
4.2.	System Administrator.....	27
4.3.	Network Administrator.....	28
4.4.	Helpdesk Assistant.....	29
5.	ELEMENTS REQUESTED FOR THE TECHNICAL PROPOSAL	30
5.1.	Overall management of the services, the service desk and telephony and internet connectivity	30
5.2.	Service level management.....	30
5.3.	Equipment Repair Service & Disposal Channel	32

The JU intends to sign a framework contract for the provision of **Managed IT Services** as described in the present document.

1. OVERVIEW OF CURRENT SITUATION

The following chapters present, for background purposes, a description of the current infrastructure management and support services.

1.1. Infrastructure

1.1.1 Staff

Currently there are around 250 people working in all 6 JUs.

1.1.2 Building

JUs are currently installed on seven floors of the "White Atrium" building situated Avenue de la Toison d'Or 56, B-1060 Brussels. This should remain unchanged unless exceptional circumstance arise with the building owner or organisational changes.

The JUs currently use an infrastructure that was put in place by the service provider of the previous Framework Contract for Managed IT services.

The cabling (data, telephone and electricity) is installed by the owner of the building.

Computer room: The building has a computer room of around 30 m². The room is equipped with UPS, air-cooling but no fire extinguishing system.

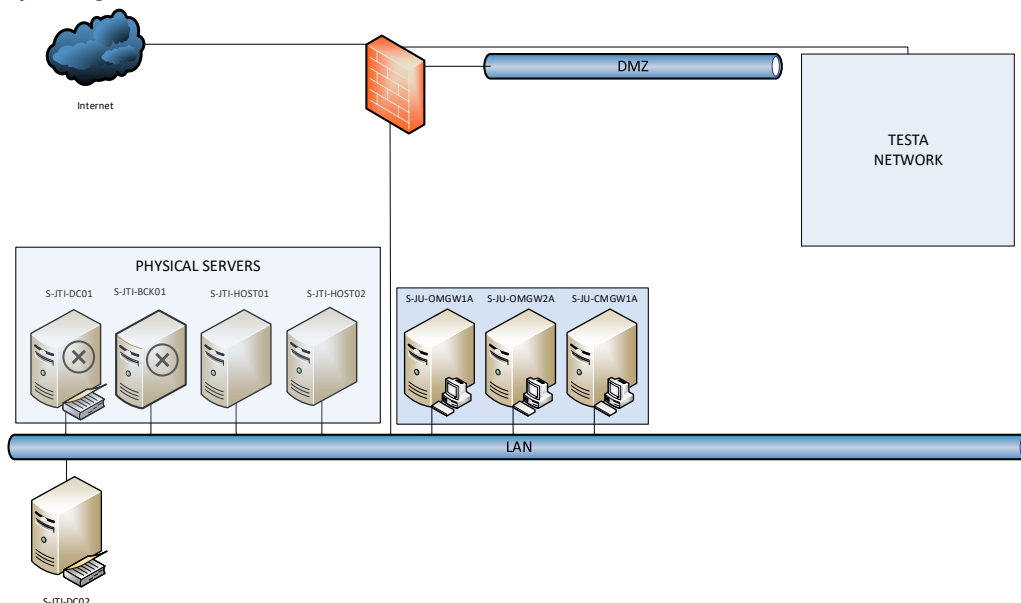
1.1.3 Cabling & Network

The current building is equipped to serve 250 people, who use desktop or laptop computers (Mostly Windows 10 based but some are Apple devices), and local printers (shared or not) and networked photocopiers / scanners. A small number of fax machines remain in use.

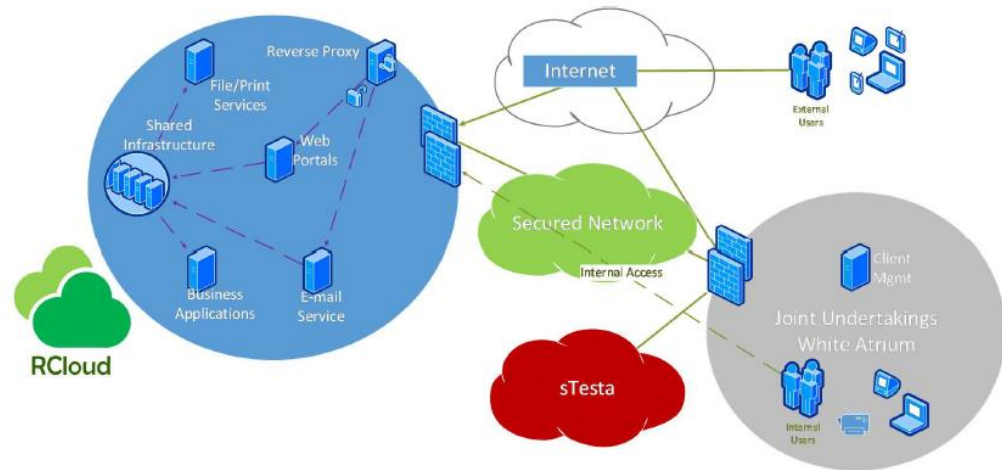
Base services like Distributed File System, Directory Named Service and Microsoft Active Directory have been put in place.

The local network is not slower than 100 Mbps at each plug.

The simplify design of the network is as below:

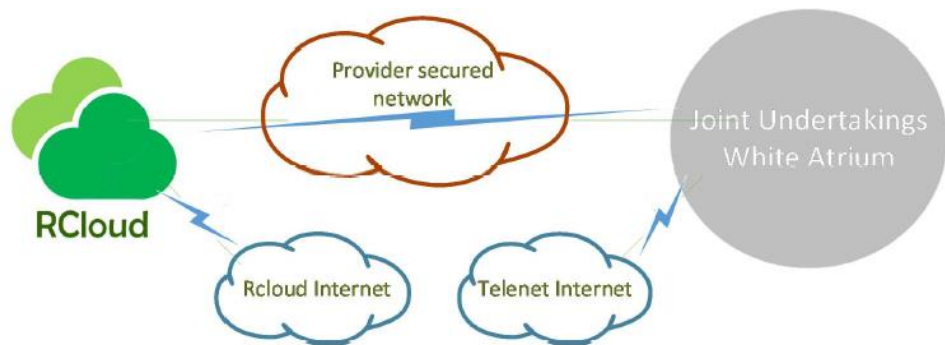


When moving the servers from on premise to an IaaS data centre in 2017, a high-performance and stable network integration was key. The solution chosen is to use a private, secured connection between the remote data centre and the Joint Undertakings. The network service provider guarantees the required bandwidth, availability and performance.



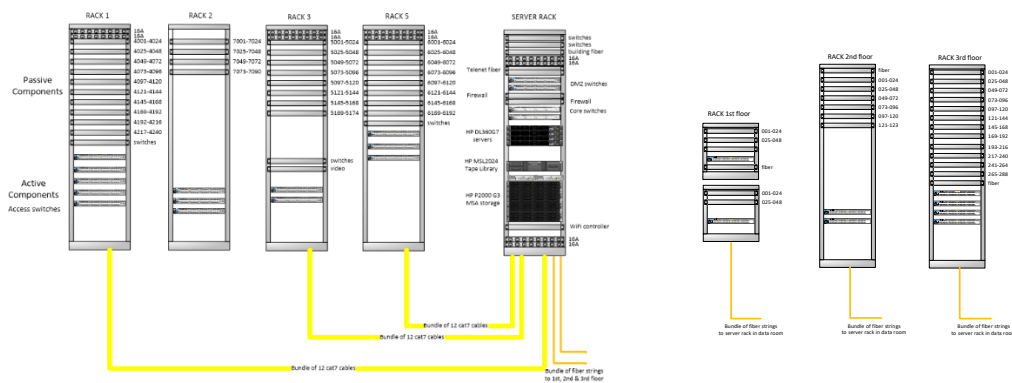
The current Internet connectivity is configured as failover path. The Internet link can also be activated on the MPLS line as fall-back for the existing Internet connectivity.

As alternative, a Virtual Private Network over the public Internet can then be used. The downside is that there is no guarantee on performance and latency because the service provider does not manage all the hops in the network flow.



Based on observations of the current on premise infrastructure and optimizing the usage and load on the servers, the Joint Undertakings are using a 300 Mbps connection with Colt.

The computer room is equipped with racks and switches according to the design below:



The core equipment is installed in racks in the computer room. Racks are used for network equipment (patches and edge switches), and a separate rack is used for the firewall, DMZ & core switches, servers and the storage.

Other racks are used for the WAN connectivity and telephony.

