REVISED SECTION 5: SCHEDULE OF REQUIREMENTS

A. SUMMARY OF REQUIREMENTS

The objective of these services is to enhance the Ministry of Justice's (MoJ) cybersecurity resilience and ICT management capabilities by means delivering, installing, and configuring the necessary hardware, software, and infrastructure components.

The document outlines the procurement, delivery, installation and configuration of specified computer hardware, IT, and office software as detailed in the tender documents.

B. BACKGROUND

The UNDP "Strengthening the capacities of the Ministry of Justice of Moldova to deliver on the justice reform mandate" (SMJ) Project is a short-term project designed to strengthen the institutional and operational capacities of the institution to deliver on its mandate and advance the justice sector reform in line with the best practices and relevant standards of performance. Acknowledging the critical role of the Ministry of Justice in organizing and coordinating the justice sector policy, the Project will strengthen the institutional and operational capacities of the institution to deliver on its mandate and advance the justice sector reform in line with the best practices and relevant standards of performance.

The Ministry of Justice (MoJ) is the key national stakeholder in the justice sector, exercising a large spectrum of functions from policy making and oversight, legal drafting, and review to regulating legal professions, facilitating access to justice, management of corrections, and developing and administering informational systems in the justice sector. Digitalization is one of the key enablers to support the modernization of the public sector, in general, and justice sector, in particular. The Government has made substantial efforts to deploy e-services in areas commonly demanded by citizens, such as identity-related documents, property, and taxes. Further digitalization of services related to judiciary procedures are amongst the 'most desirable e-services'2 in Moldova.

Digital transformation is essential for the justice sector to stay relevant, effective, and responsive in its approach to serving the public. It has the potential to touch every part of the justice process, changing the way justice institutions work, harness data, exploit available technologies, collaborate with partner organizations, and organize themselves. This approach is recognized by the new justice sector strategy paying due attention to the development and implementation of justice digital solutions. At the same time, the ever-increasing volume of information made available both to the general public and to litigants by the justice system through electronic means requires the implementation of a wide range of measures to strengthen cybersecurity. "Cybersecurity failure" is believed to become a critical short- and medium-term threat to the world.3

The MoJ is in charge of developing and managing a diverse digital ecosystem in the justice sector, harnessing the potential of information technologies to advance structural changes in this field. At the same time, critical and, at some point, confidential information used by the MoJ staff in exercising their duties, raise the exposure of these operations and data to potential risks of breaches and loss. Outdated systems and technologies, in use at the MoJ headquarter, amplify these risks. Lack of digital safety could impact the public trust in digital transformation efforts in the justice sector, led by the MoJ.

Relying on outdated systems and technologies amplifies this risk. Thus, investment in cybersecurity infrastructure is a must for the MoJ (as well as for any other public or private entity) to make the organization more resilient to eventual cyberattacks.

The upgrade of cybersecurity capabilities can help the Ministry exercise its mandate in promoting the justice sector reform by managing critical operations and data through a secured IT infrastructure, as well as increase the transparency, integrity, and efficiency of the organization. Considering the various difficulties the MoJ faces in strengthening its cyber resilience (including limited understanding of cyber vulnerabilities the institution is dealing with, insufficient and outdated hardware to underpin a solid response to a cyber threat, limited cybersecurity skills), targeted assistance will be provided to support the Ministry of Justice in strengthening institution's digital health and putting in place cybersecurity solutions and tools to safeguard critical data flows and operations.

In this regard, UNDP is seeking to contract a specialised company, further on referred to as the Service Provider, to delivery, installation and configuration of specified hardware & related components, IT, and office software as detailed in the tender documentation.

C. OBJECTIVES OF THE ASIGNMENT

The main objective is to provide MoJ with a fully operational, integrated, and documented solution that is ready for use.

As part of this assignment, the Service Provider will deliver, install, and configure the following items, the amount and technical specifications thereof being described in **section H. TECHNICAL SPECIFICATIONS FOR GOODS:**

- Enterprise Servers for virtualization
- All-Flash storage system for virtualization
- Core and aggregation switches
- Next-Generation Firewall
- Rack-mountable Uninterruptible Power Source (UPS)
- 42U Rack

All the tasks within the scope of this assignment will be carried out in close cooperation and coordination with the MoJ, ARIJ and UNDP through the Service Provider contracted to conduct the cyber security audit to assess the MoJ security program, whereas Service Provider's performance will be evaluated against such criteria as: timeliness, responsibility, initiative, communication, accuracy, and quality of the services delivered, monitored and confirmed by means of post tasks completion reports signed by UNDP and MoJ.

