ANNEX II + III: TECHNICAL SPECIFICATIONS + TECHNICAL OFFER

Contract title: Supply of IT equipment for enhancing e-Government

Publication reference: NEAR/SKP/2021/EA-OP/0085

Columns 1-2 should be completed by the contracting authority
Columns 3-4 should be completed by the tenderer
Column 5 is reserved for the evaluation committee

Annex III - the contractor's technical offer

The tenderers are requested to complete the template on the next pages:

- Column 2 is completed by the contracting authority shows the required specifications (not to be modified by the tenderer),
- Column 3 is to be filled in by the tenderer and must detail what is offered (for example the words ‘compliant’ or ‘yes’ are not sufficient)
- Column 4 allows the tenderer to make comments on its proposed supply and to make eventual references to the documentation

The eventual documentation supplied should clearly indicate (highlight, mark) the models offered and the options included, if any, so that the evaluators can see the exact configuration. Offers that do not permit to identify precisely the models and the specifications may be rejected by the evaluation committee.

The offer must be clear enough to allow the evaluators to make an easy comparison between the requested specifications and the offered specifications.

Basic Technical Specification (minimum requirements)

1. Tenderers are to offer standard production models matching or exceeding the specifications stated in the outline specifications – see detailed Technical Specifications. The tenderer shall ensure that the functions and features of the equipment meet the listed minimum conditions and should submit equipment brochures and catalogues showing the specifications of the equipment.
2. All specifications details for each item are the minimum requirements. Any improvements on the specifications or additional features offered should be clearly identified in the Tenderer's offer.
3. All the equipment shall be provided complete with the necessary accessories, cables and/or parts such as to ensure that the unit is capable of operating to the required technical and quality specifications.
4. All manuals and operating guidelines must be translated in Macedonian. Both the original and the translated versions will be handed over to each of the final beneficiaries.

OVERVIEW

1 BACKGROUND

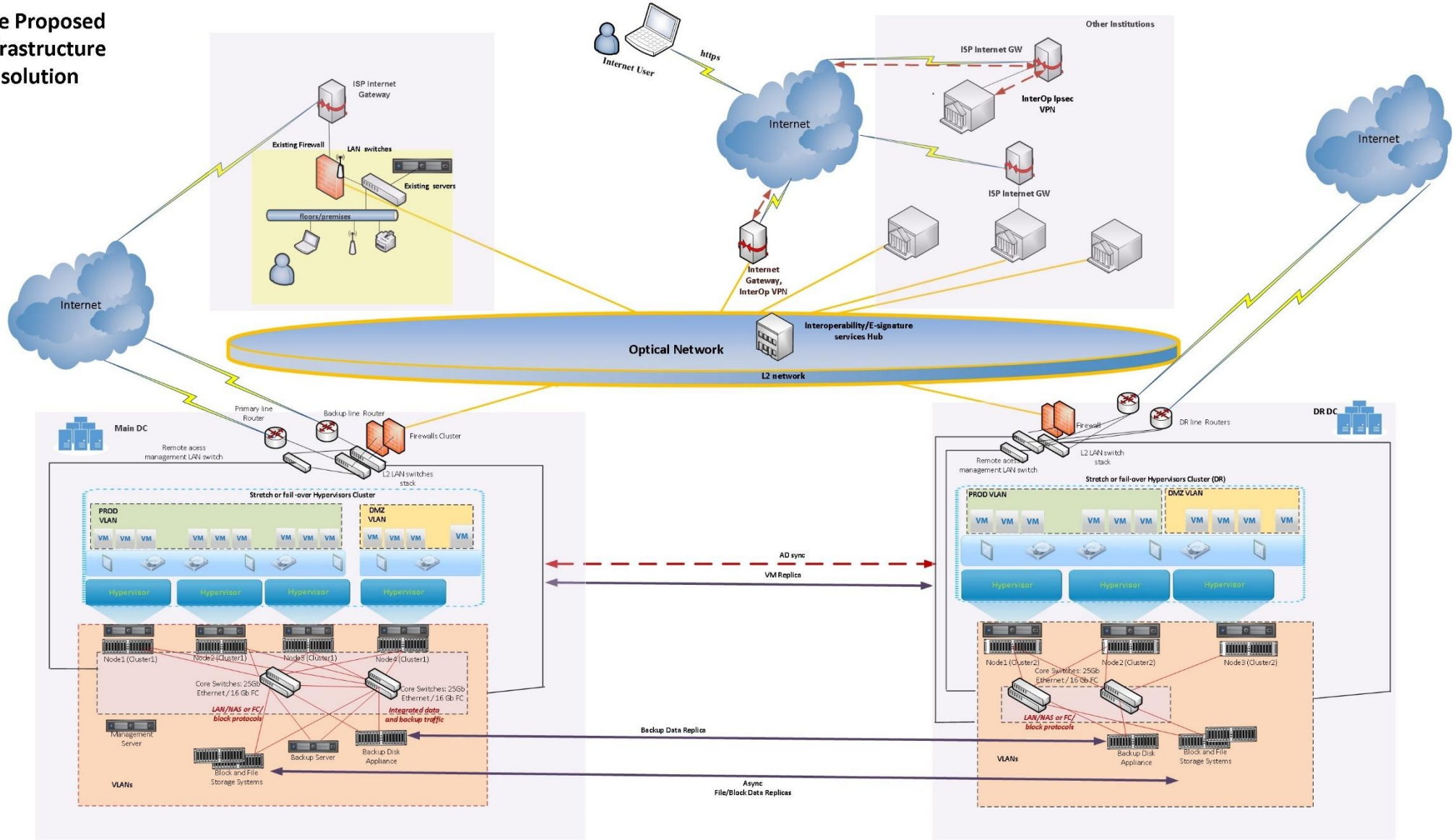
The purpose of this project is to extend the offer of available e-services on the National portal for citizens and businesses and to improve the delivery and quality of public services both to citizens and to businesses. Several public registers will also be digitalised under the project.
The authorities of the Republic of North Macedonia have already undertaken steps to ensure the delivery of e-services. To do so efficiently, the authorities have to further digitalize registers which will allow them to offer these services.
This is a strategic objective of the country, set out in the Public Administration Reform Strategy.

2 High level system description

The overall objective of the project is to provide ICT infrastructure that will host new developed registers and e-services for enhance public service delivery and reduce time and costs of citizens and businesses when interacting with public bodies.

The system should provide sufficient IT resources for operation of newly developed registers and e-services on main data centre, to provide business continuity on the disaster recovery site and should provide secure connectivity of beneficiaries that are still not part of the central Interoperability platform.

The Proposed Infrastructure solution

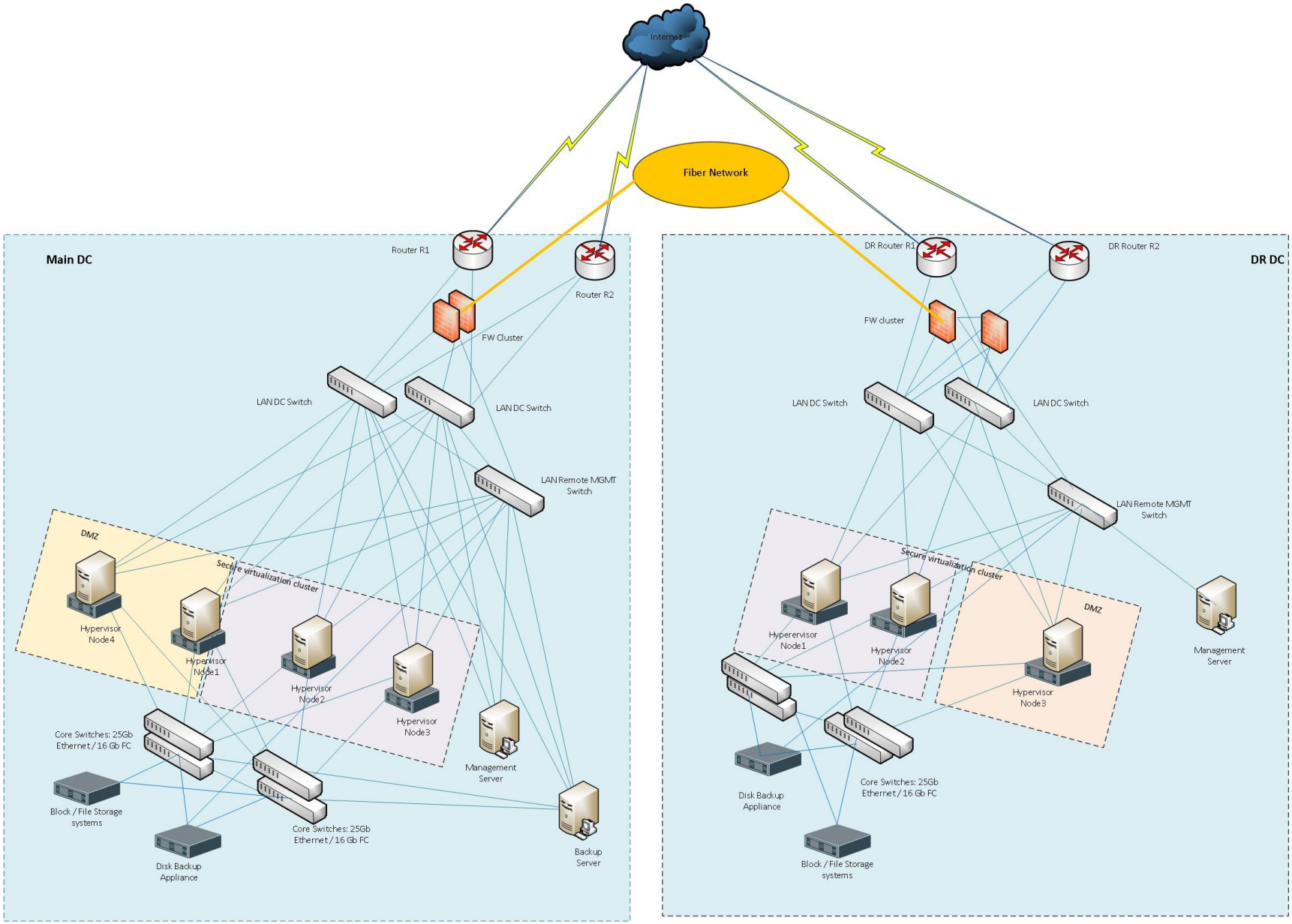


The proposed solution should include all required perpetual licenses and grant proper licensing according the proposed hardware infrastructure.

The equipment will be placed at two data centres of an external service provider that is providing collocation services to MISA. There will be 11 (eleven) beneficiaries where network and server equipment should be installed in order to be connected on Interoperability platform.

The solution includes on both the main and DR sites a cluster of virtualisation hosts for server virtualisation of resources, containing four nodes per site, with server hardware virtualisation, central block-based storage systems, network connectivity, and managed as an independent site with enough resources to provide full site redundancy in case of an outage.