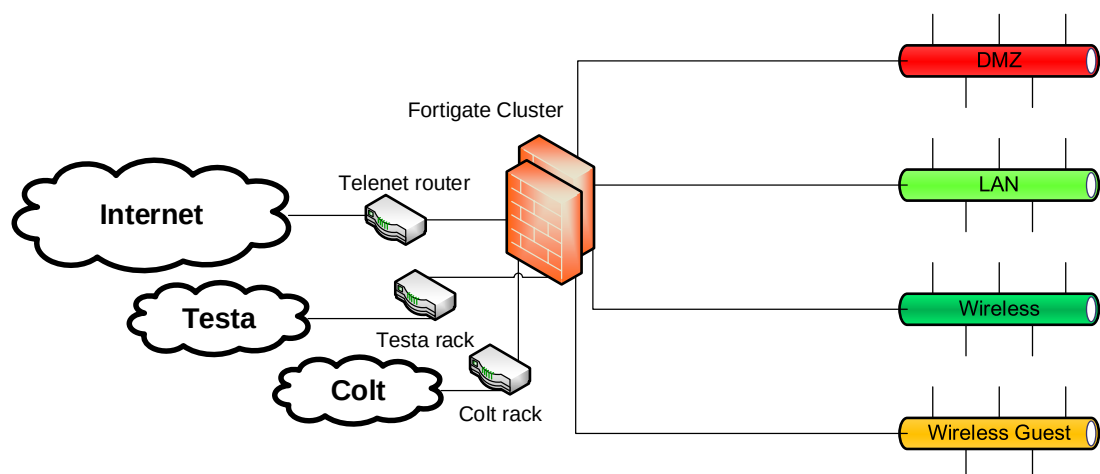
On the first and third floor, separate racks for access switches are installed with fibre connectivity to the main rack in the computer room (which is on the 5th floor)

All the core components have a redundant setup (2 Internet switches, 2 firewall instances and 2 Core switches). Only the access switches are not redundant. The access switches have a connection to each of the core switches.

The network infrastructure contains the following components:

- Two Internet switches. These switches are used for Internet and for DMZ traffic (2 separate VLANs)
- Two Firewalls
- Two core switches. On these switches the servers and storage are connected. These switches are also connected to the access switches and the firewall. These switches are full 1Gbps switches.
- Access switches. These switches connect the clients to the network..

Fortigate 200D is the gateway firewall solution to safely connect the different networks.



1.1.4 Active and passive components

The solution includes all required active and passive components, namely, switches, patch cords, racks ... There must be enough ports on the switches to serve at least 2.5 network plugs per staff at all times.

1.1.5 Router/firewall

The LAN is protected from external connections by a firewall. Only required ports are opened. A router is also installed and configured to route traffic to/from both Internet and the TESTA-ng EC secured network. Both router and firewall must be chosen with regards to the amount of potential networked devices, to assure good performance.

1.1.6 TESTA-ng EC secured connection

The TESTA-ng EC secured network is a secure, encrypted network linking EU institutions and EU member states.

For their daily business, the JUs need to access this network. They access several European Commission IT applications through this network.

A TESTA-ng EC secured connection to the EU institutions is also installed. This connection is actually served by 2 x 2Mbps line. One line is acting as the passive backup of the other. This connection is used by all JUs to access EU IT Applications and EC web sites.

1.1.7 Data Connections

Internet Access is provided through a contract with one of the current contractors. The installed line is 300 Mbps.

A dedicated 300Mbps MPLS connection is available between the offices of the JUs and the termination point of the IaaS provider.

1.1.8 Virtual Private Network

The JUs Executive Directors have commonly decided to adopt 2 VPN solutions to allow tele-working and to secure Business Continuity to all critical functions within their organizations.

The actual solutions allow secured access to office data, emulating the main office desktop (access to workstations, corporate network resources and applications - including applications accessed through TESTA-ng EC secured such as ABAC - e-mail, files, intranet...) and applications from outside the normal office environment.

The current contractor has installed a first VPN solution based on the IPSec standard, with deployment of VPN clients to the JU Laptops. The Joint Undertakings are using hardware tokens with a view of fulfilling the following requirements:

- Increased security of VPN access through hardware-based two-factor authentication
- reduced risk of tampering with personal and corporate information
- Flexibility and portability of the authentication device suited for remote access from any location.

In parallel to the above, the second solution is based on Microsoft DirectAccess setup as an alternative for the currently used VPN solution. The DirectAccess server has been installed in the IaaS DC.

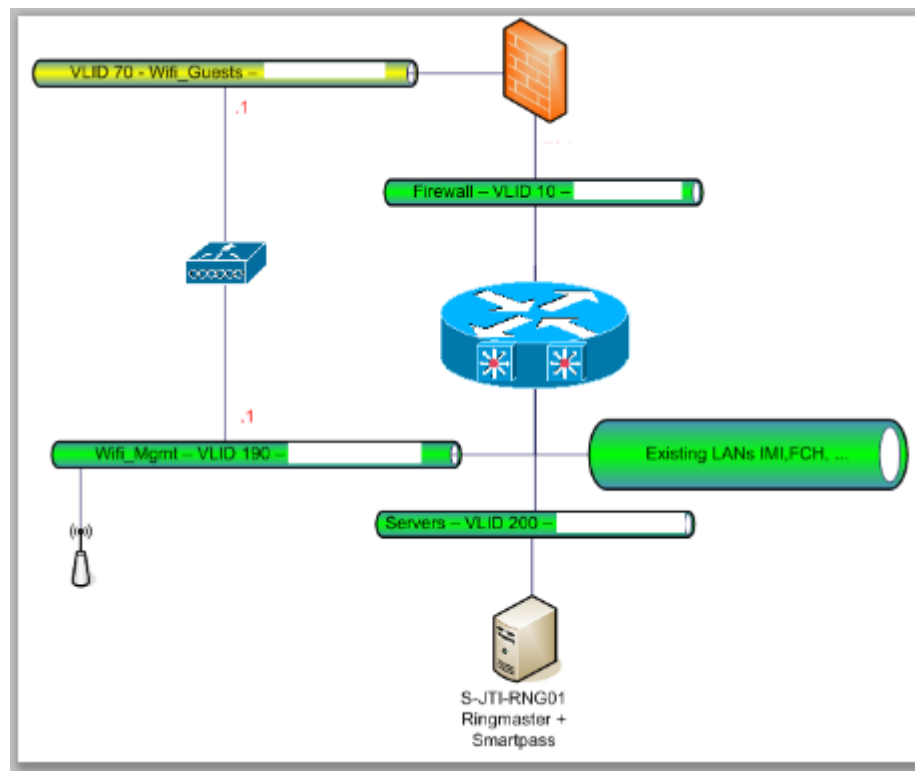
The new contractor (successful tenderer) must continue to support all aspects of the VPN including managing the licensing, maintenance, new tokens, upgrades etc.

The new contractor (successful tenderer) must also be prepared to update the VPN solution as needed. E.g. changes in token provider(s) solution and evolution of DirectAccess to Microsoft VPN.

1.1.9. Wi-Fi Access

The Joint Undertakings have two wireless networks: one for guests and one for staff.

The current global design is as below:



Further description of the WLAN can be provided upon request. A capacity upgrade and possible architecture changes to the WLAN and currently being planned but this is outside the scope of this tender. However, the new contractor (successful tenderer) must be able to support whatever WLAN solution is put in place (which might be different to that in the diagram above).

1.2. Hardware

1.2.1 Office Equipment

Computer setup (reference configuration) prevents staff from installing software on their computers on their own. They must request IT support to perform requested installations.

The current PCs are mostly Dell, HP, Lenovo and Fujitsu computers.

Local printers are mostly Lexmark 360D, group printers are Lexmark T644 and MS811. All group printers are connected to the network.

1.2.2 Server Infrastructure (IaaS servers)

Important note: The hosting of servers **is out of the scope** of this framework contract as a third-party supplier already covers it. There are no physical servers running in the computer room located in the White Atrium building.

All hosting services are provided with a reasonable level of redundancy, hosted using the IaaS cloud technology provided by a third-party supplier.

All JUs can share the infrastructure put in place, but each one is segregated from the others so that they cannot access each other's data; i.e. each JU must have its private file storage quota.

1.2.3 Disk space storage

The solution ensures minimum average storage space of 100GB per staff. This storage will be used depending on needs and spread between services like file storage, e-mail. The details of disk space allocation can be provided upon request. In any case, the storage must be easily expandable in case JUs should need more space for their business.

All data from one JU is segregated from the other JU using file/directories access rights. However, a common file exchange space between JU is also foreseen.

