ANNEX I.A

Technical specifications for

“IT INFRASTRUCTURE HOSTING SERVICES”

OPEN CALL FOR TENDERS
ACER/OP/ADMIN/14/2012

Table of contents

1. Introduction

This document contains detailed technical specifications for the requested "IT infrastructure hosting services" and describes the following:
- the technical requirements for activities and outcomes;
- the service level requirements and the reports to be provided to verify the fulfilment of the service level requirements.
- a list of staff profiles required for the delivery of the services.

2. Technical specifications

The purpose is to establish an acquisition channel for:

- The provision of dedicated managed hosting services for the Agency's IT systems and infrastructure that will be needed for the implementing of software development products, web applications, databases, services, etc.

- The provision of dedicated managed hosting services for the current ICT infrastructure Business Continuity / Disaster Recovery purposes of the Agency.

- Housing (co-location) of ICT infrastructure (such as servers, storage equipment, related networking and other equipment, etc.) owned by the Agency.

- Maintenance and support for all the above services

The Agency's ICT systems infrastructure shall be hosted in an environment optimised for continuous and secure services (i.e. hosting premises should ensure high availability and redundant access to provisions like power supply, cooling and internet connectivity in an environment with high security and protection against fire, intrusion and flooding). Also, all equipment and basic software and hardware systems (including network equipment and security) and provided support and services should focus on assuring optimal performance and uptime for the Agency's IT services.

Hosting services shall include all activities regarding configuration, testing, operation and maintenance, project management, and technical documentation of all systems hardware provided by the Contractor for the duration of contract.

2.1 Description of the requested services

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

A. IT capacity

This shall include a dedicated managed IT capacity that could be rented as a service by the Agency for a specific period of time and would include blade or rack mounted servers, virtualised servers and IT storage equipment. The indicative specifications are for:

1) Physical servers (blades or rack mounted)

   a) servers with Intel Xeon (1 CPUs, frequency ≥2,26 GHz, 4 cores), 16 GB RAM or higher, 2x 250GB hot-plug hard drives.

   b) servers with Intel Xeon (2 CPUs, 8 cores, frequency ≥2,26 GHz, 16GB or higher, 2x 250GB hot-plug hard drives),

c) servers with Intel Xeon (4 CPUs, frequency ≥2,26 GHz, 6 cores per CPU), 36 GB RAM or higher, 2x 500GB hot-plug hard drives.

2) Virtualised servers (server capacity) with CPU frequency≥2.0 Ghz, 2 cores, 6GB or higher RAM, 160GB disk space.

3) Storage

   Storage area network (SAN or equivalent), RAID options include RAID 0, 1, 5, 1/0 and 5/0, supported disk types (FC, FATA, SSD), host interface speed (4gbps), controller cache (4 GB), number of controllers (2), drives per enclosure (>=12) and provide options for 1TB, 5TB and 10TB.

4) Possibility to rent standard 42U racks or half rack (22U), private cages, etc. for certain periods of time.

All servers, SAN's and components (I/O expansions cards, etc.) should be at least VMWare vSphere (ESXi 4.1 or higher), Windows Hyper-V, Windows 2008 r2 (and higher) and Linux Redhat 5.6 (and higher) certified.

B. Hosting or collocation shall include:

- Controlled access to the Agency's racks to prevent unauthorised persons to access the Agency's equipment (e.g. locked cage or locked racks).
- Power supply and cooling with high availability and redundancy.
- Hosting premises which are secured from fire, unauthorised access and flooding.
- Temporary space for receiving, unpacking and setup of delivered equipment, for testing and installation when the Agency adds or replaces equipment without any additional cost.
- A guarantee that the Agency may remove its own equipment, software, applications, data, etc. when the contract ends and ensure cooperation with a potential new contractor for the possible handover of the equipment.

C. Connectivity shall include:

- Ability to provide redundant connections (leased lines and/or private VPN point to point connections at speeds ranging from 60 Mbps to potentially equal or more than 1Gbps) for computer access, business continuity purposes, etc. from the Agency and/or the premises of the Agency's contractor(s) to the hosting centre.
- Redundant Internet access at a capacity for the Agency of minimum 60 Mbps (upload/download) and flat-rate fee with an availability of 99.95%.
- All the needed networking devices such as switches, firewalls, routers, load balancers, proxies, etc. that will enable the proper interconnection of the Agency's ICT systems and will ensure the needed security.
- IP V6 capability.
- DNS hosting of all domains.
- Public IPs (at least 48).