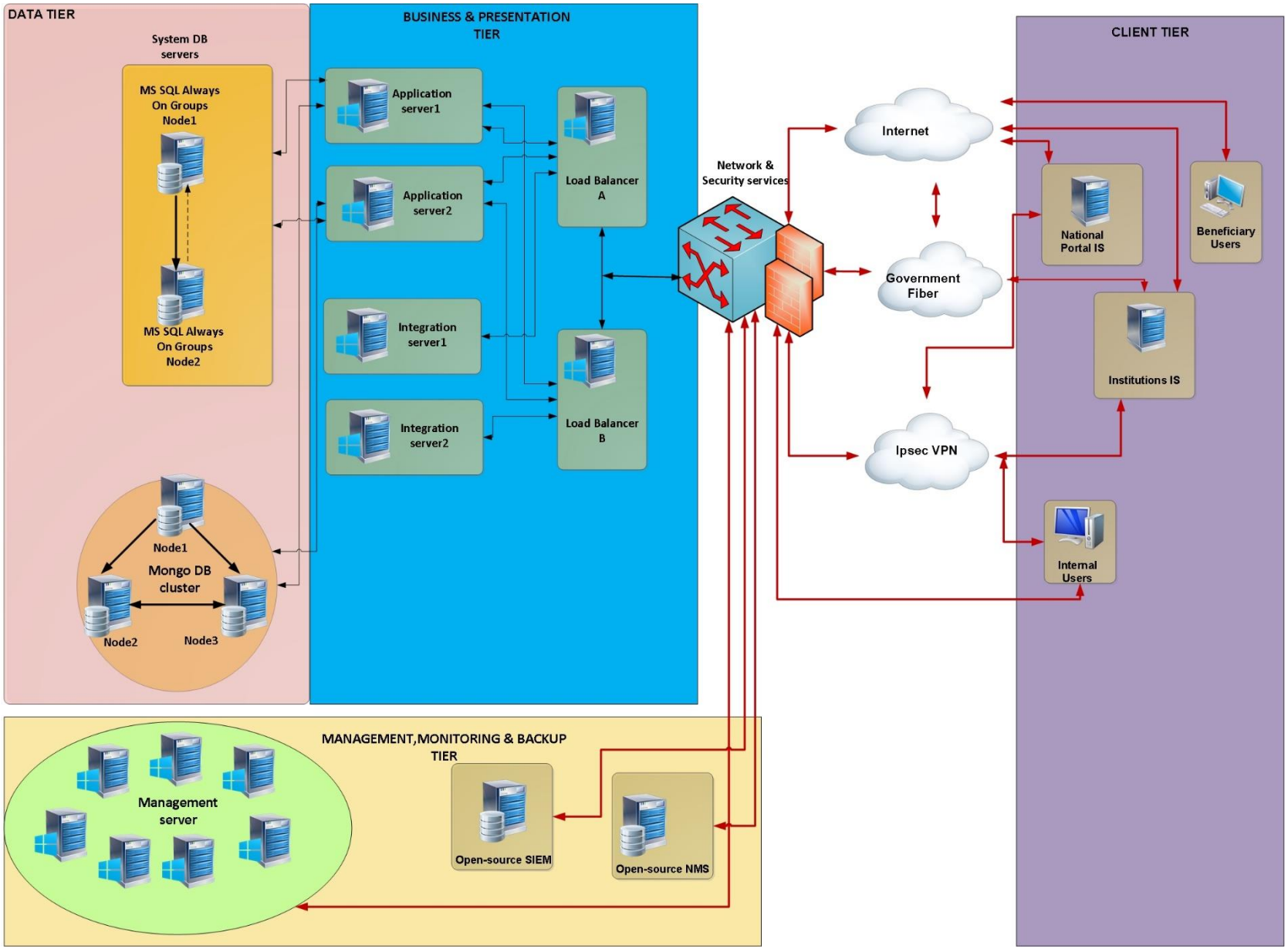
The following diagram represents the critical infrastructure elements to be located inside the new virtualized data centres at both locations, which must be supplied, installed and put into operation with this procurement:


Internet
Fiber Network
Main DC
Router R1
Router R2
FW Cluster
LAN DC Switch
LAN DC Switch
LAN Remote MGMT Switch
DMZ
Secure virtualization cluster
Hypervisor Node4
Hypervisor Node1
Hypervisor Node2
Hypervisor Node3
Core Switches: 25Gb Ethernet / 16 Gb FC
Block / File Storage systems
Disk Backup Appliance
Core Switches: 25Gb Ethernet / 16 Gb FC
Management Server
Backup Server
DR DC
DR Router R1
DR Router R2
FW cluster
LAN DC Switch
LAN DC Switch
LAN Remote MGMT Switch
Secure virtualization cluster
Hyperervisor Node1
Hypervisor Node2
DMZ
Hypervisor Node3
Management Server
Disk Backup Appliance
Core Switches: 25Gb Ethernet / 16 Gb FC
Block / File Storage systems

The solution also includes an integrated solution for centralised data backup and recovery, that will provide appropriate backup polices for the protection of valuable data.

The architecture of the main system is modern virtualisation Tier 1 hypervisor design and based on 4 nodes, with all necessary hardware resources (processor, memory, disk access, network connectors) placed in a common chassis. The solution is designed to be scalable on demand, with expansion capabilities up to 90 nodes per site.

The following diagram represents the virtual machines to be located inside the new server virtualisation platform at both locations:


DATA TIER
System DB servers
MS SQL Always On Groups Node1
MS SQL Always On Groups Node2
Node1
Mongo DB cluster
Node2
Node3
BUSINESS & PRESENTATION TIER
Application server1
Application server2
Integration server1
Integration server2
Load Balancer A
Load Balancer B
Network & Security services
Internet
Government Fiber
Ipsec VPN
CLIENT TIER
National Portal IS
Beneficiary Users
Institutions IS
Internal Users
MANAGEMENT,MONITORING & BACKUP TIER
Management server
Open-source SIEM
Open-source NMS