1.2.4 Photocopiers – Multi functional devices

Currently, the JUs make use of the following Xerox Multifunctional devices (MFD) (including copying, printing, and scanning possibilities):

- Xerox WORKCENTRE 7545 under different purchase or leasing contracts.
- Canon IR adv C355i

Currently there are eight MFDs and they are connected to the network and configured so that they allow users to use it as printers independently of the JUs. The MFDs are configured so that staff can use them as document scanners too. Scanned documents are made available on a shared folder and optionally also by e-mail. Scanned documents on the shared drive are not accessible by staff of another JU.

1.3. Applications

1.3.1 Server OS services

Under the term "Server OS services", the Joint Undertakings group all office automation servers and services (Active Directory, File, Print, DNS (Domain Name Service), CA (Certificate Authority), etc.).

Normally the Active Directory service is administrated by the new contractor (successful tenderer) but the IT Officers of each JU can also administer it by using delegation of permissions. Three types of delegated roles are available with scope limited to each JU.

1.3.2 End-user Software

All PCs are installed with a reference configuration based mostly on Windows 10 and Microsoft Office 2016. The Internet browsers are Edge, Internet Explorer, Google Chrome and Firefox installed by default and choice of use left to the user, and the mail client is Outlook.

Software included in the reference configuration for staff computers:

- 7zip
- Adobe Connect Add-in
- Adobe Flash player ActiveX
- Adobe Flash player Plugin
- Adobe Reader
- Forticlient SSL VPN (Laptops)
- Google Chrome

Microsoft Edge

WebEx

Microsoft Teams

OneDrive for Business

TeamViewer

GoToMeeting/GoToWebinar

Java

M-Files

McAfee Agent

McAfee VSE

Mozilla Firefox

Microsoft Office

Microsoft Access

Microsoft Silverlight

PrimoPDF

Skype

Skype for Business

VLC Videolan Player

The European Commission's Framework Contracts to which the JUs are signatories cover licences of this software.

The ECSEL JU owns a 15-user license for a document management system (TriDoc, from Trilobita Informatics - Hungary). This system is a self-contained package that runs on a virtual server running Windows 2012 with client access through the standard Internet browser.

The FCH 2 JU owns a 33-user license for a document management system (M-Files, from SoftAdvice - Belgium). This system is a self-contained package that runs on a virtual server running Windows 2012 with client access through the standard windows and Internet Explorer.

1.3.3. Mail system

The JUs currently use a Microsoft Exchange/Outlook solution for e-mail.

The mail servers is closely monitored and equipped with appropriate anti-spam/anti-virus tools to guarantee that staff will not suffer from these problems.

In case of false positive spam/virus e-mail, a solution exists to recover e-mails during a period of 2 weeks at the minimum.

Mailboxes have a standard maximum capacity of 2GB generally with some derogations typically for Senior Management. One mailbox must be defined for each staff with a layout such as:

first-name.last-name@JU-domainname.

JUs are able to request the availability of shared/functional mailboxes (non-nominative mailboxes such as contact@JU-domainname).

Mailbox storage extension must be possible on request or for specific mailboxes.

The maximum size of e-mail messages (with or without attachments) is 10 MB.

Each user has also an online archive mailbox to manage the size limit of its mailbox and the archiving policy rules set in place in each JU.

As the combination of Exchange and Outlook is imposed, a remote access to e-mail is also provided based on Outlook Web Access. Access to this service is appropriately secured using both passwords and encryption.

1.3.4. DNS

Each JU currently owns a domain name that is used for their e-mail addresses and for their website:

Domain name	Managed by
Cleansky.eu	Hosted and managed by a private hosting company
Imi.europa.eu	Hosted and managed by a private hosting company
Fch.europa.eu	Hosted and managed by a private hosting company
Artemis-ju.europa.eu (historical)	Hosted and managed by a private hosting company
Eniac.europa.eu (historical)	Hosted and managed by a private hosting company
Ecsel.europa.eu	Hosted and managed by a private hosting company
BBi.europa.eu	Hosted and managed by a private hosting company
S2R.europa.eu	Hosted and managed by a private hosting company

1.3.5. Certificates Management

The JUs use 3rd-party digital certificates to secure various services: email encryption, securing websites). This might be extended in the future, by, for example fully qualified digital certificates, document signing, etc.

The JUs procure these certificates via other procurement channels, and the new contractor (successful tenderer) will be required to install and manage them (monitor and apply CRLs (Certificate Revocation Lists), expiry dates, etc.).

1.3.6. Printing Service

A printing service is put in place and allows staff to print on any group printer of its own JU. Printing to photocopiers (especially for large print jobs) is also in place. As printing is a basic need for business, the end-user support on this kind of service is critical.

1.3.7. Backups and Restore

At least a daily backup of all modified data is performed and kept for potential restore request for a minimum of 6 months. This is performed in the geo-redundant data centre.

The restore service is able to restore files, mails or any other data with a timeframe of 4 office hours.

The restore of single files or mailboxes is possible on user's request.

1.4. Telephony

The JUs have a telephonic central (PABX) Siemens HiPath 3800, PABX supporting VoIP connexions, and which 24 Digital connexions plus a small number of analogue connections

The simplify design of the PABX is as below:

SIEMENS Hipath 3800		
CPU	V8 version	
DIUT2	PRA connection (Belgacom) - 30 channels	
SLMO24	24 digital extensions :	11 x OpenStage 15 T
SLMO8	8 digital extensions	
SLMAE8	8 analog extensions :	Faxes, phones lifthalls, Gigaset SL4, ...
SLMAE8	8 analog extensions :	Faxes, phones lifthalls, Gigaset SL4, ...
Xpression	Voice mail up to 500 boxes	
HG1500	IP card with 30 channels and 126 IP licences :	81 x OpenStage 15
HG1500	IP card with 30 channels and 126 IP licences :	43 x OpenStage 60
free		5 x Soundstation 7000 IP

A Service Desk and a Service Contract support the PABX. The services are covered by an SLA - annual maintenance for Hipath.

The actual end-user equipment under maintenance is composed of Openstage 15 (75), 60 (49), 15T Digital (11) and Polycom devices with or without extended microphones (11) and other accessories.

The current contractor is providing a billing system (including a dedicated PC) and the possibility to identify private calls and calls by JUs.

The central is connected to a leased E1 telephone line, providing 60 communication channels.

The following voicebox types and services are implemented:

- Mobility mailboxes
- Personal mailboxes
- Group mailboxes
- Information mailboxes
- Routing mailboxes

1.5. Security

Tenderers are informed of the obligations laid down in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, its subsequent versions, its implementing rules (as adapted from time to time) and the corresponding security standards and guidelines, as well as the Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on the security in the Commission, and the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, its implementing rules and the corresponding security notices.

These documents (as adapted from time to time) are available for consultation at the following address: https://ec.europa.eu/info/files/security-standards-information-systems_en

The **Joint Undertaking** draws the tenderers' attention to the contractual provisions on security (Article III.2.2 of the General Terms and Conditions for Information Technologies Contracts), and on confidentiality (Article II.8 of the General Conditions of the draft framework contract).

2. OVERVIEW OF REQUIRED MANAGEMENT AND SUPPORT SERVICES

The following chapters present a description of the required components, services and tasks to be performed. Detailed requirements for the services will be explained further in chapter 3 and for the profiles in chapter 4.

Important Note: Management of the White Atrium¹ building computer rooms: Air Conditioning, UPS, Fire Extinguishing Systems, European Commission Testing network hardware **are out of the scope** of this framework contract and already managed by other third parties.

The hosting of the infrastructure in the cloud and the provisioning of Office 365 and Microsoft 365 licenses **are also out of the scope** of this framework contract as a third-party supplier already covers them. However, end-user support for Office 365 and Microsoft 365 **must be covered** under this Framework Contract.

2.1. Servicedesk - Provisioning of end-user support

- (1) On-site and off-site Service Support / Service Desk for the end-users and IT Officers.
- (2) Helpdesk with incident recording as well as on-call availability of on-site technical support for the entire internal telecommunications, network and WiFi infrastructure;

Tasks

- Reporting & Documentation
- Provision of a ticketing system - Call Management, L2 Escalations
- Active Directory Password reset/VPN unlock
- Email mailbox size requests
- On-Site Support Staff + Remote Phone Support including outside normal working hours
- Front office & back office operations

The profile to be used is the Helpdesk Assistant (point 4.4). A yearly number of about 245 normal working days must be covered (242 days for 2018 as per annex B2 chapter 2.1). The provider's effort estimation shall determine the number of required persons, based on how he can secure to meet the KPI's.

On-site service desk must be provided during normal working days as defined in the general ICT conditions (Annex A4) under common administrative provisions 1.1 definitions.

The complete service window is defined in the annex B2 in chapter 2.1

¹ The White Atrium is the building where the JUs are located.