D. IT monitoring and support shall include:

- Reports on the status of the hosted equipment based on its monitoring systems and on incidents which took place and could affect the operations of the Agency's equipment.
- Support to facilitate effective management of the Agency's IT systems infrastructure at the hosting centre and performance testing and monitoring of the provided infrastructure. Different levels and options of support shall be available ranging from i.e. power cycling

of servers, cable management, physically installing or removing equipment to i.e. firmware and software updates and basic system troubleshooting.
- Physical access of Agency’s staff and/or consultants to the Agency’s equipment and data without any additional cost.
- Continuous hosting site, hardware and applications monitoring.
- A service desk which shall be operational 24/7/365 for supervision, error detection, correction and notification to the Agency staff and/or Agency’s contractors.

E. Dedicated managed hosting services for the current Agency’s ICT infrastructure business continuity/disaster recovery purposes

Dedicated managed infrastructure that will act as a disaster recovery site for the already existing Agency’s ICT infrastructure.

2.2 Requirements for building and maintaining a new IT infrastructure dedicated to REMIT

The Contractor shall ensure the provision of new infrastructure on time and completely dedicated systems, network equipment and infrastructure security which shall include basic infrastructure (cabinets, wiring, etc.), aimed at obtaining an adequate architecture that will meet all the requirements of the Agency.

The engineering path to be followed in the arrangement of the infrastructure can be schematised in the following, non-exhaustive, list of actions:

- Analyse the documentation that will result from the software/application development phase;
- Complete, with the support of the project manager of the Agency’s contractor for software development products, the technical documentation, if needed;
- Collaborate and follow the recommendations of the Agency’s contractor for software development products for designing the new architecture which will meet all the requirements that will be defined in the development phase and make the realisation of the objectives possible;
- Carry out the assurance of compatibility with applications and service levels required;
- Develop documentation of the new infrastructure;
- Implement the new infrastructure;
- Carry out internal testing and finalise the documentation of operations;
- Carry out safety testing and documentation;
- Define internal operating procedures and deliver the relevant documentation to the Agency;
- Establish the requested connections to public internet and to the Agency and/or the premises of the Agency’s contractor for software development products;
- Arrange registration of the needed domain names;
- Migrate applications;
- Test infrastructure applications and provide documentation to the Agency;
- Official acceptance, which shall be conducted on behalf of the Agency by the Agency’s contractor for software development products;
- End-to-end tuning of all the developed applications;
- Provision of the agreed maintenance and supports services;
- Establishment of the requested security standards, service level agreements (SLAs), etc.

The selected Contractor shall cooperate and coordinate his activities with the Agency’s contractor for software development products in the implementation of services as specified in the request(s) for services issued by the Agency and in the relevant specific contract.

2.3 Requirements for business continuity/disaster recovery service for the existing Agency's infrastructure

The contractor shall provide the Agency with a business continuity / disaster recovery service for its infrastructure. This shall include the following (non-exhaustive) actions:

- Evaluation of the current Agency's infrastructure,
- Define all the needed requirements and prerequisites which need to be taken into account,
- Suggest the needed hardware and software (hardware components do not need to be of the same number and type as used in the current Agency's infrastructure) which will enable proper implementation of the required disaster recovery infrastructure,
- Define an action plan for the integration of software and hardware,
- Establish the necessary networking connections between the two sites,
- Document the new infrastructure establishment and procedures,
- Test the new infrastructure,
- Reproduce the Agency's infrastructure in the new one,
- Monitor the correct functioning of the new infrastructure, monitor changes in the Agency's infrastructure, etc.,
- Ensure the continuity of the new infrastructure.

The Agency has established a virtualised infrastructure within its premises so as to deliver the desired IT services. This infrastructure consists mainly of the following components:

- Five (5) HP DL380 G7 servers, each one with 2 x 6core CPUs and 36 GB RAM. Four (4) of these servers comprise a VMware cluster whereas one (1) server is used as the main physical backup server for the whole infrastructure.
- A VMware DRS & HA Cluster based on VMware vSphere 4.1 software. This cluster includes 4 VMware ESXi 4.1 hosts (the above mentioned 4 servers). High availability and Distributed Resource Scheduling are obtained through VMware vCenter. Features like VMotion and Storage VMotion are already enabled through appropriate licensing.
- An EMC CX4-120 Disk system which covers all the storage needs of the Agency's infrastructure. The system is equipped with 2 Storage Processors for redundancy and high availability, and with the necessary FC and iSCSI ports for connectivity with the virtualised environment. The system also contains 7 disk enclosures, each of which is full with 14 (FC or SATA II) disks. 13 different LUNs have been created to serve either as VMFS data stores for the virtualised environment, or for raw backup data.