3 *Detailed Technical Specifications*

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
A	Unless specified differently for specific item, the Power supply standards for all electrical equipment shall be powered with 220V, 50Hz AC and shall be equipped with IEC-309 C13/C14 power plugs. All devices shall be compliant with electrical safety standards of the beneficiary country and European Union and follow EEC CE Marking Directive.				
B	Unless specified differently for specific item, the equipment shall comply to IEC 60 529 standard for indoor IT equipment operating under temperature range of 15°C – 30°C, relative humidity range of 20% – 80% and IP 20 protection level.				
1.	**Compute virtualisation platforms for main and DR site**	**Quantity: 1**	**Manufacturer:** **Model:**		
1.1.	Highly secure and resilient server virtualisation solution				
1.2.	Solution overview: The compute virtualisation platform solution must be constituted as a single cluster consisting of multiple (minimum four at the Primary site and minimum three at the DR site) server hardware nodes allowing for compute resource virtualisation, external network connectivity and a single unified management system. The Compute virtualisation platform at both locations must be configured for replication of data (VM level) between each other for full disaster recovery and fault tolerance functionality.				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
1.3.	Compute virtualisation platform architecture - nodes: The solution must be created as a single integrated system, which contains a minimum of four (4) individual nodes at the primary site and three (3) nodes at the DR site, with all necessary hardware resources (processors, memory, network connectors) placed in a standard chassis with a maximum size of 1U per node for space-efficient placement in collocated data centres. The solution must be designed fully redundant, with accounted complete node failure into the redundancy mechanism. The applications and databases running on the deployed virtual machines must be designed to operate primarily as active/active, or active/passive at both locations, depending on the system design of the various applications, technical capabilities of the system software and licensing capabilities. In case of unavailability of the primary site all resources, applications, systems and business processes must be made fully available at the DR site, within a maximum RTO value of two (2) hours.			
1.4.	Compute virtualisation platform architecture – server node overview: a) 1U height rack-mount server with x64 architecture, should support 64-bit operating systems and applications, type 1 hypervisor support. b) The server node must include cable management arm as well as a sliding rack mount kit for placement in a standard 19" rack cabinet.			
1.5.	Compute virtualisation platform architecture – virtualisation system			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	scalability: The compute virtualisation platform solution must be able to scale on-demand and non-disruptively, up to a minimum of 90 nodes.			
1.6.	Compute virtualisation platform architecture – memory of the nodes: Each node must contain a minimum of 384 GB working RAM memory, with a speed of at least 3200MT/s. Each node must be expandable to a minimum of 4TB total RAM memory.			
1.7.	Compute virtualisation platform architecture – processors of the nodes: Each node in the cluster must contain a minimum of two processors (CPUs), with a minimum base operating frequency of 2.6GHz or faster, a minimum of 24-cores per CPU socket and a minimum of 128 of L3 cache or more per CPU socket. The CPUs must be of newest generation, produced with a 7nm or smaller process technologies.			
1.8.	Compute virtualisation platform architecture – disk capacity of the nodes: No built-in disks – each server node must be configured for Boot-from-SAN through the Fibre Channel network.			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
1.9.	Compute virtualisation platform architecture – network connectivity of the nodes: Each node must contain a minimum of three separate ethernet network adapters: - One dual port 1Gbps adapter with 1Gbase-T ports - One four-port 25GbE SFP28 Ethernet adapter with either included optical modules or TWINAX cables for connectivity to the LAN switches. - One dual-port 25GbE SFP28 Ethernet adapter with either included optical modules or TWINAX cables for connectivity to the LAN switches. - All adapters must be from a single manufacturer / supported by the same driver.			
1.10.	Compute virtualisation platform architecture – fibre channel SAN connectivity of the nodes: Each node must contain a minimum of two separate fiber channel host bus adapters for connectivity to the block-based storage system: - Two dual port 16 Gbps PCIe adapters with included 16 Gbit/sec SFP ports - Included cables for connectivity to the SAN switches. - All adapters must be from a single manufacturer / supported by the same driver.			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
1.11.	Compute virtualisation platform architecture – virtualisation software compatibility of the nodes: The server nodes must be compatible with either the Citrix Hypervisor, the VMware vSphere or the Microsoft Hyper-V virtualisation technologies.			
1.12.	Compute virtualisation platform architecture – server nodes I/O interfaces: Each node must contain a minimum of: a) Front side ports: 1 x USB 2.0 port; 1x MicroUSB port, 1 x VGA port. b) Rear side ports: Minimum 2 x USB 3.0; 1x serial port, 1 x VGA port. c) Internal ports: at least 1x USB 3.0; d) The server must include a functionality to programmatically disable any USB port			
1.13.	Compute virtualisation platform architecture – server nodes power supplies and fans: Each node must contain a minimum of redundant Hot-Plug Platinum class power supply modules, not less than 1350W each. The server nodes must be designed to operate when cooling with fresh air, with temperatures up to 40 ° C and relative humidity up to 85%.			
1.14.	Compute virtualisation platform architecture – server nodes remote management:			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	Each node must contain: a) Embedded system management controller with own processing power which is FIPS 140-2 Level 1 certified b) Built-in wireless module for wireless diagnostics over BLE / NFC. c) The embedded controller should allow proactive for error alerts on network adapters, memory, internal drives (SAS HDDs and SSDs, NVMe), fans, power modules, RAID controllers, Fibre Channel HBAs, ambient server temperature (including graphical displays) on SSD) and other errors. d) The controller should allow quality control / bandwidth of remote access to the server. e) The controller should include independent 10/100/100 Mbit Ethernet adapter for real time remote management. The controller should provide agent-free hardware, firmware and performance monitoring, including inventory, crash screen / video capture, boot capture, and alerting. f) The controller should support the IPMI 2.0 protocol, VNC connectivity with the operating system, include HTML 5 based browser interface, SMASH-CLP, Dynamic DNS, DHCP with Zero Touch functionality, NFS v4 and WSMan support, E-mail alerts, Virtual console (KVM) as well as virtual media attachment. g) Front-facing LCD panel for local management and diagnostics.			
1.15.	Compute virtualisation platform architecture – server nodes security: a) Each node must include a Trusted Platform Module			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	(TPM) version 2.0 which is FIPS 140-2 and Common Criteria certified b) Each node must include silicon-based security to authenticate the BIOS and the firmware of the server with a cryptographic Root of Trust, during the server boot process, meeting the NIST SP 800-193 standard. c) For remote management security the server management system must include a two-factor authentication mechanism, which randomly generates a token and sends it to an administrator email when logging into the management controller d) Boot process verification for protection of the node when booting an operating system, meeting the NIST SP 800-147B and NIST SP 800-155 standards. e) Functionality for secure erasure of data from drives f) All server node firmware files must be digitally signed with SHA-256 hashing and 2048-bit RSA encrypted by the manufacturer. g) Functionality for digital signature verification of the cryptographic hash of the boot image that it matches the signature which was stored in silicon by the factory. h) Functionality for live scanning of the node BIOS, which verifies the integrity and authenticity of the BIOS image in the primary ROM when the node is powered on. i) Functionality for recovery from a corrupted BIOS or an operating system image j) Chassis intrusion detection functionality built-in to the management system			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
1.16.	Compute virtualisation platform architecture nodes warranty and support: The offered server nodes must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the week, and which provides on-site hardware replacement. The offered solution must include direct manufacturer access to latest software patches, updates and service packs, for all elements of the solution.			
1.17.	Compute virtualisation platform architecture - virtualisation management solution: The solution must have a central control application which allows: a) Installation and adding or removing nodes to the cluster b) Configuration of individual nodes c) Monitoring the nodes and the devices in the cluster d) Display processor and memory utilization at both cluster and node levels e) Installation of upgrades and patches of the virtualisation software equipment without impact to current work processes f) Integrated GUI console that performs functions related to the hardware, such as the provisioning of new nodes, upgrading system patches, checking the status of the system and shutting down the system. g) Support for predictive failure analytics with proactive alert notifications h) The solution must enable orchestration procedure for recovery which includes testing, failover and failback of each			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	or groups of virtual servers. i) The solution must enable automatic system log management and monitoring of system events and notifications in relation to the virtual environment and the hardware equipment, and report the status of the hardware to the manufacturer automatically. The solution must include a license for a centralised and automated GUI management of the virtualisation platform.			
1.18.	Compute virtualisation platform architecture - Virtualisation Hypervisor functionalities: a) The Virtualisation software shall provide a Virtualisation layer that sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability and security. b) Virtualisation software shall have the capability to create Virtual machines with up to 750 virtual processors and up to 20 TB virtual RAM, for the guest operating systems supported by the hypervisor. c) Virtualisation software should support live Virtual Machine migration from one physical host to another and between virtual switches, with enhanced CPU compatibility. Virtualisation Software Should support live Virtual Machine migrations across Physical Hosts, between virtual switches, between two different virtualisation managers or between servers physically separated over a long distance leading up to 150ms of network latency d) Virtualisation software should perform live migration of			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	virtual machines files from one storage array to another without any Virtual Machine downtime. It should support this migration from one storage protocol to another (ex. FC, iSCSI, NFS, DAS). e) Virtualisation software should support 4k native storage. f) Virtualisation software shall have High Availability capabilities for the virtual machines in the sense, if in case one server fails all the Virtual machines running on that server shall be automatically restarted to another physical server running same virtualisation software. The feature should be independent of Guest Operating System Clustering and should work with FC/ iSCSI SAN and NAS shared storage g) Virtualisation software should provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions. This option should be supported for up to 8 virtual CPUs per virtual machine with up to 128 GB RAM. h) The solution should provide option for securing virtual machines with offloaded antivirus and antimalware solutions without the need for agents inside the virtual machine with integration with 3rd party Anti-Virus/Anti-Malware solutions i) The solution should provide secure access and account management through identity federation with ADFS. j) The solution should support for increasing capacity by adding CPU, Memory or any other devices to virtual machines on an			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	as needed basis without any disruption in working or downtime for supported operating systems k) Virtualisation software shall be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts. l) The solution should be able to automate energy efficiency and optimizes power consumption by turning off hosts during periods of reduced demand. m) The solution should provide a virtual switch which can span across a virtual datacentre and multiple hosts should be able to connect to it. n) The solution must enable prioritization of storage and network access by continuously monitoring I/O load of a storage volume and over the network, and dynamically allocating available I/O resources to virtual machines according to business needs. o) Virtualisation software should support TPM 2.0 hardware modules and option to adds a virtual TPM device to shield guest OS from Operator or in-guest attacks p) Virtualisation software should support Virtual Machine Encryption, with data-at-rest encryption for virtual machine data and disks. q) Virtualisation software should support persistent memory. r) Virtualisation software should support Nvidia GRID vGPU, which enables native 2D and 3D graphics performance for virtual machines, including support for multiple vGPUs per			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	VM. s) Licensing should be based on the per physical processor licensing model, and the offer must include adequate licenses for all physical CPU sockets included in the solution.			
1.19.	Compute virtualisation platform architecture – Management platform for virtual environments: The virtualisation solution must include single point of management across all different hosts and virtual machines, which will provide HTML 5 based GUI, with option to check all alarms and notifications, simple search across all different components and which will include integrated solution for backup and recovery. The solution must enable simple orchestration which can automate some of the tasks, and which will also provide audit trail of all configuration changes. Beside this, the integrated management should support: a) Desired state configuration management capabilities. b) Create and generate interoperability and pre-upgrade checks report, which will help in upgrade planning. c) Provide native high availability configuration d) Provide native backup and restore functionality of the integrated management solution. e) Enables unified visibility and management across on-premises environment and cloud-based environments. It is required to provide license which will cover all different hosts and VM's in the environment.			
1.20.	The virtualisation solution must include the following warranty and support:			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	The system must be delivered in a unified way, from a single manufacturer and a single support, authorized to take support calls for both the hardware and the system software part of the solution – full system functionality. The offered solution must include direct manufacturer access to latest software patches, updates and service packs, for all elements of the solution. The offered solution must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the week, and which provides on-site hardware replacement.				
2.	**Central file and block-based storage system for the virtualisation platform, for main and DR sites**	**Quantity: 2**	**Manufacturer:** **Model:**		
2.1.	Unified central storage for the virtualisation infrastructure main functionality: A midrange all-flash type storage system to provide redundancy, scalability and high availability, with no single point of failure. The system should have at least two redundant storage controllers working in an active/active mode for both file and block-based data. The connection between controllers should be via backplane or via direct connected cables.				
2.2.	The provided unified storage solution needs to provide the standard features and functionalities listed below: a) Mirroring and parity-based RAID protection mechanism, protecting data against a simultaneous single or double				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	drive failure. b) Zero detection, deduplication & compression of the stored block and file-based data c) Thin provisioned disk capacity d) Block Access for external hosts, using either the Fibre Channel or iSCSI protocols e) File based access for external hosts, using all of the following protocols: CIFS, SMB v3.1, NFS v4.1, VVols, FTP, SFTP. f) Built in Health Check and Performance functions for ease of management g) Not to be server vendor specific, and to support at least servers from Cisco, Dell, HPE, Fujitsu, Lenovo. h) Should support Live-Migration for LUNs between different RAID sets i) Should support Quality-of-Service functionality for host access j) OpenStack Cinder Driver to provision and manage the block volumes from OpenStack environments k) Required licensing should be included for all required functionalities.			
2.3.	The provided unified storage solution must offer the following security features and functionalities: a) The storage system should support distributed sparing for faster drive rebuilds and for expanding a pool using a single drive. b) The storage system should provide data at rest encryption within the system, with included functionality for			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	controller-based or external key management of self-managed keys. c) File-Level Retention functionality meeting the requirements of SEC rule 17a-4(f) d) The storage system must be validated according the FIPS 140-2 Level 1 criteria. e) The storage system operating system (firmware) must be certified according the Common Criteria for IT Security Evaluation at the Evaluation Assurance Level EAL2+ f) The storage system should support a ride-through time of at least 10 msec, for tolerating electrical power input interruptions.			
2.4.	The provided unified storage solution must offer the following data copy and access features and functionalities: a) Local snapshot and full volume copies of block and file-based data b) Offloaded Data Transfer (ODX) c) Remote native synchronous and asynchronous storage-based data replication functionality, for both block and file-based data, between other systems for disaster recovery purposes, with no capacity limitations d) Remote shipping of snapshots functionality for disaster recovery purposes e) Block-based data copy from external storage systems functionality, for data migration f) Functionality to recover data to any point in time through journaling, for disaster recovery purposes			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
2.5.	The provided unified storage solution must include the following front-end ports for host access: a) A minimum of 8 x 25Gb SFP28 usable ethernet ports, per system, for both file and block protocols b) A minimum of 8 x 16Gb SFP+ usable fibre channel ports, per system c) A minimum of 4 x 10Gb Base-T usable ethernet ports, per system, for both file and block protocols			
2.6.	The provided unified storage solution must include the following usable disk capacity available to the attached host nodes: a) A minimum of 34TiB usable SSD based capacity, protected against dual drive failure, available for both file and block-based data. The included disk capacity must not account for any data optimization technologies, such as zero detection, compression, deduplication or thin provisioning. b) The disk configuration must provide a minimum performance of 59.000 IOPS to the hosts, for a mixed workload of 80% read and 20% write I/O and 8K block size. The system must be capable (designed) to provide at least ten times more IOPS performance then the initial sizing. c) At least one dedicated hot-spare drive must be included in the system, with monitoring function on drive health and which will be automatically initiated for proactive copy of any failing drive.			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
2.7.	The provided unified storage solution must include the following system capacity: a) A minimum of 128 GB cache memory to be included, per system b) Minimum supported internal drive count in the system should be 475. c) Redundant power supply / fan modules d) Included battery capacity for de-staging of the system cache memory in case of prolonged power failure (more than 10 msec). e) Maximum of 2U form factor, with a standard 19" rack mounting kit and cables.			
2.8.	The provided unified storage solution must include the following standard monitoring and management functionalities: a) Simple Network Management Protocol v3 support b) NT LAN Manager (NTLM) support c) Distributed File System (DFS) support d) TLS 1.2 support for management e) Address Resolution Protocol (ARP)			
2.9.	Unified storage solution warranty and support requirements: The offered solution must include direct manufacturer access to latest software patches, updates and service packs, for all elements of the solution. The offered solution must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	week, and which provides on-site hardware replacement.				
3.	**Central block-based storage system for the data platforms, for main and DR sites**	**Quantity: 2**	**Manufacturer:** **Model:**		
3.1.	Block-based central storage for the databases and application server infrastructure main functionality: A midrange all-flash type storage system to provide redundancy, scalability and high availability, with no single point of failure. The system should have at least two redundant storage controllers working in an active/active mode for block-based data. The connection between controllers should be via backplane or via direct connected cables.				
3.2.	The provided Block-based storage solution needs to provide the standard features and functionalities listed below: a) Mirroring and parity-based RAID protection mechanism, protecting data against a simultaneous single or double drive failure. b) Deduplication & compression of the stored block-based data c) Thin provisioned disk capacity d) Block Access for external hosts, using either the Fibre Channel or iSCSI protocols e) Built in Health Check and Performance functions for ease of management f) Not to be server vendor specific, and to support at least servers from Cisco, Dell, HPE, Fujitsu, Lenovo.				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	g) Should support Live-Migration for LUNs between different RAID sets h) Should support Quality-of-Service functionality for host access i) Required licensing should be included for all required functionalities.			
3.3.	The provided Block-based storage solution must offer the following security features and functionalities: a) The storage system should support distributed sparing for faster drive rebuilds and for expanding a pool using a single drive. b) The storage system should provide data at rest encryption within the system, with included functionality for controller-based or external key management of self-managed keys.			
3.4.	The provided Block-based storage solution must offer the following data copy and access features and functionalities: a) Local snapshot and full volume copies of block-based data b) Offloaded Data Transfer (ODX) c) Remote native synchronous and asynchronous storage-based data replication functionality, between other systems for disaster recovery purposes, with no capacity limitations d) Block-based data copy from external storage systems functionality, for data migration e) Remote disaster recovery solution for two sites, where			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	data that is written to a volume is automatically sent to both copies at the two separate sites. When one site would no longer be available, the other site must be able to provide access to the volume. Each copy of a volume should be fully independent and is at a distinct site. The solution must allow the storage devices to indicate the preferred ports for hosts to use when they submit I/O requests using Asymmetric Logical Unit Access (ALUA).			
3.5.	The provided Block-based storage solution must include the following front-end ports for host access: a) A minimum of 8 x 16Gb SFP+ usable fibre channel ports, per system b) A minimum of 4 x 10Gb Base-T usable ethernet ports, per system			
3.6.	The provided Block-based storage solution must include the following usable disk capacity available to the attached host nodes: a) A minimum of 36TiB usable SSD based capacity, protected against dual drive failure. The included disk capacity must not account for any data optimization technologies, such as compression, deduplication or thin provisioning. b) At least one dedicated hot-spare drive must be included in the system, with monitoring function on drive health and which will be automatically initiated for proactive copy of any failing drive.			
3.7.	The provided Block-based storage solution must include the following			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	system capacity: a) A minimum of 64 GB cache memory to be included, per system b) Minimum supported internal drive count in the system should be 1000. c) Redundant power supply / fan modules d) Included battery capacity for de-staging of the system cache memory in case of prolonged power failure. e) Maximum of 2U form factor, with a standard 19" rack mounting kit and cables.				
3.8.	The provided Block-based storage solution must include the following standard monitoring and management functionalities: a) Simple Network Management Protocol v3 support b) TLS 1.2 support for management				
3.9.	Block-based storage solution warranty and support requirements: The offered solution must include direct manufacturer access to latest software patches, updates and service packs, for all elements of the solution. The offered solution must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the week, and which provides on-site hardware replacement.				
4.	**SAN networking solution for the virtualisation platform, for main and DR site**	**Quantity: 4**	**Manufacturer:** **Model:**		
4.1.	Data centre SAN networking infrastructure solution:				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	The solution must include a minimum of two Fibre Channel switches in 1U 19" form factor, which offer 16 Gb storage connectivity to the DC elements. Each switch must include: a) A minimum of 24 x 16Gb short-wave SFP+ usable ports (with LC connector), per switch b) Support for software and hardware upgrades to provide up to 48 ports of 16-Gbps Fibre Channel, per switch c) Minimum of 250 Buffer credits for a single port in a group d) Dedicated bandwidth per port e) Switch types supported: F_Port, E_Port, FL_Port, B, SD, ST, and TE f) Fabric In-order delivery g) zone-based QoS h) redundant and hot-swappable power supplies			
4.2.	SAN networking solution advanced features support: a) FIPS 140-2 compliance b) FC-SP-2, Revision 2.71 support c) FC-NVMe d) Fibre Channel Inter-VSAN Routing (IVR) e) NPIV f) VSAN based Traffic Isolation,			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	g) Dynamic Path Selection, h) min. 16 ports per ISL trunk, i) Fibre Channel Security Protocol (FC-SP) switch-to-switch authentication j) Hardware zoning by using Access Control Lists (ACLs). k) Port Channel with multipath load balancing l) Stateful process restart				
4.3.	Data centre SAN networking infrastructure management functionality: a) Min. 1x 10/100/1000 Mbps Ethernet (RJ-45) out-of-band, b) 1 x serial port (RS-232), c) 1 x USB. d) Command-Line Interface (CLI) e) SSH v2 f) Secure FTP				
4.4.	Data centre SAN networking infrastructure warranty and support requirements: The offered solution must include direct manufacturer access to latest software patches, updates and service packs, for all elements of the solution. The offered solution must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the week, and which provides on-site hardware replacement.				
5.	**External networking solution for the virtualisation platform, for main and DR site**	**Quantity: 4**	**Manufacturer:** **Model:**		