2.2. Network infrastructure Management

- (1) Continuous system management and operations of the existing IT network infrastructure and future extensions or adaptations of the same.
- (2) Design, installation and configuration of upgrades or possible extensions of the existing IT network and telecommunication infrastructure on request.

Tasks

- System design and integration
- Installations
- Infrastructure Operations and System Management
- PC application support, troubleshooting
- LAN, switches, cabling, VLANs etc... including security
- WAN - Internet links, DC Links, Cloud Links, Testa, Proxy, Firewalls, security management, DNS
- WIFI in White Atrium
- VPN Remote Access / DirectAccess

The profile to be used is the network administrator and/or system administrator working mainly remotely with automated monitoring. The presence on-site for diagnostic, deployment or meeting is estimated to 1 day/month

2.3. Hardware Management & Support

- (1) Continuous system management and operations of the end-user equipment
- (2) Design, installation and configuration of upgrades or possible extensions of the end-user equipment on request.
- (3) Secure deletion of data and secure disposal of equipment or any storage device.
- (4) Collection of used ICT equipment, obsolete or broken for refurbishment.
- (5) Destruction of any sensitive JU information present on the ICT equipment before disposal for resale.

Tasks

- PC & Phone HW install/upgrade/move/remove/ work place preparation
- Printing support, Multi-functional devices management, incl. toner replacement
- Mobile Device Management (security)
- AD + Email + OWA Management
- SCCM/Intune: PC/laptop Image preparation, patching, OS Updates, App Updates
- Setup and installation of end-user equipment
- Inventory
- Group obsolete ICT equipment in bundle for disposal;
- Erasure of information according to EC rules (**Annex A3**);
- Disposal of ICT equipment to charity or educational organisations.

The profile to be used is the helpdesk assistant used for the Servicedesk – end user support services.

2.4. Application Services Management

- (1) Continuous system management and operations of the end-user software configuration.
- (2) Design, installation and configuration of upgrades or possible extensions of both the server and end-user software components.

Tasks:

- Identity Management, File server, groups access management
- Antivirus administration and maintenance (McAfee)
- Antispam (Symantec MessageLabs) -- could be replaced by MS Threat management
- EC Address book synchronization, antispam, antivirus
- Public DNS service management (currently ordipat.fr)

The profile to be used is the system administrator working mainly remotely with automated monitoring. The presence on-site for diagnostic, deployment or meeting is estimated to 1 day/month.

2.5. Voice and Telecom / PABX end-user support

- (1) Continuous system management and operations of the existing IT telephony infrastructure and future extensions or adaptations of the same.
- (2) Installation and configuration of handset and other telephony equipment
- (3) Design, installation and configuration of upgrades or possible extensions of the existing telephony infrastructure.

Tasks:

- PABX Administration and Maintenance, including allocation of numbers by JU.
- Office Telephony Support
- Distributed telephony and Messaging Platform
- Monthly extract of user / telephone number data and use of this to itemise (by JU) the list of calls made. The latter is provided in a log file by telephony provider.

The profile to be used is the helpdesk assistant used for the Servicedesk – end user support services.

2.6. Microsoft Cloud Support Services

- (1) Management of and end-user support to cloud services (including, but not limited to Microsoft's O365/M365).

Tasks

- Office/Microsoft 365 Management and Support, where applicable (Office Suite + SharePoint, Skype4Business, OneDrive, etc.)
- Azure AD Support
- AD Password/VPN unlock
- Functional mailbox create/modify/delete, Email mailbox size requests
- File server groups access management
- Antivirus support

The profile to be used is the Helpdesk Assistant used for the Servicedesk – end user support services.

3. DETAILED REQUIREMENTS FOR THE MANAGEMENT AND SUPPORT SERVICES

Throughout the framework contract's duration (maximum 4 years), the provider shall deliver infrastructure management services aiming at keeping the infrastructure functioning, maintaining the core and end-user infrastructure and securing the complete IT infrastructure.

The use of IaaS has the additional benefit of allowing for maximum scalability in the environment, both for easily activating additional virtual machines when required based on standard templates (e.g. test and release of future business applications), and for adding additional server capacity including memory, CPU power, and access to storage on the SAN.

3.1. Servicedesk – Provisioning of end user support

The new contractor (successful tenderer) shall provide:

- a separate facility for logging calls and e-mails, and immediately fix issues such as password lock-outs, printer spool re-starts, etc.,
- End-user self-service tools for simple problem-resolution in the form of a wiki page for FAQs and procedures.

Calls handling and incident management database recording could be done remotely by a call centre, with a pool of experienced people in that field.

The following requirements are essential:

- **Change Management:** recording of change requests, assessing the impact, cost, benefit and risk of proposed changes, approving, managing and coordinating change implementation;
- **Incident Management:** : incident logging, follow up and resolution with guaranteed Resolution time of 8 working hours after the incident occur or better;
- **Problem Management:** : root cause analysis and resolution;
- **Hotline Service:** The provider must offer a hotline with helpdesk for support;
- **Ticketing System:** The provider must give an access to their ticketing system
- **Proximity services:** Installation of hardware & software, move of hardware items, organising repair / replacement of defective hardware, reinstallation or deployment of software components acquired via another contractor of the JUs.
- **Documentation creation / update:** Update the associated system and user documentation and procedures accordingly.
- **Knowledge transfer to end users:** organisation and provision of training sessions to end-users.
- **Statistics and reporting:** on incident and problem types, response time, resolution time, etc.

Calls handling and incident management database recording can be done remotely but it is mandatory to have at least one IT support person on site during office hours.

The tenderers should also include in their offer the functionality to have quick on-call availability of technical support on site during office hours for patching and cabling issue.

A full description of service requests categories, catalogue of actions and SLA assigned is to be found in the **Annex B2**. The Servicedesk will provide the following basis services:

- Define, maintain and install the reference configuration on all PCs, keeping software up to date, applying published patches, etc.
- Install and move IT hardware and software on request.
- Repair or replace defective hardware or software within one business day.

- Provide hardware/software usage assistance for every hardware/software delivered or already existing in the JU to all JU users.
- Maintain an incident and request management database allowing providing statistics on incidents types, response time, etc.
- Maintain a hardware and software inventory.
- Support must be available in English.

3.2. Network Infrastructure Management

The following requirements are essential:

- **Consultancy services:** The new contractor (successful tenderer) may be called to provide consultancy in the areas covered. The consultants would be assigned tasks such as design, implementation and administration of solutions.
- **Service availability:** The availability of the service must be greater than 99.9% during office hours within 12 months period up to the end-user equipment. The downtime provoked by interventions not requested by the JUs will be taken into account to calculate the availability rate; the downtime provoked by scheduled interventions agreed by the JUs will be excluded ;
- **Where repair/replacement of hardware and software elements is needed,** the new contractor (successful tenderer) shall advise the JUs on the need for them.
- **Infrastructure operations:** Backing up data, restoring data and testing restoration.
- **Maintenance of the infrastructure:** Corrective and preventive maintenance of all hardware components involved in the installation in order to reduce the frequency and impact of failures or performance degradation, standard tuning, standard software update and maintenance (OS, security patches, new versions/releases, etc.).
- **Infrastructure monitoring and availability:** maintain the performance of the infrastructure in optimised levels, providing sufficient system capacity and availability. The maintenance of the ground floor common space and common meeting rooms on each floor is essential. The equipment installed must be checked on a weekly basis to ensure that everything is still functioning (AV systems, beamers, cables...)
- **Security control:** Ensure that security techniques and procedures (e.g., firewalls, security appliances, and network segmentation, intrusion detection, Network Access Control) are used to authorise access and control information flows from and to the JU network.
- **Statistics and reporting:** Keep the IT Officers of the JUs informed about the status of changes to the systems, processes and procedures. Compile monthly reports on system performance and on forecasted system performance to determine if sufficient capacity exists. Implementing an online dashboard for IT officers to display the real-time performance of IT and network infrastructure is also required.
- **The local network infrastructure** contains the following components: 7 access switches: These switches connect the clients to the network. Patching of cables from those switches up to the end-user computer is under the responsibility of the on-site support as is the configuration management (VLAN, diagnostics, upgrades ...). It should be noted that this support in cabling phones is more important for the ECSEL-JU because they are using digital phones whereas the other JUs use the VoIP version.
- **Documentation:** Keep current documentation updated and create new documentation as necessary.

Network Connectivity

The actual setup of the local area network is described previously in this document in chapter 1.1.3. A complete documentation of the infrastructure design is maintained by the actual service provider and will be at disposal for the new contractor. Internet connectivity will be the responsibility of only one supplier, the winner of this tender.

The supplier will both setup any new installation and manage all requested changes (i.e. re-patching after printer or PC move).