The main and highly prioritised IT services provided at the Agency can be identified and briefly described in the following list. Each one of the following services is hosted on the Windows Server 2008 R2 Operating System:

- File server allowing end users to store corporate files and documents and storing end users' roaming profiles. The service is based on the File Services provided by the FSRM Role of Windows Server 2008 R2.
- Active Directory services, Name Resolution services and Dynamic Host Configuration Protocol services. These services are hosted in two different Windows Server 2008 R2 domain controllers for the sake of redundancy and high availability.
- Email Server allowing end users to communicate through email with both colleagues and external parties in the context of every day Agency's activities. The Agency uses Microsoft Exchange Server 2010 for email functionality.
- Intranet Web Server, which hosts the intranet portal of the Agency. The intranet servers supports several document libraries according to departmental needs, shared calendar, discussion board and public HR and finance and budget documents. The platform used by the intranet portal is Microsoft SharePoint 2010

- Public Web Server, which hosts the public web site of the Agency (www.acer.europa.eu) as well as a protected area for members (mainly for registered users of the member from the National Regulatory Authorities). The platform used by the Web Server is Microsoft SharePoint 2010.
- HR Application Server, which hosts e-HR tools, i.e. Leave Management, Missions Management and Performance Appraisal tools. The platform used by the server is Microsoft SharePoint 2010, along with Microsoft InfoPath 2010, Microsoft Visual Studio 2010, and Microsoft SharePoint Designer 2010.
- Print Server allowing a streamlined and centralised mechanism for delivering shared IP based printers, copiers and scanners. This functionality is served by the Print Services of the Windows Server 2008 R2 Operating System.

For the above mentioned services the Agency needs to guarantee at least 99.5 % levels of uptime and uninterrupted availability. In case of any kind of disaster at the Agency's premises such us (indicatively but not exclusively) flooding, fire or structural damages in the building, the Agency needs to resume its operational status as soon as possible. Therefore the Agency has defined the minimum acceptable Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

By defining RPO, which is usually deceptively difficult to explain, the Agency refers to the maximum time period in which data might be lost if there is a major incident affecting an IT service - not a direct measure of how much data might be lost. The required threshold for this objective is set by the Agency at 6 hours.

By defining RTO, the Agency refers to the duration of time within which the service levels must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. This objective includes the time to fix the problem without a recovery, the recovery itself, testing and the communication to the users. Decision time for the Agency's representative is not included. The required threshold for this objective is set by the Agency at 3 hours.

The tenderer should map the above mentioned metrics to the underlying IT systems and infrastructure that support these processes. The tenderer should determine the most suitable recovery strategy. Below is a list of the most common strategies for data protection that the Agency acknowledges. This list is by no means exhaustive and the Agency is open to any further well documented suggestions:

- Backups made to tape and sent off-site at regular intervals,
- Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk,
- Replication of data to an off-site location, which overcomes the need to restore the data (only the systems that need to be restored or synchronised), with the use of storage area network (SAN) technology,
- High availability systems which keep both the data and system replicated off-site, enabling continuous access to systems and data.

The selected Contractor shall include control measures in the suggested Business Continuity Process / Disaster Recovery Process. Indicatively but not exclusively, the following measures are mentioned:

- Preventive measures - these controls are aimed at preventing an event from occurring.
- Detective measures - these controls are aimed at detecting or discovering unwanted events.
- Corrective measures - these controls are aimed at correcting or restoring the system after a disaster or an event.