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
5.1.	Data centre infrastructure external networking solution: The solution must include a minimum of two Layer 3 network switches in 1U 19" form factor, which offer 25/100 GbE external connectivity to the DC elements. Each switch must include: a) A minimum of 24 x 25GbE SFP28 usable ports, per switch b) A minimum of 4 x 100GbE QSFP28 usable ports, per switch c) Minimum of 8GB memory included d) Maximum switching latency of 885 nano seconds. e) Minimum switching capacity of at least 2.15 Tbps full duplex f) Minimum switch throughput of 950Mpps g) Minimum packet buffer memory of 32MB h) Minimum SSD capacity of at least 32 GB.			
5.2.	The external networking solution switches for the must include support for the following standard protocols: a) RFC 4271 b) RFC 2545 c) IEEE 802.1t d) IEEE 802.3ad e) RFC 5340 f) RFC 3315 g) RFC 4552			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
5.3.	The external networking solution switches must integrate with the virtualisation solution through the following protocols: a) iSCSI TLV, including DCB converged lossless transactions b) VXLAN and Data Centre Bridging eXchange (DCBx) c) Control Plane Services, d) 802.1AB LLDP and 802.1w RSTP e) 802.1Qbb Priority-Based Flow Control and 802.1Qaz Enhanced Transmission Selection (ETS) f) IEEE 1588v2, Expedited Forwarding PHB Group VRF (BGPv4/v6) g) LAG load balancing The switches must include hot swappable and redundant power supplies as well as fans.			
5.4.	The provided external networking solution switches must include the following standard monitoring and management functionalities: a) RFC 3176 b) RFC 8040 c) Simple Network Management Protocol v2 support d) RestConf APIs for Layer 2 e) IPv6 TACACS support f) Ansible, Puppet, Chef and SaltStack support for management			
5.5.	External networking solution warranty and support requirements: The system must be delivered in a unified way, from a single			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	manufacturer and a single support, authorized to take support calls for both the hardware and the system software part of the solution – full system functionality. The offered solution must include direct manufacturer access to latest software patches, updates and service packs, for all elements of the solution. The offered solution must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the week, and which provides on-site hardware replacement.				
5.6.	Assembly, integration, configuration and testing: All components must be fully assembled, upgraded, configured, tested and put into production operations at both the main and the DR site. Data replication must be configured between the sites.				
6.	**Centralised backup solution for the main and DR site**	**Quantity: 1**	**Manufacturer:** **Model:**		
6.1.	Integrated and highly available solution for centralised data backup and recovery				
6.2.	Solution overview: The solution must be constituted as a centralised platform for backing up and restoring data to and from disk, LTO magnetic tape and cloud, as a single unified management system. The software solution must provide granular data recovery, recovery of individual files, folders, emails, databases, spreadsheets or entire virtual				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	machines directly from the backup storage. The solution must include an independent backup server located at the Primary site. The solution must include an independent and certified storage system, specialized for long term backup storage with de-duplication functionality, one at the Primary site and one at the DR site, with data replication between the two systems.			
6.3.	Backup software installation and configuration: The central backup server software can be installed on multiple OS (minimum on Windows and Linux). The central backup server software can be installed in a cluster system at a single site, for high availability. The central backup server software should be installed at each site, with replication of the data sets between the main and the DR site.			
6.4.	Backup software management and reporting: a) The central Backup software must support multi-tenancy administration b) The central Backup software must support Granular User Roles Administration c) The central Backup software must have an integrated reporting mechanism d) The central Backup software should be managed from a centralised console			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	e) The central Backup software must include an authentication and authorization feature integrated with the standard LDAP and AD facilities			
6.5.	Backup software functionality: a) The central Backup software should allow for of complete recovery backup catalog by reading data from the tape or disk even in the event of complete failure and losing backup software catalog b) The central Backup software should support multiplexing. c) The central Backup software must support "check point" functionality (restart of backup job from the last backup check point, etc.). The check point can be set granularly (file level, folder level) d) The central Backup software must support Full, Incremental (Transaction Log), Differential, Copy Backup for MS SQL e) The central Backup software must support encryption of backup data f) The central Backup software must support writing and reading from the disk devices at the same time g) The central Backup software must support sharing of devices between multiple storage nodes / media agents h) The central Backup software must include Dynamic Parallel Savestreams, where the backup SW breaks the single save stream into smaller save streams i) The central Backup software must support Synthetic full backups			
6.6.	Backup software compatibility:			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	a) The central Backup software must support Windows, Linux (Cent OS, Debian, Fedora, Oracle Linux, Red Hat, Suse, Redflag Asianux, Ubuntu), Unix (Solaris, AIX , HP - UX) , Mac OS platforms as well as applications on those platforms: SQL , Exchange , Oracle , SharePoint , Meditech , DB2 , Lotus Domino / Notes , Informix , Sybase , PostgreSQL, SAP HANA, MySQL b) The central Backup software should support leading virtualisation technologies, including support for VMware, Hyper-V and OpenStack KVM c) The central Backup software should support vSphere including automatic detection and graphic display of virtual servers d) The central Backup software must support the MS VSS technology (Volume ShadowCopy service) for backup of MS SQL, MS Exchange, MS AD, Hyper - V e) The central Backup software must support granular Exchange backup / restore f) The central Backup software must support Hyper-V image and GLR backup / restore g) The central Backup software must support Hyper-V CSV backup / restore h) The central Backup software should support Block based backup (Changed block tracking) for Windows and Linux file systems, as well for Hyper-V and Exchange i) The central Backup software should must include REST API for integration with Self-service portals j) The central Backup software must include client direct			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	support, with no media agent required in the data path between backup the client and the backup target k) The central Backup software must support integration with the offered Purpose-Built Backup Appliance and it must support "smart" replication, which is under control of the backup SW and the SW is aware of both copies (on the primary and on the DR site) l) The central Backup software must support MongoDB integrated backup / restore m) The central Backup software must support MySQL integrated backup / restore n) The central Backup software must support PostgreSQL integrated backup / restore			
6.7.	Central backup server hardware: a) Standard 1U height rack-mount server b) A minimum of one CPU module, with 7nm production technology and operating at a minimum of 3.1GHz operating frequency c) Minimum of 8 CPU cores and 16 hardware threads d) A minimum of 64GB DDR4 RAM memory with a transfer speed of at least 3200MT/s e) Included TPM 2.0 module f) Minimum of 2 x 480GB hot-swap SSD 6Gbps 2,5" drives with a capacity of at least 3 DWPDs with hardware RAID 1 protection g) 12Gb/s PCI Express RAID Controller, with support for RAID 0, RAID 1 and RAID 10, SATA SSDs in Pass-Thru mode, T10-DIF and 4K Native Sector.			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	h) Minimum of 2 x 1Gbit RJ-45 Ethernet ports and 2 x 25 Gbit SFP28 Ethernet ports i) Minimum of 2 x Dual Port FC PCIe 3.0 Host Bus adapters (HBA), with transfer speed of 14.000 Gbps full-duplex of each port and at least 255 virtual functions. The adapter must support T10-PI protection from data corruption and include short wave laser modules with an LC connector. j) Included integrated graphic card with a resolution of 1920x1200 and at least 16 MB video frame buffer. k) Front ports included: at least 1x USB 2.0 port; 1x MicroUSB port, 1 x VGA port. l) Rear ports included: at least 2x USB 3.0; 1x serial port, 1 x VGA port. m) Internal ports included: at least 1x USB 3.0; n) Included redundant and Hot-Plug Platinum class of power supplies and fans, with C13/C14 PDU power cables o) Included rack mount kit and a cable management arm for a standard 19" rack			
6.8.	Central backup server management controller: a) Embedded system management controller with own processing power and a wireless module for wireless diagnostics over BLE / NFC. b) The controller should allow proactive for error alerts on CPUs, network adapters, memory, internal drives (SAS / SATA HDDs and SSDs), fans, power modules, RAID controllers, ambient server temperature (including graphical displays) on SSD) and other errors. c) The controller should allow quality control / bandwidth of			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	remote access to the server. d) The controller should include independent 10/100/100 Mbit Ethernet adapter for real time remote management. The controller should provide agent-free hardware, firmware and performance monitoring, including inventory, crash screen / video capture, boot capture, and alerting. e) The controller should support the IPMI 2.0 protocol, VNC connectivity with the operating system, include HTML 5 based browser interface, SMASH-CLP, Dynamic DNS, DHCP with Zero Touch functionality, NFS v4 and WSMan support, E-mail alerts, Virtual console (KVM), Virtual media. f) The server must also include a front-facing LCD panel for local management and diagnostics. g) For management security the server must include Two-factor authentication, FIPS 140-2 support, Secure Root-of-Trust functionality, Secure Run and Secure Move for protection when running and operating the operating system and applications.			
6.9.	Central backup server operating system: a) The server must include a perpetual license for an operating system which is certified and compatible with the backup software b) The server must be certified for at least VMware ESXi, MS Windows Server Hyper-V, Canonical Ubuntu Server LTS and other virtualisation technologies			
6.10.	Central backup appliances for Primary and DR site general description:			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	A Purpose-Built Backup Appliance, capable of secure backup data storage, with advanced space efficiency technologies. One identical appliance should be included for each site, with functionality for remote replication of the stored backup data.			
6.11.	Central backup appliances efficiency functionalities: a) The device must include support for inline data deduplication b) In addition to deduplication, data saved on the device should also be compressed. Different method of the compression must be possible (lz, gz, gz-fast) c) The device must also include software plugin for deduplication at the source and must be fully supported and integrated with the offered backup SW			
6.12.	Central backup appliance for Primary and DR site capacity: a) Required throughput of the devices in native transfer mode must be at least 4 TB/hour b) Required throughput of the device with use of SW plugin for deduplication on the source is at least 7 TB/h c) Minimum usable capacity of the unit must be at least 32 TB d) The devices should be offered with a minimum of 4 x 10 GBaseT Ethernet ports with speed of 10Gb and 2 x 10Gb SFP+ ports.			
6.13.	Central backup appliance storage functionalities: a) The backup data can be sent to the devices across a LAN using CIFS, NFS and NDMP protocols b) The backup data can be sent to the device through the SAN /			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	FC (Storage Area Network / Fibre Channel protocol) c) The LAN and SAN transfer methods must work simultaneously d) The device must support and use software plug-ins for enabling deduplication before sending it to the device (Deduplication on the source) e) The device must also include software plugin for deduplication on the source and must support integration with applications via their native backup tools. Supported applications must be as a minimum Oracle RMAN, IBM DB2, SAP, SAP Hana, MS SQL, MS Exchange, Hortonworks and Cloudera. License shouldn't be included in the offer f) Deduplication must be done with variable block size g) Deduplication must be global, between all shares, folders and VTL pools on the device. h) Device must support the verification of the written data i) Device must support encryption for replication j) Device must support encryption for data-at-rest k) Device must support replication of deduplicated and compressed data to the same or a similar device l) Device should be able to replicate the entire content, as well as the granular content, i.e., replication of individual virtual tape pools or individual folders m) Device must support archiving of data with ability to lock files (retention lock) n) The Device must support Multitenancy			
6.14.	Central backup system warranty and support requirements:			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	The system must be delivered in a unified way, from a single manufacturer and a single support, authorized to take support calls for both the hardware and the system software part of the solution – full system functionality. The offered solution must include direct manufacturer access to latest software patches, updates and service packs, for all elements of the solution. The offered solution must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the week, and which provides on-site hardware replacement.				
7.	**Management server for main and DR site**	**Quantity: 2**	**Manufacturer:** **Model:**		
7.1.	Management server overview: c) 1U height rack-mount server with x64 architecture, should support 32- and 64-bit operating systems and applications, type 1 hypervisor support. d) The server must include cable management arm as well as a sliding rack mount kit for a standard 19" rack cabinet.				
7.2.	Management servers' number of processors / cores: Minimum 1 physical processor, with a minimum of 8 cores and 16 threads, minimum of 32MB level 3 cache, operating at a frequency of not less than 3.1 GHz.				
7.3.	Management server RAM requirements:				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	Minimum of 96GB DDR4 RAM memory with a speed of 3200MT/s. The server must be expandable up to 2TB total memory.			
7.4.	Management server's Internal storage: The servers should be offered with at least 2 x 480GB hot-swap SSD 6Gbps 2.5" drives, with a capacity of at least 3 DWPDs with hardware RAID 1 protection			
7.5.	Management servers Storage Controllers: Hardware 12Gb / s PCI Express RAID Controller, with support for SATA SSDs in Pass-Thru mode, T10-DIF and 4K Native Sector. The controller should support RAID levels RAID 0, RAID 1, and RAID 10.			
7.6.	Management servers ethernet network ports Minimum included ports per server: a) 2 x 1Gbit RJ-45 ports. b) 2 x 25 Gbit SFP28 ports			
7.7.	Management servers I/O interfaces: e) Front side ports: Minimum 1 x USB 2.0 port; 1x MicroUSB port, 1 x VGA port. f) Rear side ports: Minimum 2 x USB 3.0; 1x serial port, 1 x VGA port. g) Internal ports: at least 1x USB 3.0;			
7.8.	Management servers power supplies and fans:			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	Redundant Hot-Plug Platinum power supply modules, not less 550W. The server must be designed to operate when cooling with fresh air, with temperatures up to 40 ° C and relative humidity up to 85%.			
7.9.	Management server's remote management: h) Embedded system management controller with own processing power and a wireless module for wireless diagnostics over BLE / NFC. i) The controller should allow proactive for error alerts on CPUs, network adapters, memory, internal drives (SAS / SATA HDDs and SSDs), fans, power modules, RAID controllers, ambient server temperature (including graphical displays) on SSD) and other errors. j) The controller should allow quality control / bandwidth of remote access to the server. k) The controller should include independent 10/100/100 Mbit Ethernet adapter for real time remote management. The controller should provide agent-free hardware, firmware and performance monitoring, including inventory, crash screen / video capture, boot capture, and alerting. l) The controller should support the IPMI 2.0 protocol, VNC connectivity with the operating system, include HTML 5 based browser interface, SMASH-CLP, Dynamic DNS, DHCP with Zero Touch functionality, NFS v4 and WSMan support, E-mail alerts, Virtual console (KVM), Virtual media. m) The server must also include a front-facing LCD panel for local management and diagnostics. n) For management security the server must include Two-factor			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	authentication, FIPS 140-2 support, Secure Root-of-Trust functionality, Secure Run and Secure Move for protection when running and operating the operating system and applications.			
7.10.	Management servers operating system: Included perpetual license for an enterprise class server type operating system, capable of joining the centralised MS Active Directory infrastructure as a member server. The offered operating system must include a centralised browser-based Administration Centre software, Advanced Threat Protection (ATP), Datagram Transport Layer Security (DTLS) for encryption of virtual network traffic between virtual machines and Low Extra Delay Background Transport (LEDBAT) latency optimized network congestion control The offered operating system must include the appropriate license for the offered hardware resources, as well as a hypervisor functionality for server virtualisation of at least two additional VMs, and additionally built-in support for Kubernetes. The offered operating system must include access to latest releases of hotfixes and service packs during a period of at least five years. Proposed solution must be fully compatible with Beneficiary current infrastructure. Please refer to https://mioa.gov.mk/?q=mk/node/1320 for detailed information.			
7.11.	Management servers' warranty: The offered servers must include direct technical support during a period of 12 months, which is available 24x7, all days of the week, and which			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	provide on-site hardware replacement.				
8.	**Main and DR site Web and application traffic load balancing and protection solution**	**Quantity: 2**	**Manufacturer:** **Model:**		
8.1.	Web and application traffic load balancing and protection solution overview: a) The solution must be designed as a virtualized fully redundant load balancing system, at each site b) The solution must be constituted as a centralised platform for redundant load balancing of web, application and other types of client and data server traffic. c) The solution must provide HTTP/2 support, perform Application Delivery and operate at L4-L7. d) The solution must perform Server Load Balancing (SLB) for TCP/UDP based protocols and TLS (SSL) Offload. e) The solution must perform Layer 7 Content Switching. f) The solution must perform Transparent caching for HTTP/HTTPS as well as compression of static and dynamic HTTP/HTTPS content.				
8.2.	Load balancing solution advanced security: a) Built-in Web Application Firewall (WAF) functionality, with real-time application threat mitigation and daily rule updates.				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	b) Types of threats mitigated by the solution: c) Data loss prevention d) SQL injection e) Cookie tampering f) Cross site request forgery g) Cross site scripting h) SNORT-rule compatible Layer 7 intrusion prevention system (IPS). i) DDoS mitigation, including Layer 7 rate-based attacks. j) PCI-DSS Section 6.6 compliance. k) Black List (Access Control List). l) IP reputation filtering, with automatic updates.			
8.3.	Load balancing solution capacity: a) Standard Load Balancer Throughput capacity for each site must be at least 3 Gbps and also support at least 4,000 SSL transactions per second (TPS). b) The solution must be scalable and support up to 1,000 virtual, up to 1,000 real servers and up to 3,000,000 Layer 4 Concurrent Connections. c) The solution must support 802.1Q and 802.3ad redundancy protocols.			
8.4.	Load balancing solution balancing functionality: a) Round Robin balancing method			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	b) Weighted Round Robin balancing c) Least Connections balancing d) Weighted Least Connection balancing e) SDN Adaptive balancing f) RDP Login ID (L7) balancing g) HTTP/HTTPS WebClient-session (L7) balancing h) Source-IP address-based Hash balancing i) Weighted source IP address-based hash algorithm balancing			
8.5.	Load balancing solution certificate and encryption support: a) Support for FIPS 140-2 Level 1 b) Support for TLS 1.2 & 1.3 support c) Support for EV (Extended Validation) certificates d) Support for OCSP certificate validation e) Support for STARTTLS mail protocols (POP3, SMTP, IMAP) f) Support for Server Name Identification (SNI)			
8.6.	Load balancing solution session persistence support: a) Types pf session persistence supported: b) By source IP (L4) c) By TLS (SSL) SessionID (L4) d) By HTTP/HTTPS Browser-session (L7) e) By HTTP/HTTPS WebClient-session (L7) f) By RDP Login ID (L7) g) Port Following for mixed HTTP/HTTPS sessions			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	h) Session reconnection for Microsoft RDS			
8.7.	Load balancing solution authentication support: a) Two-factor authentication support b) Forms to Forms based authentication c) Active Directory and SSO authentication d) RADIUS & LDAP authentication e) Multi-domain and authentication f) Authentication using X.509 client certificate			
8.8.	Load balancing solution management support: a) The solution must be delivered and configured with a centralised management console which includes 3rd party load balancer support. b) Centralised orchestration and performance management support. c) Support for automated backups and scheduled firmware updates			
8.9.	Load balancing solution warranty and support: a) The offered solution must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the week. b) The offered solution must include direct manufacturer access to latest software patches, updates and service packs, for all			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	elements of the solution.				
9.	**Remote access Management Network switches for primary and DR sites**	**Quantity: 4**	**Manufacturer:** **Model:**		
9.1.	Switches for the dedicated equipment Ethernet management ports overview: Programmable pipeline ASIC switches with micro-engine capabilities, which enable Full Flexible NetFlow (FNF). The LAN switches at each site must be redundantly connected (stacked) and provide connectivity for all network management ports of the various systems. The switches at each site must operate as a single virtual switch, with a single management plane and control plane. Switch stack failover must take place in under 50 milliseconds.				
9.2.	Management Network switches Ports: a) Included minimum of 24 x RJ-45 1000Mb auto-sensing, ports b) 4 x 1/10 Gbit SFP+ uplink ports c) 2 x stacking (stacking cables included) d) RJ-45 console port with RS232 signaling				
9.3.	Management Network switches Advanced network functionalities:				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	a) Signed images and Secure Boot functionality b) Included near-real-time dashboard GUI monitoring of the entire network, as well as per client, application, switch and wired client c) Layer 3 capabilities: ISIS, routed access, OSPF, EIGRP and RIP d) IPv6 routing, using OSPFv3 and EIGRPv6 e) Auto recovery of switch ports when an error occurs f) Differentiated Services Code Point (DSCP) field classification g) Quality of Service (QoS) and 802.1p Class of Service (CoS) h) Shaped Round Robin (SRR) i) Access Control Lists (ACLs) j) AES-128 MACsec inter network device encryption, with MACsec Key Agreement (MKA)			
9.4.	Management Network switches Performance: a) Committed Information Rate (CIR) b) 802.1p Class of Service (CoS) c) MAC addresses: 32K d) IPv6 routing entries: minimum 2,000 e) Switch capacity: minimum of 128Gbps / 208 Gbps stacked f) Forwarding rate: minimum of 95 Mpps / 152 Mpps stacked g) Flash memory: Minimum of 4 GB h) DRAM memory: Minimum of 2 GB i) Jumbo frames supported at size of 9198 bytes or more			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	j) Protocol-Independent Multicast (PIM) as well as Source-Specific Multicast (SSM) k) VLANs supported: minimum of 4,092 l) Virtual interfaces supported: minimum of 512			
9.5.	Management Network switches IEEE Compliance and support: a) IEEE 802.1AE b) 802.1D Spanning Tree c) 802.1p Ethernet Priority d) 802.1Q VLAN e) 802.1S Multiple Spanning Tree (MSTP) f) 802.1W Rapid Spanning Tree (RSTP) g) 802.1x-Rev h) 802.3 10BASE-T and 802.3ab Gigabit Ethernet (1000BASE-T) i) 802.3ad Link Aggregation with LACP j) 802.3at, 802.3af and 802.3x			
9.6.	Management Network switches management and security: a) Embedded RFID tag for asset and inventory management b) Protocol-Independent Multicast (PIM) for IP multicast routing is supported, including PIM sparse mode (PIM SM), and Source-Specific Multicast (SSM) c) SMIv1, SNMPv2			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
9.7.	Management Network switches Power and mounting: a) Energy Efficient Ethernet (EEE) b) Redundant fans c) Redundant power supplies per switch d) Rack mount kit included e) Rack PDU Power cables included.				
9.8.	Management Network switches solution warranty and support: a) The offered solution must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the week. b) The offered solution must include direct manufacturer access to latest software patches, updates and service packs.				
10.	**Redundant Next-Generation Firewall cluster system for primary and DR sites**	**Quantity: 2**	**Manufacturer:** **Model:**		
10.1.	Overview of the Firewall cluster systems: Cluster of a redundant Next Generation firewall nodes or appliances, quantity 2 per site, with an internal storage capacity of not less than 200 GB SSD per appliance/node.				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
10.2.	Firewall cluster systems connectivity / interfaces: a) Support for up to 24 x 1 or 10 Gbit interfaces per appliance b) Support for up to 4 x 10GE SFP+ interfaces per appliance c) Included minimum of 12 x 1G RJ-45 interfaces per appliance d) Included minimum of 4 x 10GE SFP+/TWINAX interfaces per appliance			
10.3.	Firewall cluster systems performance: a) Stateful inspection firewall throughput of minimum 10 Gbps per appliance b) Firewall throughput with active application control mechanisms, including IPS functionality: minimum of 4.9 Gbps per appliance c) Concurrent Sessions with active application control mechanisms: minimum of 2 million per appliance d) New Sessions/Second with active application control mechanisms: minimum of 26.000 per appliance e) IPsec VPN Throughput (1024-byte packets): minimum of 1.5 Gbps per appliance f) VPN peers: minimum of 7,400 per appliance			
10.4.	Firewall cluster systems Redundancy: a) High Availability Configuration: included Active/active and active/standby clustering functionality b) Redundant dual power supplies per appliance			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	c) hot-swappable fans per appliance			
10.5.	Firewall cluster systems Advanced security features: a) Included Indicators of Compromise (IoC) intelligence b) Included detection, blocking, tracking, analysis, and containment of targeted and persistent malware c) Included URL categorization, with a minimum of 75 URL categories included d) Included URL Filtering, with a minimum of 275 million URLs pre-categorized e) Threat correlation by endpoints f) Support for the OpenAppID application-layer network security plugin g) Included threat intelligence: minimum per IP, URL and DNS			
10.6.	Firewall cluster systems Device / system management: a) Console port b) Web interface c) USB port d) Included Centralised configuration, logging, monitoring, and reporting			
10.7.	Firewall cluster systems Multi-Factor Authentication (MFA)			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	functionality for secure remote system access: a) Included cloud-based solution for using a second source of validation, like a phone or token, to verify user identity before granting access to the firewall VPN service. b) Included functionality for security keys from an offered mobile application (for iOS and Android phones, with push notifications), as well as from SMS, phone call-back, hardware token and biometrics (U2F, WebAuthN). c) Ability to enforce policies for the user based on global settings as well as per application or per authorized networks d) Single Sign-On (SSO) integration with different applications as well as cloud services. e) Central web-based dashboard for self-enrolment and self-management of the users f) Included license for a minimum of 25 users. g) Included direct manufacturer subscription for a period of 12 months, as well as direct technical support.			
10.8.	Firewall cluster systems Updates and subscription: a) The firewall appliances must include a license for a minimum of 25 SSL based VPN user access. b) The firewall appliances must include subscription for regular updates of latest threats, malware definitions and URL categorization service as well as IPS definitions for a period of at least 12 months.			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
10.9.	Firewall cluster systems warranty and support: a) The offered solution must include direct manufacturer technical support during a period of 12 months, which is available 24x7, all days of the week. b) The offered solution must include direct manufacturer access to latest software patches, updates and service packs.				
11.	**Data Centre rack cabinet for the main site**	**Quantity: 1**	**Manufacturer:** **Model:**		
11.1.	Rack capacity: 19" 42U rack cabinets, compatible with the EIA-310-E standard				
11.2.	Size of the cabinet: Maximum dimensions (W x D x H): 61 x 110 x 201 cm, compatible with the specified and offered equipment. Minimum of 80% perforated doors for cooling of the components. Static load capacity of the cabinets: 950 kg minimum.				
11.3.	Other components:				