In order to achieve the stated objectives, the Service Provider will have the following responsibilities:

- Organise, coordinate with stakeholders and timely provide basic installation services as described at **1. Basic installation services**;
- Organise, coordinate with stakeholders and timely provide training services as described at **2. Training**;
- Organise, coordinate with stakeholders and timely provide data migration services as described at **3. Data migration services;**
- Organise, coordinate with stakeholders and timely provide services related to implementation and deployment as described at **4. Specific services implementation and deployment;**
- Organise, coordinate with stakeholders and timely provide cyber security services as described at **5. Security services implementation and deployment;**
- Organise, coordinate with stakeholders and timely provide redundant interconnection of existing network devices with new equipment in the data centre as described at **6. Organization of Vertical Optical Connections and redundant interconnexion of existing network devices with the equipment in the new data room;**
- Provide proper documentation of all necessary/required aspects and guides/instructions or methodological documents, to ensure knowledge transfer and all necessary guidelines for ARIJ, as specified at **7. Documentation requirements.**

1. Basic installation services

The Service Provider shall assemble, install, and integrate with other components the infrastructure system in the server room specified by the MoJ.

The assembly will include, but is not limited to:

- **Provision of Components.** In this regard, the Service Provider, shall also ensure that all required and ordered components necessary for compliant completion of the tasks are provided, ready for use, and in accordance with specifications and target descriptions.
- **Installation and configuration of the equipment in rack.** In this regard, the Service Provider shall ensure that all spare materials, cables, accessories, and other material necessary for compliant completion of the tasks related to the items described in **section H. TECHNICAL SPECIFICATIONS FOR GOODS**. The Service

Provider shall also to ensure that the works in the scope of the services are carried out in accordance with manufacturer recommendations and applicable technical standards.

- **Cabling and interconnection of all devices.** In this regard, the Service Provider shall ensure all necessary interconnecting activities in rack and to/from the rack, including cabling and cable management accessories.
- **Testing and Approval.** The newly built infrastructure system will be tested, consolidated, and approved for productive operation.

2. Training

Training[1] is an integral part of the current assignment so as to ensure knowledge and relevant skills transfer to the designated personnel of MoJ and ARIJ, as well as alignment with the provided hardware and software solutions. The introduction of new hardware and software requires pre-operational training planning.

For the scope of the assignment, throughout delivery of all services listed in the present INVITATION TO BID in **section H. TECHNICAL SPECIFICATIONS FOR GOODS**, appropriate training so as to ensure that technical staff of MoJ and ARIJ have sufficient knowledge to manage the provided solutions. The overall objective of the trainings is to ensure that the technical personnel of MoJ and ARIJ are actively involved in the implementation process, have the knowledge and skills to facilitate a smooth transition to new technology and subsequent use thereof.

Specific technical training will be coordinated MoJ, ARIJ and UNDP through the Service Provider contracted to conduct the cyber security audit to assess the MoJ security program, in terms of learning needs.

The trainings will be conducted for designated personnel of MoJ and ARIJ to ensure proper administration, maintenance, and operation of the provided software and hardware described in **section H. TECHNICAL SPECIFICATIONS FOR GOODS.**

Each training session will last at least 2 hours per topic.

Training will cover at least the following topics:

Subject matter	**Completion criteria**
Active Directory administration and configuration, including OUs, Groups, and Group Policies.	Training on the job Specific trainings provided, according to Beneficiary's learning needs Short instruction and necessary methodological support and training to ARIJ experts provided, necessary to handle proper AD integration of Windows systems (Integration of user PCs (~140 workstations with Windows 11 Pro x64 and one server used to host accounting system[2]) with AD and application of security and access policies).
Windows services configuration such as file server, print server, and DHCP.	Training on the job Specific trainings provided, according to Beneficiary's learning needs
Hardware management, maintenance, and service (servers, storage, NGFW, UPS, switches), including safety and environmental requirements,	Training on the job Specific trainings provided, according to Beneficiary's learning needs

[1] For the scope of services listed at" 2. Training", trainings shall foresee advice, explanations and methodological support.