2.4 Factors critical for the provision of IT hosting infrastructure services

For the provision of infrastructure hosting services the following critical factors should be taken into account:

a) **Confidentiality of data.** The data collected by the Agency for its institutional activities must be treated in a way to ensure the highest level of confidentiality. In addition, as certain data could be used for legal actions, the data integrity must be guaranteed during many years, also for use in lawsuit.

b) **The Contractor shall refer to the Information Technology Infrastructure Library (ITIL) framework** (at least v.3) for the definition of its operating procedures for maintenance and service desk. The use of a common framework is required to ensure coordination between the application services and infrastructure services, in particular with reference to the interactions related to the following processes and functions:

- Service Desk (function),
- Incident Management Process,
- Problem Management Process,
- Change management process,
- Release management process,
- Configuration management process.

The tenderer must provide a description of the processes and functions listed above, using the ITIL concepts and terminology, highlighting also the points of connection and coordination with the Agency and any subcontractors.

c) **Security policies**

The Contractor must align its procedures to international standards on safety systems (with particular reference to the standard ISO 27001) and the following indications on safety:

- prevent misuse of the information processing facilities and systems;
- control and regulate access to the information assets of the Agency, carried out by the Contractor's staff as part of activities under the contracts for outsourcing;
- ensure compliance with security policies set by the Agency, ensuring the dissemination of the principles at all staff who interacts with the information system;
- ensure the availability of information, facilities and systems of information processing;
- produce and maintain plans for the continuity of services provided under contracts resulting from the procedure and submit these plans to periodic testing;
- have in place all necessary actions to reduce risks related to the following threats:
    - Breaches of security due to poor organisation,
    - Accidents and malfunctions of computer systems,
    - Unauthorised use or misuse of equipment, information processing systems, system utilities or applications, unauthorized removal of objects,
    - Unauthorised access to information or systems,
    - Injection of malicious code, worms, trojans, and generally any type of computer virus,
    - Inappropriate or non-conforming user,
    - Any type of attack from the internet,
    - Malicious use of the infrastructure or application by the supplier's staff in order to cause damage to third parties.
- collect reports and formalise timely reports on all breaches of security, actual or alleged, and where required provide support for the conduct of investigations;
- achieve and maintain updates according to the needs of the Agency, with the involvement of contractors, procedures in support of security policy, including:
    - Classification and control of assets,

- Protection of natural resources,
- Logical security of information,
- Management of removable media,
- Back-up information,
- Management of accidents and malfunctions related to safety,
- Check for viruses and spam,
- Ensuring continuity of services, in compliance with contractual service levels,
- Periodic review of the validity and effectiveness of countermeasures taken in time, by defining appropriate metrics and implementation of monitoring and control.

d) Vulnerability tests

The Contractor is required to perform, either on its own or through a third party, at least quarterly, tests of vulnerabilities in systems engineering and infrastructure involving at least:

- scanning of physical systems, looking for patterns of basic software and application considered unsafe and vulnerable to attack (vulnerability assessment);
- penetration tests that evaluate the resistance of certain systems to simulated cyber-attacks (penetration testing);
- the vulnerability tests which should include testing of systems and applications; the Contractor shall inform the Agency of these tests in advance and the Agency reserves the right to appoint any trusted third party to oversee these tests during their execution;
- a dedicated managed infrastructure which will not be shared with other customers of the Contractor; the Agency reserves the right to have, without notice, the vulnerability tests done by a designated third party. In this case the Contractor is required to provide the required support through coordinated activities between the resources devoted to the application services and resources dedicated to the infrastructure services, under the supervision of the Agency;
- reporting test results to the Agency; the Agency reserves the right to make the test results a subject of analysis and may use designated third parties to identify potential problems and suggest corrective actions, if necessary. The implementation of these corrective actions shall not represent any additional cost to the Agency.

e) Helpdesk and support service procedure requirements

The selected Contractor shall provide at least the following levels of support which shall include at least the following (non-exhaustive) tasks:

Level 1 support

- Performing hardware inventory of 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 from colocation environment;
- Device labelling.

Level 2 support

- 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;
- Performing any Agency's supplied system administration procedure;
- 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.

f) Software licences needed for the operation of the hardware infrastructure and technical support

Costs for all licenses necessary to provide the services (software needed for the operation of the infrastructure) shall be an integral part of the infrastructure costs, calculated as a fixed monthly fee. This shall also include, if needed, the cost of permits, costs for technical support of specific choices and platforms used for hosting. This shall represent an active technical support with various vendors of various components of the technological platform.

The Contractor shall ensure that the systems, hardware and software defined configurations are always appropriate for the operation of applications and able to cope with the workloads.

During the implementation of the contract no additional costs should be borne by the Agency.