Important note: The access to the European Commission's network by the TESTA-ng EC secured connection is out of scope in this contract, as it is provided by a third party supplier.

Specific requirements are:

- Firewall management: redesign a more integrated, simplified but robust solution for the firewall and proxy management in liaison with the Firewall installed on the IaaS provider side..
- Network management: The provider must proactively manage and monitor the Internet service and /or any related connectivity services and hardware (router) and this 24h/24, 7d/7;
- Reporting: The provider must provide reports about the utilization and the availability of the connectivity. Reports must be available in electronic forms.

WiFi Network Connectivity

The new contractor (successful tenderer) must manage the licensing, maintenance, potential expansion and all other aspects of the Wi-Fi installation.

Specific requirements are:

- The Wi-Fi access must provide access to Internet to JUs guests and visitors, as well as dedicated network for the staff.
- At the minimum connections for 802.11b and 802.11g must be implemented and isolated from the local network of the JUs on a VLAN-level.
- Similar to the Internet connections of JU staff, all Wi-Fi activity must be logged and authentication must be performed prior to provide access to Internet.
- Visitors will receive the required connection credentials at their arrival.
- The provider must proactively manage and monitor the Internet service provided over the WiFi and /or any related connectivity services and hardware (router) and this 24h/24, 7d/7;
- Reporting: The provider must provide reports about the utilization and the availability of the connectivity. Reports must be available in electronic forms.

Virtual Private Network

The solution in place has been described in chapter 1.1.8 and must be kept functional. All traffic will be allowed from the VPN Users to the LAN so the users can work at home, as they would at the office.

3.3. Hardware Management & Support

Multi -functional devices (MFDs) management

A small number (1 to 4) of additional MFDs from third party suppliers can be expected to be included under the hardware management tasks to be covered under the future contract of this call for tender.

The leasing of current copiers will be ending in 2019 at different times for each JU. From that moment, the JUs will rely on European Commission's Framework Contract to which the JUs are a party for providing the leasing, renting or buying of similar copiers. The new devices to replace

the current ones will be covered by a standard warranty and maintenance contract. The new models proposed will have equivalent capabilities and setup as with the existing models.

The tenderers will take over the complete management of the existing and any future copiers including installation of devices, services, supplies and repairs requests.

Setup and installation of end-user equipment

The new contractor (successful tenderer) will plan, prepare, test and install the Hardware, Software and telecommunications components for newcomers, ensuring integration into the overall infrastructure without impact in the overall performance of the global environment.

Reference configurations for user workstations must be defined, maintained and used. The creation and maintenance of such images or configurations must be done in such a way as to ensure rapid, reliable, and current installation of operating and application software on all desktops and laptops in use by the JUs.

This includes the configuration, maintenance and helpdesk of all staff computers, including current ones and new ones to be acquired by the JUs.

The tenderer should ensure the installation/configuration of any hardware and reference software.

See the description of the current situation for a detail of existing hardware. The new contractor (successful tenderer) must be able to provide the requested support for all existing hardware (virtual or physical), including Apple notebooks, iPhones, Android or other smartphones actually in place or to be added. Basic support for printers and copiers should also be covered.

JUs may also request additional PCs to be installed during the course of the contract.

Proactive advice on need for replacements/additional supplies should be covered by the service under the contract. However, further supply (purchase or leasing) of hardware is not within the scope of the current contract but will be organized through the JUs' contractors for these supplies.

Detailed Requirements for Equipment Repair Services & Disposal Channel

The Joint Undertakings have a variety of ICT equipment of different types from different manufactures, some relatively new and some up to 4 years old. Some items are covered by extended warranties, which will expire at different times in the future; some items are already out of warranty.

Some of the items, which are out of warranty, will undoubtedly require repair in the coming years. Most items will eventually require disposal. That is the purpose of the services required covered in this chapter.

Range of Equipment

An indication of the type and quantity of equipment in use by the JUs is documented in the parts of this document, which describe the current situation. An evolution in this inventory is to be expected but an increase in staff, and therefore equipment, for current and future JUs is very unlikely to exceed 50%.

The repair channel should cover the following category of equipment:

- Desktop and laptop computers (both Windows PCs and Apple OS)
- Desktop flat screen monitors and large wall mounted "TV" monitors
- Ceiling mounted and portable projectors
- Desktop printers & Desktop scanners
- VOIP, Digital and analogue telephones & Fax machines
- Network switches, tape drives, servers

- Upon request and if possible, other common ICT peripherals and office electrical equipment (e.g. desk lamps, laminators, CD burners, modems, small routers, sound bars, etc.)

The disposal channel should include:

- All items covered in the repair channel
- Items under warranty elsewhere for repair but not suitable for repair
- Network switches, tape drives, servers, telephone routers (PABX) and other equipment typically found in an office technical room.
- Other items of office electric equipment, not necessarily ICT related, which are subject to the WEEE regulations (Waste Electrical & Electronic Equipment). Items such as microwave ovens, electric kettles, coffee machines, lamps, small heaters etc.)

Service level required

The service level can range from same day to intervention planned far in advance depending on the requirements.

- For repair of printers, computers (laptop or desktop) and ICT equipment, tenders should provide their minimum delay for off-site repair, which will be part of the quality assessment.
- Tenderers should provide a table of the type of on-site interventions, which they can provide with response times. Note that on-site will always mean in the city of Brussels at our current or any future premises.
- For equipment, which cannot be repaired on-site typical prices should be quoted for collection and return.
- If the winning tender cannot repair a specific item, alone it can sub-contract the work to a specialist. If this is the case, the identity and cost charged by the sub-contractor must be visible to the JUs along with any charges by the winning tender for transport and supervision of the repair.
- For disposal, prices should be quoted for data erasure per item (typically per hard disk – details below) and for the actual collection and disposal by the appropriate price metric (volume or weight). Typically, equipment for disposal will be stored by the JUs until a worthwhile volume for removal has accumulated.

Compliance with data protection and environmental regulations.

All equipment for disposal must comply with European Institution standards for data protection and environmental protection (see **Annex A3**). Items for disposal must not be sold for profit. However, they can be recycled or re-used for charitable purposes as detailed in the chapter 4.16 of the **Annex A3**. Rules for removal of items from the inventory are set in the chapter 4 of the same document (Annex A3) and will apply by analogy to the JU.

3.4. Application Services Management

See the description in chapter 1.2 above of the actual situation for a detailed description of existing software components.

The JU will supply all the operating system and office licences to cover the existing PCs and laptops, since these licences belong to the JUs.

As regards the client operating system, the choice is open to the JUs. Core infrastructure is based on Windows server OS only, while end-user machines are mainly on Windows 10 but some also under Apple iOS/osX.

When applicable, open source or free software should be used / proposed in agreement with the JUs' IT representatives.

The following requirements are essential:

- Maintain all **servers** providing service to the JUs: keeping software up to date, performing backups and restore, applying patches.
- All published patches and updates must be applied to software in the **client reference configurations**. In addition, JUs might request additional software installation at any time.
- **Security control:** manage user identities and accounts (creation, modification, deletion). Ensure that all users (internal, external, temporary) are uniquely identifiable, and their identities and access rights are kept and maintained in the central repository (Active Directory). Ensure up-to-date security patches and anti-virus checks are permanently in place and in general preventive, detective and corrective measures are in place protecting against malware and unauthorised access to the IT assets (especially data and information).

3.5. Voice and Telecom / PABX end-user support

The current setup of the telephony network is described in chapter 1.4. A complete documentation of the infrastructure design is maintained by the current service provider and will be made available to the new contractor (successful tenderer). Spare parts and standard exchange of damaged phones must be foreseen in the next business day if under warranty or maintenance contract. The tenderer must provide the functionalities mentioned below including the possible future evolution towards virtual/cloud PABX, unified communications, etc.