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	Lockable side panels must be included. A minimum of two Power Distribution Units (PDUs) must be included in a zero U form factor (taking up no rack space) for connecting all hardware components to two independent power sources. The PDUs should include IEC309 32A power input cables and provide a minimum of 20 x C13 outlets each, in a vertical placement which does not use any rack units. All necessary power connectors, accessories and cables must be included for the hardware components specified in this procurement.				
12.	**Basic Software for the main and DR sites**	**Quantity: 2**	**Manufacturer:** **Model:**		
12.1.	Relational database system software licenses and Reporting server perpetual licenses, per site: a) Included perpetual licenses for an enterprise version of a relational database management system (RDBMS) system software, properly licensed for a minimum of two (2) server instances (VMs), each with a minimum of six (6) physical cores or vCPUs. b) The database software must include no limitations to the number of connected users, allocated RAM memory to a				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	database instance or compute capacity for a single database instance. c) The database software must include functionality for online creation and rebuilding of indexes, hot addition of memory and CPU, peer to peer transactional replication, star join query optimizations, distributed partitioned views and parallel indexed operations. Proposed solution must be fully compatible with Beneficiary current infrastructure. Please refer to https://mioa.gov.mk/?q=mk/node/1320 for detailed information.			
12.2.	Enterprise class server operating system perpetual licenses, per site: a) Included perpetual licenses for an enterprise version of a server class operating system, properly licensed for the included virtualisation server hardware at each site (minimum of 48 physical cores per node and a minimum of 4 nodes at the primary site and 3 nodes at the DR site). b) The server class operating system software must include no limitations to the number of additional operating server Virtual Instances (Virtual Machines) which can be run and hosted on the virtualisation server hardware. c) The server class operating system software must include support for Storage Spaces Direct Host Guardian Hyper-V Support. Proposed solution must be fully compatible with Beneficiary current			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	infrastructure. Please refer to https://mioa.gov.mk/?q=mk/node/1320 for detailed information.			
12.3.	Open-source utilities – RDBMS, network monitoring and SIEM System requirements: a) Open-source MongoDB cluster of three nodes must be installed and configured for the primary and the DR site. b) Open-source network monitoring utility must be supplied and configured for the primary and the DR site. The tool should monitor the availability of critical elements of the system, such as services (systems) and communication links. c) Open-source Security information and event management (SIEM) must be supplied and configured for the primary and the DR site. The tool should monitor the system event logs of all critical elements of the system, collect (store) the logs in a repository and perform correlation of any security related events. d) The open source SIEM solution should include its own operating system, which must be deployed as a VM in the virtualisation platform. All proposed open-source utilities should be available for commercial usage with no limitations.			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
13.	**Interoperability client software for the institution sites**	**Quantity: 11**	**Manufacturer:** **Model:**		
13.1.	Interoperability client server operating system perpetual licenses, per site: Included perpetual license for at least sixteen (16) physical cores of an enterprise class server type operating system, capable of joining the centralised MS Active Directory infrastructure as a member server. The offered operating system must include a centralised browser-based Administration Centre software, Advanced Threat Protection (ATP), Datagram Transport Layer Security (DTLS) for encryption of virtual network traffic between virtual machines and Low Extra Delay Background Transport (LEDBAT) latency optimized network congestion control The offered operating system must include the appropriate license for the requested hardware resources, as well as a hypervisor functionality for server virtualisation of at least two additional VMs, and additionally built-in support for Kubernetes. The offered operating system must include access to latest releases of hotfixes and service packs during a period of at least five years. The offered operating system must be fully compatible with the Macedonian Information Bus – MIB communication client (CC) defined in the "Guidelines on the technical requirements, manner of operation and functioning of the communication client and recommendations for use of the interoperability system" as a hardware device with an				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	adequate software which shall provide the interface for electronic documents and data exchange, whereby the documents and data are exchanged among information systems of authorities taking part in the exchange process. Proposed solution must be fully compatible with Beneficiary current infrastructure. Please refer to https://mioa.gov.mk/?q=mk/node/1320 for detailed information.			
13.2.	Included perpetual licenses for a standard version of a relational database management system (RDBMS) system software, properly licensed for a minimum of six (6) physical cores or vCPUs. The database software must include no limitations to the number of connected users, support for at least 32 GB RAM memory to a database instance. The database software must include functionality for transparent database encryption, database audit, contained databases, data classification and auditing, snapshot replication, transactional replication and partitioned table parallelism. The offered RDBMS software must be fully compatible with the Macedonian Information Bus – MIB communication client (CC) defined in the "Guidelines on the technical requirements, manner of operation and functioning of the communication client and recommendations for use of the interoperability system" as a hardware device with an adequate software which shall provide the interface for electronic documents and data exchange, whereby the documents and data are exchanged among information systems of authorities taking part in the exchange process.			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	Proposed solution must be fully compatible with Beneficiary current infrastructure. Please refer to https://mioa.gov.mk/?q=mk/node/1320 for detailed information.			
13.3.	Included perpetual licenses for a branch version of an Enterprise Service Bus (ESB) / enterprise application integration (EAI) system software, properly licensed for a minimum of six (6) physical cores or vCPUs. The ESB software must include no limitations to the number of connected users. The hub and spoke deployment scenarios ESB software must include full EAI, B2B, and Business Process Management functionality. The offered ESB software must be fully compatible with the Macedonian Information Bus – MIB communication client (CC) defined in the "Guidelines on the technical requirements, manner of operation and functioning of the communication client and recommendations for use of the interoperability system" as a hardware device with an adequate software which shall provide the interface for electronic documents and data exchange, whereby the documents and data are exchanged among information systems of authorities taking part in the exchange process. Proposed solution must be fully compatible with Beneficiary current infrastructure. Please refer to https://mioa.gov.mk/?q=mk/node/1320 for detailed information.			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
14.	**Connectivity infrastructure for the main and DR sites**	**Quantity: 4**	**Manufacturer:** **Model:**		
14.1.	Must have minimum throughput of min 1 Gbps, with Firewall, NAT and QoS services active				
14.2.	Must have ability to be included in controller-based SD-WAN solution without hardware or software upgrades (license or subscription add-on is allowed)				
14.3.	Must have a minimum of 4 x Combo 1 Gbps interfaces				
14.4.	Must have at least 3 slots for additional network interfaces modules with on-line insertion and removal capability				
14.5.	Must support following types of modules: - Voice PSTN modules – analog FXO, FXS, ISDN BRI, PRI - WAN data modules – serial, ADSL, VDSL, ISDN BRI, PRI, LTE - Ethernet switch modules - Cable modem modules - Storage – SSD drive modules - X86-based server modules				
14.6.	Must have at least 4GB DRAM with possibility to be upgraded to at least 16GB				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
14.7.	Must have at least one USB 2.0 port			
14.8.	Must have at least one serial port for management console			
14.9.	Must have stateful packet inspection Firewall system with the possibility of defining zones - Zone Based Firewall			
14.10.	Must have authentication, authorization and accounting (AAA) through a local database or through external RADIUS server			
14.11.	Must support replacement of interface modules without stopping the system			
14.12.	Must support IPSec and SSL VPN tunnels with IKE/IKEv2 session control and following protection methods: - Encryption: DES, 3DES, AES-128 и AES-256; - Authentication: RSA (748/1024/2048bit), ECDSA (256/384 bit); - Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512 - All US export restrictions and limitations on encrypted traffic removed			
14.13.	Must have included support for Generic routing encapsulation (GRE) tunnels			
14.14.	Must have included support for filtering of traffic based on ACL (lists for access control) using any combination of L3 and L4 parameters			
14.15.	Must have included support 802.1Q VLAN			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
14.16.	Must have included support for following routing protocols: IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM),			
14.17.	Must have included support for QoS and HQoS with the ability to classify traffic into traffic classes based on at least following parameters: - Classification of traffic based on ACL's with any combination of 802.1p, DSCP/DiffServ, L3/L4 parameters - Classification of traffic flows based on L7 information			
14.18.	Must have at least following methods of traffic management: - Marking and re-marking of 802.1p and DSCP tags based on defined policies - Traffic shaping on an interface level - Traffic shaping on a traffic class level - Traffic policing on an interface level - Traffic policing on a traffic class level for at least 3 levels - Weighted Fair Queue and Class Based Queueing (CBQ) or similar algorithms for queue management - Class Based Weighted Fair Queuing (CBWFQ) or similar algorithm for queue management with the ability to set a minimum guaranteed bandwidth for each queue or minimum guaranteed percentage of the interface bandwidth			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	- Management of packet queues depth - Preventing congestion by using Weighted Random Early Detection or similar algorithm - Ability to define priority queue (PQ), for traffic sensitive to delay and jitter - HQoS - Applying different QoS policies on IPSec VPN tunnels			
14.19.	Must support option to add the following functions: - Classification and filtering traffic based on Layer 7 information - IP routing based on Layer 7 information - Virtualisation of routing tables, addresses and services - L2 and L3 MPLS VPN - Automatic route selection based on following parameters of WAN links: o Jitter o Packet loss o Delay o Availability of IP connectivity to a specific host or hosts, tested with ICMP o MOS score for VoIP traffic			
14.20.	Must support option to add optimization of network traffic with minimum the following functions: a) Data deduplication or similar algorithm for optimized transmission of repetitive data b) Optimization of TCP sessions on WAN connections with high latency c) Compression of network traffic			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	d) Optimization for least the following protocols - HTTP, CIFS, Exchange MAPI, Microsoft Share Point and NFS e) Optimization for SMB printing			
14.21.	Must support option of adding an HTTP object cache with the following features as a minimum: a) Caching an HTTP objects on the additional HDD or SDD media with cache size of at least 200GB b) Caching objects of automatically generated and dynamic URLs c) Caching of objects marked as non-cashable d) Pre-loading of objects in the cache.			
14.22.	Must have at least following methods to configuration and monitoring: a) Management through console, HTTP and HTTPS b) RMON c) IPv4/v6 ping d) DNS e) TFTP f) FTP g) NTP h) SSHv2 and SNMPv3 i) Built-in DHCP server with the possibility of working in at least 20 IP subnets j) Export traffic information through IPFIX k) Configuration in separate configuration file which allows quick and easy migration of the configuration on the new device l) Built-in environment for scripting commands, automatically			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	triggered when predefined events occur m) Set the level of access control system for each user n) Authorization of users to access any command o) Working with external system to store information about entered commands by each user p) Traffic policing to control network traffic towards control plane of the router			
14.23.	Must be mounted in a standard 19 " rack, occupying no more 1RU (Rack units)			
14.24.	Must have support for input voltage from 100 to 240 V			
14.25.	Must have minimal range of operating temperature 0 - 40ºC			
14.26.	Must have a minimal range of operating humidity 5 - 85%			
14.27.	Must meet at least the following safety standards - EN 60950-1			
14.28.	Must meet at least the following standards for EMC: - EN 300-386 - EN 61000 (Immunity) - EN 55024 , CISPR 24 - EN50082-1 - EN55022 Class A			
14.29.	Warranty and service conditions: - 12-month access to the technical support centre of equipment manufacturer or its authorized service partner			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	- 12-month access to software updates for the equipment offered, through manufacturer's website or physical media - 12-month access to the latest software versions for the equipment offered, through manufacturer's website or physical media - 12-month replacement of failed equipment NOTE: The router must be supplied with included all licenses for the features mentioned in the above requirements. If some licenses are time-limited, supplier should include subscriptions for at least 5 years.				
15.	**Connectivity infrastructure for the institution sites**	**Quantity: 11**	**Manufacturer:** **Model:**		
15.1.	Must have minimum throughput of 100 Mbps with Firewall, NAT and QoS services active				
15.2.	Must have ability to increase throughput to min 300 Mbps with license only				
15.3.	Must have ability to be included in controller-based SD-WAN solution without hardware or software upgrades (license or subscription add-on is allowed)				
15.4.	Must have a minimum of 2 x Combo 1 Gbps interfaces				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
15.5.	Must have at least 1 slot for additional network interfaces modules with on-line insertion and removal capability			
15.6.	Must support following types of modules: - Voice PSTN modules – analog FXO, FXS, ISDN BRI, PRI - WAN data modules – serial, ADSL, VDSL, ISDN BRI, PRI, LTE - Ethernet switch modules - Cable modem modules - Storage – SSD drive modules - X86-based server modules			
15.7.	Must have at least 4GB DRAM with possibility to be upgraded to at least 16GB			
15.8.	Must have at least one USB 2.0 port			
15.9.	Must have at least one serial port for management console			
15.10.	Must have stateful packet inspection Firewall system with the possibility of defining zones - Zone Based Firewall			
15.11.	Must have authentication, authorization and accounting (AAA) through a local database or through external RADIUS server			
15.12.	Must support replacement of interface modules without stopping the system			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
15.13.	Must support IPSec and SSL VPN tunnels with IKE/IKEv2 session control and following protection methods: a) Encryption: DES, 3DES, AES-128 и AES-256; b) Authentication: RSA (748/1024/2048bit), ECDSA (256/384 bit); c) Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512 d) All US export restrictions and limitations on encrypted traffic removed			
15.14.	Must have included support for Generic routing encapsulation (GRE) tunnels			
15.15.	Must have included support for filtering of traffic based on ACL (lists for access control) using any combination of L3 and L4 parameters			
15.16.	Must have included support 802.1Q VLAN			
15.17.	Must have included support for following routing protocols: IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM),			
15.18.	Must have included support for QoS and HQoS with the ability to classify traffic into traffic classes based on at least following parameters: - Classification of traffic based on ACL's with any combination			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	of 802.1p, DSCP/DiffServ, L3/L4 parameters - Classification of traffic flows based on L7 information			
15.19.	Must have at least following methods of traffic management: - Marking and re-marking of 802.1p and DSCP tags based on defined policies - Traffic shaping on an interface level - Traffic shaping on a traffic class level - Traffic policing on an interface level - Traffic policing on a traffic class level for at least 3 levels - Weighted Fair Queue and Class Based Queueing (CBQ) or similar algorithms for queue management - Class Based Weighted Fair Queuing (CBWFQ) or similar algorithm for queue management with the ability to set a minimum guaranteed bandwidth for each queue or minimum guaranteed percentage of the interface bandwidth - Management of packet queues depth - Preventing congestion by using Weighted Random Early Detection or similar algorithm - Ability to define priority queue (PQ), for traffic sensitive to delay and jitter - HQoS - Applying different QoS policies on IPSec VPN tunnels			
15.20.	Must support option to add the following functions: - Classification and filtering traffic based on Layer 7 information - IP routing based on Layer 7 information			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	- Virtualisation of routing tables, addresses and services - L2 and L3 MPLS VPN - Automatic route selection based on following parameters of WAN links: o Jitter o Packet loss o Delay o Availability of IP connectivity to a specific host or hosts, tested with ICMP o MOS score for VoIP traffic			
15.21.	Must support option to add optimization of network traffic with minimum the following functions: a) Data deduplication or similar algorithm for optimized transmission of repetitive data b) Optimization of TCP sessions on WAN connections with high latency c) Compression of network traffic d) Optimization for least the following protocols - HTTP, CIFS, Exchange MAPI, MS Share Point and NFS e) Optimization for SMB printing			
15.22.	Must support option of adding an HTTP object cache with the following features as a minimum: a) Caching an HTTP objects on the additional HDD or SDD media with cache size of at least 200GB b) Caching objects of automatically generated and dynamic URLs c) Caching of objects marked as non-cashable d) Pre-loading of objects in the cache.			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
15.23.	Must have at least following methods to configuration and monitoring: a) Management through console, HTTP and HTTPS b) RMON c) IPv4/v6 ping d) DNS e) TFTP f) FTP g) NTP h) SSHv2 and SNMPv3 i) Built-in DHCP server with the possibility of working in at least 20 IP subnets j) Export traffic information through IPFIX k) Configuration in separate configuration file which allows quick and easy migration of the configuration on the new device l) Built-in environment for scripting commands, automatically triggered when predefined events occur m) Set the level of access control system for each user n) Authorization of users to access any command o) Working with external system to store information about entered commands by each user p) Traffic policing to control network traffic towards control plane of the router			
15.24.	Must be mounted in a standard 19 " rack, occupying no more 1RU (Rack units)			
15.25.	Must have support for input voltage from 100 to 240 V			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
15.26.	Must have minimal range of operating temperature 0 - 40ºC				
15.27.	Must have a minimal range of operating humidity 5 - 85%				
15.28.	Must meet at least the following safety standards - EN 60950-1				
15.29.	Must meet at least the following standards for EMC: - EN 300-386 - EN 61000 (Immunity) - EN 55024 , CISPR 24 - EN50082-1 - EN55022 Class A				
15.30.	Warranty and service conditions: - 12-month access to the technical support centre of equipment manufacturer or its authorized service partner - 12-month access to software updates for the equipment offered, through manufacturer's website or physical media - 12-month access to the latest software versions for the equipment offered, through manufacturer's website or physical media - 12-month replacement of failed equipment NOTE: The router must be supplied with included all licenses for the features mentioned in the above requirements. If some licenses are time-limited, supplier should include subscriptions for at least 5 years.				
16.	**Server infrastructure for the institution**	**Quantity: 11**	**Manufacturer:**		