[2] Soft Contabil - accounting system developed in Visual Foxpro, running on Windows Server 2022. It supports 4-6 users who access the system via the local network through Remote Desktop Protocol (RDP), using usernames and passwords.

Subject matter	Completion criteria
updates, patching, and configuration management.	
Virtualization environment configuration and management/administration.	Training on the job Specific trainings provided, according to Beneficiary's learning needs
SIEM management, reporting, integration of new sources, alerts, etc.	Training on the job Specific trainings provided, according to Beneficiary's learning needs
Web-Proxy management and configuration.	Training on the job Specific trainings provided, according to Beneficiary's learning needs
NGFW management, including URL filtering and rules management.	Training on the job Specific trainings provided, according to Beneficiary's learning needs
Networking: VLANs, ACLs, principles, etc.	Network security principles trainings provided Training on the job Specific trainings provided, according to Beneficiary's learning needs

The premises for the training will be provided by the MoJ following prior coordination and endorsement of the timing of the trainings. The training will be provided in Romanian in person.

3. Data migration services

Specific service requirements are to support MoJ and ARIJ in migration of specific files and folders from current servers. Objective of this task is to propose the migration concept and provide support to ARIJ personnel in file migration, including revision of access rules.

4. Specific services implementation and deployment

The Service Provider shall ensure the implementation and configuration of specific servers, services, and systems provided within the assignment.

The following specific services and associated documentation where relevant, are to be provided:

Activity	Completion criteria
Installation, configuration, and deployment of hight available virtualization environment based on Microsoft Hyper-V (newest build).	• Creation of a virtualisation cluster on provided servers and storage (2 physical Servers) • Creation and configuration of virtual switches required by HLD • Performance optimisation and external networking
Creation of Windows virtual server template, with basic configurations and	• One Windows 2022 server template, configured with basic parameters (updates, patches, account management, etc.) and ready for deployment.

Activity	Completion criteria
parameters adapted for the local environment.	
Installation, configuration, and deployment of Active Directory Services.	• Creation of User Groups and Organizational Units according to MJ organizational chart. • Creation of primary Group Policies in collaboration with external experts and ARIJ. • Setting the migration strategy and data migration from current AD server (users, rights, etc.), if required and applicable.
Configuration of rules and policies for file sharing and printing for all type of users.	• One Windows 2022 server configured as file server integrated in AD, with AD based users access (users groups). • One Windows 2022 server configured as print users services, integrated in AD, with AD based users access (users groups). • ~~One Windows 2022 server configured as File Server services, integrated in AD, with AD based users access (users groups).~~
Integration of all required components wit AD.	Up to 10 services integrated, including: • File server, • Print server, • Authentication server (NPS) • DNS/NTP Services • WSUS
Basic configuration and configuration of security rules for internet access on the provided NGFW.	• Access to and from the outside network is delimited for all users of the MJ network. • Access is provided according to specific needs and based on AD groups. • Creation of access groups and rules for internet resources (ex: general access list, governmental, news, social media, restricted, prohibited). • Other rules and required configurations.
Configuration of remote access service on provided NGFW	• Access to corporate network via secured connection from windows and non-windows devices • Access is provided according to specific needs and based on AD groups and AD authentication. • Access logs are transmitted to SIEM.
Implementation of Graylog SIEM:	• A virtual server with Debian 12 is provisioned and configured as a template. • Graylog log management system is installed and configured. • Key nodes are connected to Graylog (syslogs level for all installed servers, AD logs, NGFW and all network equipment).
Implementation and deployment of WSUS server:	Based on Windows 2022 server template, created the WSUS server.

Activity	Completion criteria
	• Integrated with existing Windows Servers, PCs, and MS Office products. • Basic rules for different types of updates configured and deployed. • Rollback process is documented and explained to ARIJ experts. • Test groups of PC and Servers are used for preliminary testing of new updates. • Integrated with SIEM and specific alerts configured.

Service Provider will ensure application of all updates, service packs and patches for provided components, include firmware updates for equipment and its components.

5. Security services implementation and deployment

The Service Provider shall provide specific services related to the cybersecurity of the MoJ.