The following requirements are essential:

- Provide connectivity to support sufficient external lines / channels for 250 staff (Currently there are 60 channels). Possibility to extend the number of external lines if the JUs request so ;
- The solution shall cover at least the following services:
 - Filtering International or toll calls
 - Caller identification (using lcd screen on telephone set)
 - Call forwarding
 - Call cascade/grouping
 - Call pickup
 - Conference call (both with internal and external users)
 - Hands-free telephone sets
 - Voice mail with option to forward the notification & content by email as well as remote dial-in access
- Take over and preserve the existing numbers ;
- Provision of additional new numbers ;
- Upgrade of the existing telephone central Unify HiPath 3800 for both the latest software releases and any potential hardware need.
- Configuration and maintenance of HiPath 3800 in the location of the JUs ;
- Configuration and installation of new phone sets
- Faxes: provide the required lines allowing the utilisation of the five existing analogue fax devices and preserve the existing fax numbers ;
- Virtual fax: A virtual fax solution allowing staff to send and receive faxes via their Outlook client is desirable. This service may be requested by a particular JU at a later stage ;
- Integrated Voice Mail: The solution actually in place and to maintain is the HiPath™ Xpressions Compact is the integrated voice mail solution for HiPath 3800.
- Service availability: The availability of the service must be greater than 99.9% during office hours within 12 months period to the access point. The downtime provoked by interventions not requested by the JUs will be taken into account to calculate the availability rate; the downtime provoked by scheduled interventions requested by the JUs will be excluded ;

- Reporting: Detailed figures on minutes of outgoing calls by country/zone with unit price per call. Such reports shall be provided in electronic format and support the monthly invoices ;
- A billing solution must be included that allows to invoice each JU its respective phone communications. Currently the PhoneEX Pro Call Management System is in place but not used to its full extent.
- Private calls identification: Staff should be able to identify private phone calls that should be charged to them by the JU (i.e. by composing a code prior to dialling).
- Trainings: The JUs might request training sessions to be organised.
 1. User- basic
 - Number of participants : max. 15
 - Place : on site
 - When : upon request
 - Duration : approx. 30 min
 - Price : included in the proposal
 2. User- advanced
 - Number of participants : max. 5
 - Place : on site
 - When : upon request
 - Duration : approx. 2 hrs
 - Price : included in the proposal
 3. System Management - basic
 - Number of participants : max. 5
 - Place : on site
 - When : upon request after installation or configuration
 - Duration : approx. 1 day
 - Price : included in the proposal
 4. System Management- advanced
 - Number of participants : max. 5
 - Place : on site
 - When : upon request after installation or configuration
 - Duration : approx. 1 day
 - Price : included in the proposal
 5. Billing System
 - Number of participants : max. 5
 - Place : on site
 - When : upon request after installation or configuration
 - Duration : approx. 1 day
 - Price : included in the proposal

3.6. Microsoft Cloud support services

Scope

In 2018, various JUs will be seeking to change their approach to the provision of core IT and telephony services, including but not limited to end user devices, core enterprise computing stack, service management and support, ongoing maintenance, in line with the expiry of its existing service contract. The JUs may be migrating part of or their entire infrastructure to either Office 365 or MS 365.

As such, the new contractor (successful tenderer) must include in its offer the supporting of these SaaS based services.

Assumptions:

There will be no detail on specifics such as SLAs. For more details please refer to Service level required described in the section below.

The new contractor (successful tenderer) will need to provide support for various configurations.

Some JUs may opt:

- Not to migrate
- To partially migrate their infrastructure
- To fully migrate their infrastructure

Service level required:

The future contractor will also have to support various SaaS services provided by Microsoft, as follows:

- All applications and services with Office 365 E3 and E5 packages, including any future application additions
- All applications and services with Microsoft 365 E3 and E5 packages, including any future application additions
- Skype for Business conferencing, Cloud PSTN and Cloud PABX
- Microsoft Azure AD, AD Connect

Moreover, the new contractor (successful tenderer) must be able to provide:

- 24/7 premium support services.
- Must be a Microsoft Silver or Gold Certified Partner.
- Must be able to provide support up to third level and be capable of escalating to Microsoft if necessary.
- Should be able to provide guidance to services such as information protection device and app management, identity & access mgmt. and threat protection, amongst other SaaS services.
- Proactive service monitoring and reporting. IT Officers should be alerted if there is any degradation in SaaS services.
- Must be able to provide user training on SaaS services.
- Must be able to ensure the support coverage of any new Office 365/Microsoft 365 applications and/or features.

3.7. Description of Future needs – Extended infrastructure projects

The current architecture has been described in chapter 1.

1°) **End-user equipment described in chapter 1.2** dates from 2013-2017. Most have already been renewed during the last 4 years but some old equipment remains active and will still be used, repaired if necessary and finally decommissioned after replacement by new material. All the end user equipment must be covered by maintenance contracts / warranties and ultimately disposed of under this contract. Diagnostics, updates and support must be provided by the new contractor (successful tenderer).

2°) **The network equipment** are purchased with a warranty period of 4 year and for the oldest one purchased in 2010 they are no longer under warranty. Potential new equipment (replacement or extensions) needs to be covered by a warranty extension after the default manufacturer period. All network equipment must be patched frequently.

3°) **Redesign of the shared storage** and office automation system will take place probably end 2018 or after. Some JUs may opt to migrate to Microsoft Cloud Services (for Office365 and/or Microsoft 365). Any chosen option will have to remain inside the geographic area of the European Union.

4°) Any **newly created EU body** that might be hosted in the White Atrium will need new domain in the active directory structure to be integrated as well as new share disk space from the actual storage solution.

5°) **New virtual servers** necessary for the JUs to manage project applications or for other specific needs may be requested from the new contractor (successful tenderer). The winning tender will cover at no extra cost end-user support in relation to the services provided for such new servers.

6°) **Extensions of the core infrastructure on JU(s) request:** the new contractor (successful tenderer) shall implement specific infrastructure projects that extend the core infrastructure and support the development or the evolution of Information Systems in the JUs.

7°) **Wi-Fi redesign:** As the currently implemented solution will have reached its end-of-support period by 2019, the JUs have started investigating the solution to replace it. It is also foreseen to make a redesign of the actual setup, as it has been proven not solving the entire business requirement (capacity, bandwidth, coverage, wireless/mobile offices, future/digital workplace, etc

These extensions may be requested by a particular JU, and be implemented for a part or all the participating JUs with eventually additional monthly costs for the services to be charged to the JU concerned.

Such extensions shall be implemented by means of:

- **Analysis and design:** The supplier shall conduct an analysis and a design for the requested extended infrastructure solution aiming at integrating to the existing technical environment. Cost estimate will also be provided.
- **Supplies:** Occasionally the JU could purchase hardware or software components that may be outside the standard reference configurations described in chapter 1.2 and 1.3. However, the new contractor (successful tenderer) must provide configuration and support of these assets.
- **Installation, configuration and testing:** The configuration, installation and testing of equipment and software acquired by the JTI must be performed by the winner of this tender.
- **Rollout in production:** will be under the responsibility of the new contractor (successful tenderer) after the approval of the planning and scope by the JUs.
- **Documentation and knowledge transfer to the JUs:** must be performed at all times during the contract.

4. DETAILED PROFILE DESCRIPTION

Monitoring services are all activities related to the active and manned monitoring of the components under the scope of this contract to be performed during the agreed service window for the monitoring service. The monitoring services are provided by the monitoring team composed of the **Helpdesk Assistants** (4.4) (e.g. operating the monitoring system, logging incidents based on alerts) and the **Service Manager** (4.1) (e.g. fine-tuning and optimization of the monitoring rules, documentation, handling the logged alerts).

Their overall responsibilities are:

- Develop and document monitoring procedures that meet the requirements of and adhere to defined policies agreed upon by Service provider and the Joint Undertakings.
- Provide proactive and scheduled console monitoring of infrastructure and systems in scope of this agreement, respond to alerts and take corrective action as required
- Develop and maintain standard automated scripts to perform monitoring on systems and software for which no standard monitoring plugin/pack is available
- Identify and report problems to the appropriate teams; including problems with operating systems, files, disk space and applications
- Identify and report warnings that may impact service availability if no action is scheduled (e.g. disk capacity threshold warnings)
- Provide troubleshooting, repair and escalation of problems related to the in-scope components, including active communication and notifications to Joint Undertakings according the approved escalation and communication model.
- Provide preventative measures for proactive monitoring and self-healing capabilities to limit outages.

The Service Manager is responsible for the overall delivery of services within the scope of this agreement and ensures that the agreed level of quality is met according the service levels agreed upon within the contract.

When no dedicated person has been appointed, the Service Manager takes also the role of Incident Manager (for priority1 incidents), Change Manager for small changes that do not require the presence of a dedicated project manager; and Problem Manager.

System and network administration is the main responsibility of the **System and Network Administrators** (4.2 and 4.3 respectively). These responsibilities include the proactive administration and maintenance of the technologies in scope of this contract, resolving incidents and problems received through monitoring or escalated from the service desk and handling service and change requests.