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	sites	**Model:**		
16.1.	Institution sites server overview: a) 1U height rack-mount server with x64 architecture, should support 32- and 64-bit operating systems and applications, type 1 hypervisor support. b) The server must include cable management arm as well as a sliding rack mount kit for a standard 19" rack cabinet.			
16.2.	Institution sites servers' number of processors / cores: Minimum 1 physical processor, with a minimum of 8 cores and 16 threads, minimum of 32MB level 3 cache, operating at a frequency of not less than 3.1 GHz.			
16.3.	Institution sites server RAM requirements: Minimum of 64GB DDR4 RAM memory with a speed of 3200MT/s. The server must be expandable up to 2TB total memory.			
16.4.	Institution sites server's Internal storage: The servers should be offered with at least 2 x 480GB hot-swap SSD 6Gbps 2.5" drives, with a capacity of at least 3 DWPDs with hardware RAID 1 protection			
16.5.	Institution sites servers Storage Controllers: Hardware 12Gb / s PCI Express RAID Controller, with support for SATA SSDs in Pass-Thru mode, T10-DIF and 4K Native Sector. The controller should support RAID levels RAID 0, RAID 1, and RAID			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	10.			
16.6.	Institution sites servers ethernet network ports Minimum included ports per server: a) 2 x 1Gbit RJ-45 ports.			
16.7.	Institution sites servers I/O interfaces: a) Front side ports: Minimum 1 x USB 2.0 port; 1x MicroUSB port, 1 x VGA port. b) Rear side ports: Minimum 2 x USB 3.0; 1x serial port, 1 x VGA port. c) Internal ports: at least 1x USB 3.0;			
16.8.	Institution sites servers power supplies and fans: Redundant Hot-Plug Platinum power supply modules, not less 550W. The server must be designed to operate when cooling with fresh air, with temperatures up to 40 ° C and relative humidity up to 85%.			
16.9.	Institution sites server's remote management: a) Embedded system management controller with own processing power and a wireless module for wireless diagnostics over BLE / NFC. b) The controller should allow proactive for error alerts on CPUs, network adapters, memory, internal drives (SAS / SATA HDDs and SSDs), fans, power modules, RAID controllers, ambient server temperature (including graphical displays) on SSD) and other errors.			