These services should include:

Activity	Completion criteria
Propose concept and create VLANs	• Proposed and created relevant to MJ VLans, according to the concept (at least Management, OOB, Users, DMZ, Servers, DB, Guest, etc.) • Basic ACLs between VLANs (according to the concept) configured, tested and deployed.
AD authentication (Radius/NPS) for network equipment and non-windows servers	• AD authentication (Radius/NPS) for network equipment (provided within this assignment) configured • AD authentication (Radius/NPS) tested • AD authentication (Radius/NPS) deployed
Secure configuration (hardening) for network equipment (Switches and NGFW)	• Switches and NGFW configured according to CIS Benchmarks for specific equipment (minimum for the following areas: Identity, backups, updates, hardening Network Protocol Settings) • Switches and NGFW tested • Switches and NGFW deployed
Security configuration parameters and their implementations for Windows Servers	• Windows Server Security configuration rules (based on CIS and/or Microsoft security guides) proposed • Security rules tested and verified • Security rules deployed into production for domain controller, print server, file server, WSUS and AD service
Security configuration of Linux-based (Debian) template of virtual server	• Debian secure configuration rules (based on CIS) proposed • Security rules tested and verified • Security rules deployed into production for Graylog system
Support in the implementation of backup processes for network equipment	• Backup process configured, based on freeware and/or open-source solutions • OS/Configurations backup process tested and verified • OS/Configurations backup process deployed into production

All documentation necessary to ensure compliance with the Completion criteria will be submitted for clearance to MoJ, ARIJ and UNDP through the Service Provider contracted to conduct the cyber security audit to assess the MoJ security program.

6. Organization of Vertical Optical Connections and redundant interconnexion of existing network devices with the equipment in the new data room

The project involves organizing new LAN architecture based on new Core switches, FC vertical cabling and reusing of all old access and core switches.

All network connections are aggregated on each floor, in specialised technical cabinets with patch panels and active equipment. In the following table is presented list of reordering network access equipment:

Actual placement	Actual role	Model	New placement	New function
Floor 0 Server room	Core Switch	Juniper ex4200-48t	Floor 2 tech. cabinet	Floor switch extension
Floor 0 Server room	Core Switch	Juniper ex4200-48t	Floor 4 tech. cabinet	Floor switch extension
Floor 2 tech. cabinet	Access Switch	Juniper ex2200-24t-4g	Floor 0 Server room	Old Servers access switch
Floor 4 tech. cabinet	Access Switch	Juniper ex2200-24t-4g	Floor 0 tech. cabinet	Uses access switch

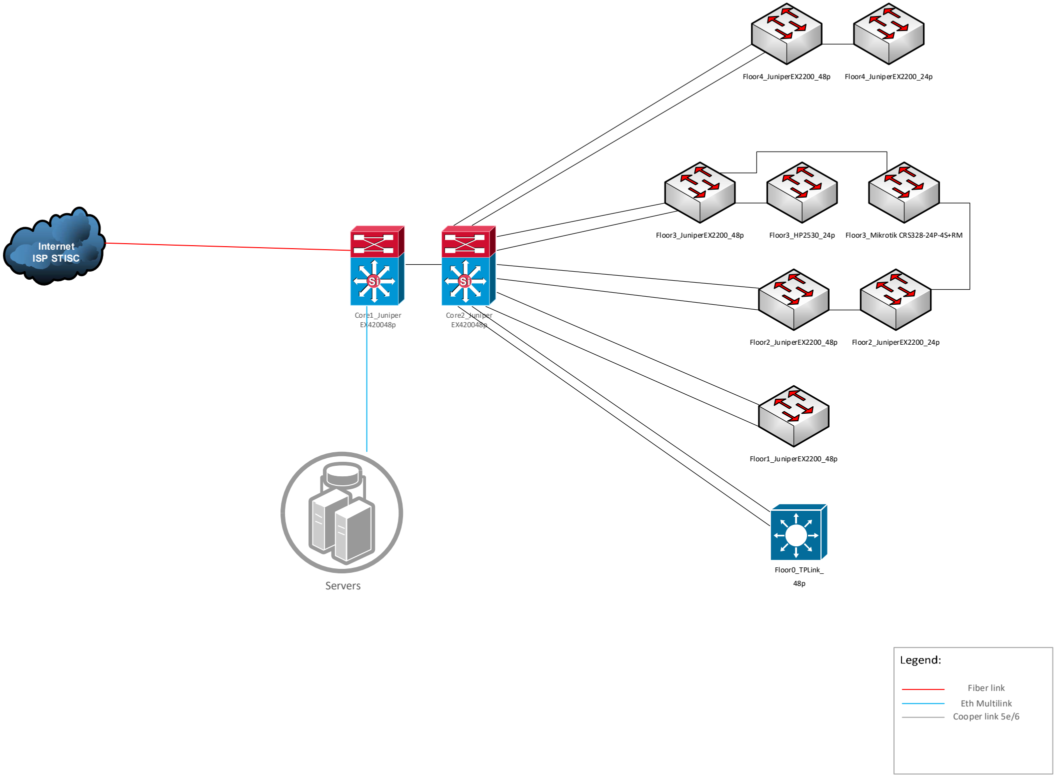
The project involves OS upgrade to last OS version for all MoJ access switches.