3. Service level requirements

The minimum service level requirements (SLR) defined below are mandatory for the selected Contractor. Any liquidated damages in case of non-fulfilment of the required service level requirements shall be set in the service level agreements (SLAs) annexed to the Framework contract and 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, are binding.

The service level requirements will provide the basis for the SLA for the Framework Contract and specific contract(s) which will be defined by the Agency's contractor for software development products, after approval by the Agency.

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;
- **Power availability:** Electricity power for the Agency's infrastructure and services shall be 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:** Tenderers should ensure that access to the Agency's Data Centre Services facility(s) will be monitored and restricted at all times. Efforts to ensure security to the facility is 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;
- **Network availability:** The Tenderer'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 tenderer's 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 tenderers IP backbone network, which should include tenderer's owned and controlled routers and circuits (including any transit connections);
- **Internet availability:** Internet connections provided by the tenderers 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 tenderers upstream Internet providers' or peers' BGP interfaces. Internet latency should be measured to tenderers' 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:** Tenderer should 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 tenderer'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):** Tenderers should 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 10 minutes from the submission of a report of DoS activity.
- **Outage notification:** Tenderers should 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 one (1) hour after the occurrence of any unavailability affecting the Agency's infrastructure.
- **Disaster Recovery / Business Continuity:** Tenderers shall be able to insure the activities of the Agency's 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, ensuring the provision and management of all hardware and software resources and connectivity, to ensure the operation and provision of services to users in case of disaster. 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 service level agreement 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 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 Contractor may propose additional benchmarks, before 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 - Planned unavailability of the infrastructure) 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 one service 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.

3.2 Reporting of service actual levels during the contract

The Contractor shall provide monthly reports to the responsible project manager at the Agency, in the layout proposed by the Contractor and accepted by the Agency.

The report, with complete and accurate information at the end of the previous month, must be delivered at least on the 10th day of the current month.

The monthly report shall include:

- A summary of the activities.
- Data on the request processing and specific contracts from the start of the framework contract.
- The actual values of the quality indicators (as calculated by the Contractor) and compared with SLR/SLA.
- The risks identified, the problems encountered and the corrective measures proposed and undertaken.
- Analytical billing report.

The content and layout requirements of the report may evolve to better suit the Agency's needs. This evolution will be handled in collaboration with the Contractor.

4. Professional profiles

4.1 A-level profiles

Project Manager (PM)	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Economics
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; – Experience in quality assurance procedures; – Must have successfully completed the project management for at least 2 international projects.

4.2 B-level profiles

ISO 27001 Lead Auditor	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Economics, Mathematics, Business Administration
Tasks	– Consultancy, supervision and responsibility for the implementation of Information Security Management Systems according to ISO/IEC 27001. – Consultancy and supervision for risk assessment and establishment of Information Security Plan. – Final Audit according to ISO/IEC 27001of the implemented ICT infrastructure.
Knowledge and skills	– ISO/IEC 27001 certification. – Excellent knowledge of information systems security, threats and vulnerabilities, risks, selection of security controls, ISO 27001 auditing techniques, interview techniques. – Audit reporting.
Experience	– At least 5 years' experience in the relevant field. – Completed at least 4 audits for a total duration of at least 20 days, as well as 3 audits as a lead auditor for a total duration of at least 15 day.

IT Infrastructure Architect	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Mathematics
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's 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. – Excellent experience in Data Centre relocation and transformation projects, – Wide experience of current infrastructure technologies and with major IT companies including Oracle, Sun, Microsoft, IBM, HDS, RedHat, NetApp and VMWare. – Good experience in network systems design, implementation and management. – 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

Storage Area Network Engineer	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Mathematics
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. – 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, Vion, NetApps, Hitachi, Clarion, and IBM and their associated file system structures. – Experience in supporting Fiber 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
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. – At least 2 certifications on proposed LAN component (router – switching, etc.). – Working knowledge of major networking components and hardware components.

4.3 C-level profiles

Virtualisation Engineer	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Mathematics
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 3 years' experience in the relevant field. – At least 1 certification on the proposed virtualisation component. – Excellent experience in designing virtualisation infrastructure that meets customer requirements.

Infrastructure Server Engineer	
Minimum education	University degree in the field of Computer Science, Computer Engineering, Mathematics
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.
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.
Experience	– At least 3 years' experience in the relevant field. – 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.