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	c) The controller should allow quality control / bandwidth of remote access to the server. d) The controller should include independent 10/100/100 Mbit Ethernet adapter for real time remote management. The controller should provide agent-free hardware, firmware and performance monitoring, including inventory, crash screen / video capture, boot capture, and alerting. e) The controller should support the IPMI 2.0 protocol, VNC connectivity with the operating system, include HTML 5 based browser interface, SMASH-CLP, Dynamic DNS, DHCP with Zero Touch functionality, NFS v4 and WSMan support, E-mail alerts, Virtual console (KVM), Virtual media. f) The server must also include a front-facing LCD panel for local management and diagnostics. g) For management security the server must include Two-factor authentication, FIPS 140-2 support, Secure Root-of-Trust functionality, Secure Run and Secure Move for protection when running and operating the operating system and applications.			
16.10.	Institution sites server operating system: Included perpetual license for a properly licensed enterprise class server type operating system, capable of joining the centralised MS Active Directory infrastructure as a member server. The offered operating system must include a centralised browser-based Administration Centre software, Advanced Threat Protection (ATP), Datagram Transport Layer Security (DTLS) for encryption of virtual network traffic between			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	virtual machines and Low Extra Delay Background Transport (LEDBAT) latency optimized network congestion control The offered operating system must include the appropriate license for the requested hardware resources, as well as a hypervisor functionality for server virtualisation of at least two additional VMs, and additionally built-in support for Kubernetes. The offered operating system must include access to latest releases of hotfixes and service packs during a period of at least five years. Proposed solution must be fully compatible with Beneficiary current infrastructure. Please refer to https://mioa.gov.mk/?q=mk/node/1320 for detailed information.				
16.11.	Institution sites servers' warranty: The offered servers must include direct technical support during a period of 12 months, which is available 24x7, all days of the week, and which provide on-site hardware replacement.				
17.	**Delivery, assembly, installation and configuration**	**Lump sum**			
17.1.	All components of the procurement must be fully installed, assembled, integrated, configured and tested for operations, redundancy and high availability. All components must be fully upgraded to latest version of system software, connected with other MISA sites and infrastructure, tested and put into production operations at both the main and the DR site. Data				