All actual network connections are aggregated on each floor, in specialised technical cabinets with patch panels and active equipment. In the following table is presented list of network equipment:

Function	Model	Quant.	Installed OS ver.
Core/Agregation	Juniper ex4200-48t	2	11.475
Access/Agregation	Juniper ex2200-48t-4g	4	12.3R4.6
Access/Agregation	Juniper ex2200-24t-4g	2	11.4R7.5
Access/Agregation	HP J9782A 2530-24	1	YB.15.12.0015
Access/Agregation	TPLink TLSG1024	1	-
Access/Agregation	Mikrotik CRS328-24P-4S+RM	1	-

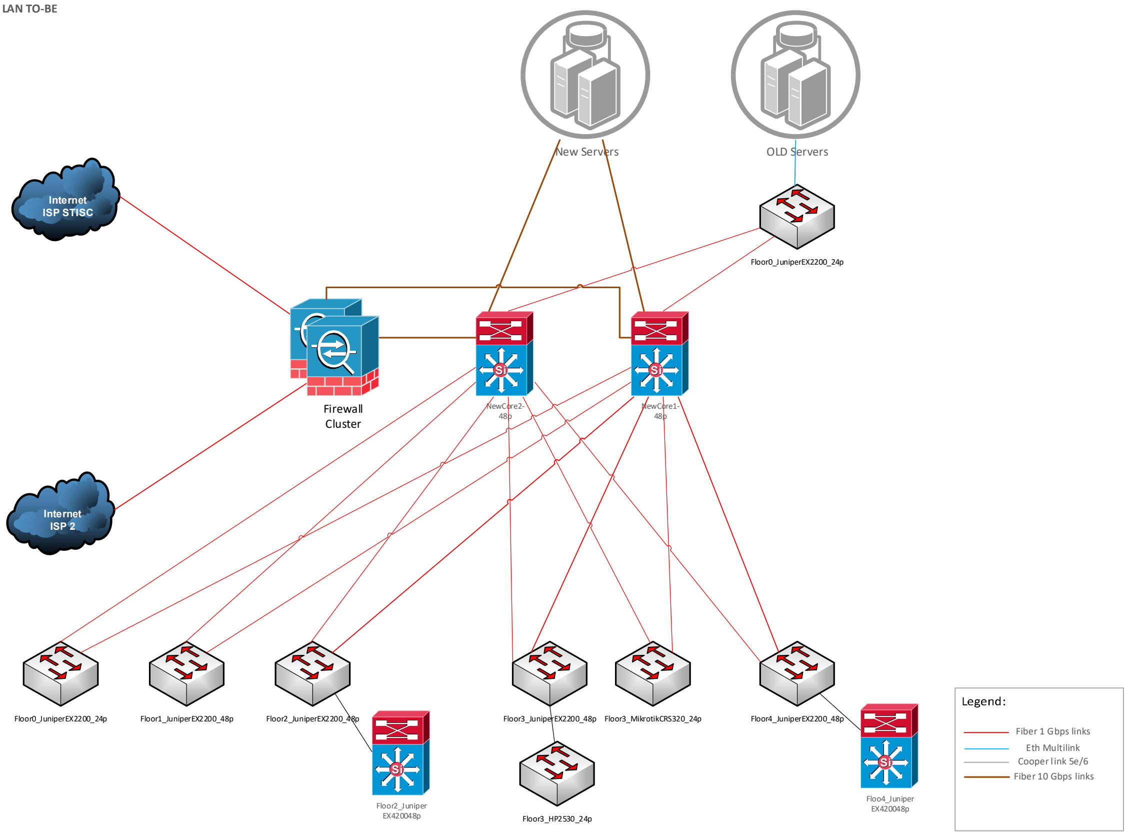
In the following scheme is presented current physical scheme of MoJ network.