In combination with incident management and change management, the proactive maintenance and support includes the following activities:

- Manage event and workload processes across all systems in scope
- Provide technical support for all systems in scope and related operations (e.g. systems monitoring, Incident diagnostics, troubleshooting, resolution and escalation, security management, and capacity analysis) as required to meet Joint Undertakings computing requirements
- Implement, coordinate and appropriately communicate all changes to the systems in scope including those that may affect the Service Levels of any other service providers and Third Parties
- Provide proactive and scheduled console monitoring of infrastructure and respond to messages and take corrective actions as required
- Maintain standard automated scripts to perform monitoring on systems software
- Identify and report problems
- Provide a communication and escalation model for critical issues
- Provide troubleshooting, repair and escalation
- Provide preventative measures for proactive monitoring and self-healing capabilities to limit outages
- Resolve or assist in resolving problems in accordance with SLA's and escalate as required
- Start-up and shut-down systems according to defined schedules or upon approved request

- Perform system or component configuration changes necessary to support computing services in conformance with Change Management requirements
- Provide qualified support and consulting for the systems in scope
- Respond to availability and performances alerts reported by the monitoring systems or by the Joint Undertakings
- Implement and ensure that all systems in scope are up to the recommended patch level
- Follow and respect customer procedures, processes and policies
- Case follow up and resolution in collaboration with supplier support teams

They are located off-site and are by default IT professionals with a broad knowledge of the technologies used by the Joint Undertakings. Their knowledge has to be sufficient to be able to resolve most of the incidents. In case they cannot find a solution the ticket will be sent to a the next level of competence according to the escalation procedure defined in the Service Delivery Plan requested in chapter 2.6 of the annex B2.

The Helpdesk Assistant will act as contact point for all operational related issues, incidents and questions and will be prime contact point. Users can contact the Helpdesk Assistant for all IT related questions, requests and incidents by walk-in, telephone calls or via the Service Desk email contact.

The main tasks are:

- Operating the monitoring system;

The Helpdesk Assistant has the responsibility to create tickets for all incidents & service request being send towards the Service Desk. After registration, the IT Officer of the initiator of the ticket and the initiator will receive an automated e-mail including the ticket number and a direct link towards the ticket as registered in the ticketing system.

- Providing 1st line support to the end users;

He acts as a first line support for all IT related services (On-Site Service Desk) and occasionally as second line support for those fields covered by his knowledge. As such, he acts as an experienced technical generalist and a specialist of the specific environment. Service requests or incidents that cannot or are not to be resolved by the Helpdesk Assistant will be escalated to the second line support.

- Handling service requests.

He performs the day-to-day management of the requests logged in the ticketing system and takes overall commitment for the operational quality and performance of the systems. He is dedicated to ensuring superior end user experience. In addition, he/she plays an important role in proximity services including installation of hardware and software, move of hardware items and repair / replacement of defective hardware or software components. He is responsible for documentation including updates on the associated system and user documentation and procedures, and for knowledge transfer to end users, being organization and provision of targeted on-the-job training to end users related to known problems. (This excludes formal end user training like Office classroom training or intervention on external premises.)

He/she will be the single point of contact for all operational related issues and reports back to the Service Manager.

4.1. Service Manager

Description of main tasks (non-exhaustive):	• Planning • Definition of tasks and deliverables • Ensure that all documentation is reviewed once per year by all parties concerned
---	--

	• Ensure that the agreed level of quality is guaranteed according the agreed Service Levels (Quality control, Prepare and maintain quality plans • Coordinate the Root Cause Analysis process and revision on a regular basis of incidents • Ensure that Incidents and Service Requests are registered according the table of priorities by performing a monthly review of the logged Incidents and Service Requests • Performs and manages escalations regarding the overall performance and quality of the delivery of services • Provide tactical advise to IT Officers and manage adjustments in the co-operation • Ensure overall quality control and continuous service improvement of the delivered services • Follow-up of decisions and activities • Ensure management of operational team (holiday, work instructions, Human resource management, workload...) • Ensure that all activities are executed according agreed procedures and processes • Ensure that involved staff is technically trained as required to support the systems in scope • Estimation of costs, timescales and resource requirements • Organize all governance meetings and provide service reports according to the agreed reporting frequencies Timely submission and due substantiation of invoices • Management of execution of projects against time, quality and cost criteria • Management of the change control process gaining agreement for revisions to the project from project owners • Hold presentations at all levels (from team members to executive level) • Capability of integration in an international/multi-cultural environment, rapid self-starting capability and experience in team working, understanding the needs, objectives and constraints of those in other disciplines and functions • Management of conflicts
General competences and skills:	• at least C1 level in the Common European Framework for Reference for Languages in English • Experience in multicultural organisations • Experience in the public sector • Ability to reach common understanding and agreement from all stakeholders • Conflict management • Presentation skills (ability to give presentation to people of all management and team members' levels) • Ability to use the project management tools and methodologies • Ability to manage one's own time, even in the face of stressful situations • Ability to prioritise between competing tasks on a rational basis and in a decisive manner • Negotiations skills
Required proficiency in Information Services:	• Professional experience acquired in a similar technical environment to that of the JU's IT activities. • Solid experience in business processes and requirements analysis • Solid hands-on experience in managing any IT project type (web, software, infrastructure and security) • Solid hands-on experience in handling multiple projects in parallel • Solid experience in monitoring and reporting on time and cost performance during project execution • Solid hands-on experience with SAP PPM or any other project management tool • Education and work experience: • Qualification in a project/programme management methodology: PMI or Prince2 • ITIL certification in service management (ITSM) is desirable • A minimum of 3 years of professional experience as project manager

4.2. System Administrator

Description of main tasks (non-exhaustive):	• Support the installation, configuration, security, operation, and maintenance of all equipment and software related to the servers & client infrastructure and associated components • Work with IT Officers and the IT team to evaluate, design and develop solutions to address business needs and opportunities, and propose changes that would make the server environment a more effective solution • Document the technical implementation, policies and procedures to support the operational environment and participate in the design and ongoing refinement of technical implementation documentation, procedures and policies • Examine requirements documents and support creation of technical design documents, unit test, system test and capacity and implementation plans for small to complex projects • Perform, in close collaboration with the team, typical system administrative activities including daily performance monitoring, routine equipment checks and preventative maintenance, updating, controlling access permissions and privileges or issue troubleshooting and resolution • Ensure compliance with standard practices, processes and enterprise standards • Hardware and OS case follow up and resolution in collaboration with supplier support teams • Support developing, managing and testing back-up and recovery plans of the servers, server functions and data • Software packaging & deployment • Client OS image build, deployment & updates • Administer application installation and integration on production systems • Administer Virtual Systems (Hyper-V) • Administer Active Directory & GPO Settings • Administer Exchange Infrastructure • Administer OCS/Lync Infrastructure • Administer Server Infrastructure Monitoring tools • Server and client patch management • Case follow up and resolution in collaboration with supplier support teams • Other duties as required
General competences and skills:	• Good communications skills, including the ability to produce clear and concise memos, give technical explanations and present recommendations and status reports in user friendly language • Technical documentation skills • Capability of integration in an international/multicultural environment • Rapid self-starting capability and team player • Strong analytical and troubleshooting skills combined with a disciplined approach to problem solving • Able to prioritise and execute tasks in a high-pressure environment • at least B2 level in the Common European Framework for Reference for Languages in English
Required proficiency in Information Services:	• Experienced in server and storage hardware and technologies • Experienced in operating systems administration Windows and/or Linux • Experienced in server applications integration and maintenance • Experienced in scripting & packaging solutions • Experience with SCCM desirable • Experience with Active Directory, DNS and Network & Security Principles • Experience with SAN storage systems • Deep MS Exchange 2010 experience • E-mail archive, and SharePoint experience desirable

Education and work experience:	• MCSE on Windows Server 2008 is desirable • MCSE Messaging certification desirable • ITIL certification is desirable • Project Management Certification desirable
--------------------------------	---

4.3. Network Administrator

Description of main tasks (non-exhaustive):	• Support the installation, configuration, security, operation, and maintenance of all network equipment and software • Work with IT Officers the IS team (especially the Technical Infrastructure and Support Section) to evaluate, design and develop solutions to address business needs and opportunities, and propose changes that would make the network environment a more effective solution • Document the technical implementation, policies and procedures to support the operational environment and participate in the design and ongoing refinement of technical implementation documentation, procedures and policies • Examine requirements documents and support creation of technical design documents, unit test, system test and capacity and implementation plans for small to complex projects • Perform, in close collaboration with the team, typical system administrative activities including daily performance monitoring, routine equipment checks and preventative maintenance, updating, controlling access permissions and privileges or issue troubleshooting and resolution • Ensure compliance with standard practices, processes and enterprise standards • Network case follow up and resolution in collaboration with supplier support teams • Support developing, managing and testing back-up and recovery plans of the servers, server functions and data • Second level and standby support • Administer LAN/WAN infrastructure • Administer Wireless Network Infrastructure • Administer Network security components (Firewall, Remote access facilities, NAC, Load balancing, etc.) • Administer Video conferencing services • Quality of Service (QoS) handling • Cable management • Updating of the network diagram, documentation and information databases • Other duties as required
General competences and skills:	• Good communications skills, including the ability to produce clear and concise memos, give technical explanations and present recommendations and status reports in user friendly language • Technical documentation skills • Capability of integration in an international/multicultural environment • Rapid self-starting capability and team player • Strong analytical and troubleshooting skills combined with a disciplined approach to problem solving • Able to prioritise and execute tasks in a high-pressure environment • at least B2 level in the Common European Framework for Reference for Languages in English
Required proficiency in Information Services:	• Experience in managing network components from the major vendors (Cisco, Juniper, Fortinet, Open source etc.) • Strong expertise in recent network technologies • Education and work experience: • Cisco Certification (CCNA, CCNP, CCIE) desirable • Other vendor certification desirable • ITIL certification is desirable • Project Management Certification desirable