1.	2.	3.	4.	5.
Item Number	**Specifications Required**	**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	replication must be configured between the sites. The backup solution must be integrated with the production Virtual Machines, databases and file systems to include application aware regular backups. The solution must include a fully redundant Enterprise class Relational Database cluster of at least two active nodes, with Always On availability groups, at each site. The system must be configured for database automatic read write connection re-routing. The solution must include a fully redundant MongoDB Community version cluster of at least three active nodes, at each site. The MongoDB and the Enterprise class RDBMS data must be replicated between the sites, using replica sets or similar solutions. The solution must include an open source SIEM solution, installed at both the main and the DR sites. The system must monitor the following objects: - all production VMs which are part of the system - the firewall devices at each site - the routers at each site - the physical hardware of the virtualisation nodes at each site. All institution sites must be connected with the main and DR sites. All servers, operating systems and system software for the institution sites must be installed in each location and connected with the main and DR sites.			

1.	2.		3.	4.	5.
Item Number	**Specifications Required**		**Specifications Offered**	**Notes, remarks, ref to documentation**	**Evaluation Committee's notes**
	All installation activities must be fully documented before systems are put in production operations. Proposed solution must be fully compatible with Beneficiary current infrastructure. Please refer to https://mioa.gov.mk/?q=mk/node/1320 for detailed information.				
18	**Training**	**Lump sum**			
18.1	The Tenderer shall present and include a proposal for training. This shall describe the organisation and delivery of training as appropriate regarding the structure, configuration and functionality of the installed equipment as well as the day-to-day use of the system supplied. The training shall be delivered by practically experienced trainer(s). The Tenderer must present the details of their proposal in respect of this requirement.				
18.2	The training must be organised as appropriate for all institutions supplied with equipment and must be conducted in Macedonian.				

Annex 1 –equipment delivery locations

No.	Item(s)\Institution	MISA MDC	MISA DRDC	CA	EWSRC	FVA	IA	MTC	ME-E	MEPP	MH	MI	MJ	PDIF	PCM	UVMK	MAWVE	ESA	EA	MLSP	Quantity
1.	Compute virtualisation platforms	X	X																		1
2.	Central file and block-based storage system for the virtualisation platform	1	1																		2
3.	Central block-based storage system for the data platforms	1	1																		2
4.	SAN networking solution for the virtualisation platform	2	2																		4
5.	External networking solution for the virtualisation platform	2	2																		4
6.	Centralised backup solution	1	1																		1

7.	Management server	1	1																	2
8	Web and application traffic load balancing and protection solution	1	1																	2
9	Remote access Management Network switch	2	2																	4
10	Redundant Next-Generation Firewall cluster system	1	1																	2
11	Data centre rack cabinet	1																		1
12	Basic Software for the main and DR sites	1	1																	2
13	Interoperability client software for the institution sites				1	1	1		1	1	1		1		1		1		1	1	11
14	Connectivity infrastructure for the main and DR sites	2	2																	4

15	Connectivity infrastructure for the institution sites				1	1	1		1	1	1		1		1		1		1	1	11
16	Server infrastructure for the institution sites				1	1	1		1	1	1		1		1		1		1	1	11

The equipment for all the institutions is to be delivered in Skopje, as they are all located in Skopje. The only exception is the MISA Disaster Recovery Data Centre (MISA DRDC), for which the equipment should be delivered in Prilep.

List of abbreviations:

MISA Ministry of Information Society and Administration

MDC Main Data Centre

MISA DRDC MISA Disaster Recovery Data Centre

CA Cadastre Agency

EWSRC Energy and Water Services Regulatory Commission

FVA Food and Veterinary Agency

IA Institute for Accreditation

MTC Ministry of Transport and Communications

ME-E Ministry of Economy

MEPP Ministry of Environment and Physical Planning

MH Ministry of Health

MI	Ministry of Interior
MJ	Ministry of Justice
PDIF	Pension and Disability Insurance Fund
PCM	Pharmaceutical Chamber of Macedonia
UVMK	Office for management of registers of births, marriages, and deaths
MAWVE	Ministry of Agriculture, Forestry and Water Management
ESA	Employment Service Agency
EA	Energy Agency
MLSP	Ministry of Labour and Social Policy