4.4. Helpdesk Assistant

Description of main tasks (non-exhaustive):	• Pickup incoming technical support calls and log them in the Ticketing System • Register all important alerts from the monitoring system as a ticket • Qualification/categorization/orientation of the ticket • Try to resolve a maximum of calls at first level • Forward technical support issues that cannot be addressed by the Help Desk to the appropriate technician • Supervise the handling of incidents according agreed service, e.g. to avoid that tickets are not resolved according to the objectives and, in case so happens, escalate and inform the escalation contacts • Analyse and detect recurring incidents and consequently create a well-documented problem ticket and present it to 2nd line • Initiate investigations such as problem analysis, troubleshooting and solution identification regarding : ○ end-user hardware, operating system, and software related problems, when possible from the Help Desk ○ basic network and server access problems for end users, when possible from the Help Desk ○ issues with WAN, Wi-Fi, firewall, VPN, VoIP etc. systems, when possible from the Help Desk • Provide initial response to the users • Keep user informed on progress towards resolution • Report incident and problem, and progress towards a solution to the appropriate team • Ensuring constant update and optimization of documentation and related work instructions as well as end-to-end follow-up of incidents and requests until closure within the knowledge base • Maintain configuration item information • Follow and respect customer procedures, processes and policies • Provide support to users in the supported languages • Ensure the availability/reachability of the Off-Site Service Desk • Ensuring correct logging of the tickets allowing to provide call statistics including incidents types, response time and help to prepare Service management KPI reports • Defining, maintaining and installing the reference configuration on all PC's, keeping software up to date, applying published patches; • Installing and moving IT hardware and software on request and replacing defective hardware or software; • Cable Management: Office/computer room cabling by means of patch cables; • Providing hardware/software usage assistance for every hardware/software delivered or already existing in the Joint Undertaking to all Joint Undertaking users; • Follow and respect customer procedures, processes and policies • Case follow up and resolution in collaboration with supplier support teams •
General competences and skills:	• Capability of integration in an international/multicultural environment, rapid self-starting capability and experience in team working • Good communication skills to communicate effectively with all levels of users • Must be knowledgeable and have supported SaaS environments • High level of service orientation • at least B2 level in the Common European Framework for Reference for Languages in English
Required proficiency in Information Services:	• ITIL Service Management knowledge • Knowledge of PC, laptop, printer as well as mobile devices • Good knowledge of operating systems (Microsoft) • Good knowledge of office applications (Microsoft Office family)
Education and work experience:	• IT Service Management ITIL foundation certification desirable • Project Management Certification desirable

5. ELEMENTS REQUESTED FOR THE TECHNICAL PROPOSAL

5.1. Overall management of the services, the service desk and telephony and internet connectivity

Tenderers shall consider the following points as the minimum content to provide. They may add elements that according to them may add value. The proposal should take account of the framework set in this Service Requirements document.

Note that the service desk proposal should cover the entire infrastructure, IT as well as telephony and Internet.

- Describe the overall management that you intend to put in place to have an integrated management of the JUs' IT and network environment and to optimise system design and updates, from higher-level project management to the on-site support and off-site service desk.
- Describe the off-site support service desk (outside core hours of the on-site support).
- Describe the role and the tasks of the requested IT/telephony support person who will be dedicated from the successful tenderer to the JU premises. She/he will act as single point of contact for the JU users on a daily basis.
- Articulate how from the single point of contact Incident management, problem management, capacity and availability planning will be implemented as managed services for the proposed infrastructure.
- Describe how the telephony and network aspects and the IT infrastructure will be integrated in your service approach.
- Describe the approach for identifying material needs (repairs, upgrades) and managing the ordering process with the JUs (that will use their suppliers of hardware/software).
- Describe the management of subcontractors and/or consortium partners, where applicable.
- Give examples of reports that can be delivered to the JU IT Managers on incident and problem types, response time, resolution time, etc.
- Give examples of reports that can be provided on system performance (traffic statistics, availability, performance, etc.) including forecasted system performance to determine if sufficient capacity exists.

5.2. Service level management

Tenderers are requested to present this part of their offer in the form of a draft SLA.

Note that the SLA proposal should cover the entire infrastructure, IT as well as telephony and Internet.

The JUs require high levels of performance and reliability for the service provided. The service covering the entire infrastructure must also be covered by the SLA document. Tenderers are required to provide in their offers details of:

- Key Performance Indicators (KPIs)
- Methodology for ensuring quality of service
- Penalties offered in case of non-compliance with KPIs.

The KPIs and corresponding penalties offered by the tenderers will form an important competitive element in the selection of the winning tender. Tenderers must include with their offer a detailed draft SLA with KPIs.

Proposals for enhanced SLA options (with cost implications) may be provided which can be the subject of negotiations with the new contractor (successful tenderer) but a minimum level of service must be described and fully priced.

Tenderers must also describe how they will confirm compliance with the SLA through regular reports and meetings. They will also describe the process for reviewing or modifying the SLA / KPIs over the life of the contract.

Notwithstanding the quantitative elements of the SLA and KPIs, on a qualitative level the JUs are seeking a cooperative relationship with the future IT services provider based on mutual respect. The JUs are seeking a supplier who has a customer satisfaction focus, which goes beyond a robotic compliance with KPIs and demonstrates a willingness to support the JUs' work in a pro-active way.

The template given in Annex B2 should be considered the minimum reference. This is to ensure a minimum continuity in the existing monitoring of services. Tenderers may extend or modify the contents of the SLA but must, as a minimum, address all the aspects in the template.

A final negotiation around the details of the SLA will take place with the signature of the first specific contract. Revision of each SLA is foreseen on a yearly basis.

The proposed SLA shall address at the minimum the following topics:

- **Service Availability:** Specify the service availability you can guarantee (please bear in mind the value must be 99,9% or better) Please explain the measures you will undertake to guarantee the proposed Service Availability;
- **Service Level Metrics:** Please indicate the service level metrics you propose with their detailed definition and their target values that you guarantee. Explain how you measure the guaranteed Service Levels at the end of each year ;
- **Incident Management:** Guaranteed Resolution time must be maximum 8 hours or less after the incident occurs; this includes a full 100% connectivity and its related services up and running again, as well if needed a full hardware replacement. The last known up and running configuration must always be applied to any incident management resolution ;
- **Proactive Management:** Please describe the technical measures you intend to undertake to proactively manage the service ;
- **Ticketing system:** Please describe the way your ticketing system is organised and operated;
- **Hotline service:** Please describe the organisation and the functioning of the Hotline service for the JUs ;
- **Penalty scheme:** Please propose a penalty scheme in case of failure to provide the minimum service levels. It has to be highlighted here that in case the KPI's are not reached the penalty should be established and will be executed in line with the article 4.6.4 of the tender specifications. ;
- **Service Level Agreement (SLA) Management:** Please describe the organisational structure you intend to set up in order to manage the proposed SLA and the communication with the Joint Undertakings. Give a description of the roles and the tasks assigned to them. Describe escalation procedures for problem handling. Describe how the renegotiation process for the SLA that you envisage.

Notwithstanding the quantitative elements of the SLA and KPIs, on a qualitative level the JUs are seeking a cooperative relationship with the future IT services provider based on mutual respect. The JUs are seeking a supplier who has a customer satisfaction focus, which goes beyond a robotic compliance with KPIs and demonstrates a willingness to support the JUs' work in a pro-active way.

Note: An SLA will be signed together with the first specific contract with the new contractor (successful tenderer). This part of your technical proposal shall be the minimum basis for negotiating the SLA. A final negotiation round of the details of the SLA will take place with the signature of the first specific contract. Revision of each SLA is foreseen on a yearly basis.

5.3. Equipment Repair Service & Disposal Channel

The assessment of the technical quality will be based on the ability of the tenderer to meet the purpose of the contract as described in the terms of reference. To this end, technical proposal shall contain the following information:

- A document describing the repair facility proposed.
- A document describing the disposal facility proposed.