Figura 1. MJ LAN ASIS



In the following scheme is presented to-be physical architecture o MoJ network.

Figura 2. MJ LAN TO-BE



At the finish of all services activities, Service provider will made testing activities to demonstrate proper working and compliance of provided solutions/services with requirements.

7. Documentation requirements

All requested technical documentation must be provided in Romanian language. For the whole project there must be system documentation (HLD):

- Graphical view and description for High availability virtualization environment
- Graphical view for the rack layout
- Cabling plan & structure
- IP-Address lists
- List and description of AD security and access policies
- AD architecture and topology
- AD organizational units and user's groups, with description

Other relevant documents to be developed and provided:

- List and description of NGFW security and access policies
- List of hardware components with product number, serial number, description
- List of software components with description, manufacturer, serial number, order number, license-key (where is applicable)
- List of accounts and passwords for each component (software and hardware)
- List for support calls: service contacts, telephone, web-address, how-to
- Instructions for (to handle):
    - Crash of a server (physical, virtual)
    - Crash of a hard disk (server, storage system)
    - Expansion of the storage array
    - Crash of a Core-Switch
    - Procedure for complete shutdown and start-up.

All documentation necessary to ensure compliance with the Completion criteria will be submitted for clearance to MoJ, ARIJ and UNDP through the Service Provider contracted to conduct the cyber security audit to assess the MoJ security program.

D. ACCEPTANCE PROCESS

At the final stage of goods and service delivery, Service Provider will perform comprehensive testing/validation process to ensure proper and correct functioning of all/any of the components, security configurations, as well as delivery of required documents.

Results should be included in acceptance documents, which are to be signed by MJ, ARIJ and UNDP Project. Acceptance documents will consist of list of tested validated items/activities, description of testing process and results of evaluation.

E. INSTITUTIONAL ARRANGEMENTS

The company will work in close collaboration with UNDP SMJ team and Service Provider contracted to conduct the cyber security audit to assess the MoJ security program for the substantive aspects of the assignment, and the UNDP Component Manager – with regards to administrative aspects.

All the deliverables should be cleared by UNDP. The above-listed deliverables will be finalised based on inputs from UNDP SMJ Project Team and will be adjusted to the needs of the end beneficiary.

All hardware related documentation must be provided in Romanian.

The latest available versions and patch levels for all system components must be installed at the time of implementation.

F. QUALIFICATIONS AND EXPERIENCE REQUIREMENTS

The bidder should demonstrate capacity to implement this project at highest quality level. It is required to demonstrate organisational capacity and expertise in accordance with required activities/services.

In particular for services described in the section C. OBJECTIVES OF THE ASIGNMENT of this Schedule of Requirements, it is required to prove availability of key personnel with the required academic and professional qualifications, proven by CVs and valid certificates, consisting of at least the following experts:

1. Project Manager
2. Infrastructure expert
3. Network expert
4. Security expert
5. Other experts (in accordance with proposed solutions/technologies and equipment, e.g. AD, SIEM, etc.)

Every of proposed expert must sign Statement of Availability for entire project period. All experts must have an advanced level of Romanian language.

Bidders agree that proposed experts will provide high quality services and expertise and participate in the project at the level and duration specified. Should any changes be necessary in this regard, a formal request for the agreement of UNDP Project team to allow substitutions, shall be submitted.

CVs of proposed team must be included in the offer. Submitted CVs should be detailed and comprehensive and prove that the experts fit to provide assigned activities and tasks. Specifically, CVs should include:

- *Anticipated role and level of participation in the project;*
- *Previous experience relevant to the assigned role in the project;*
- *Education, training and certification details, depending on the area to be involved and related technologies;*
- *Linguistic skills.*

Descriptions of subcontractor staff members, if applicable, should follow the format utilized for the Bidder organization.

Bidder must demonstrate expertise and organisational expertise to execute all necessary activities and works at higher level of quality an in agreed timelines. For the project purposes is required at least following experts, with indicated minimal qualifications.

Project Manager

- Master degree (or 5 (five) years university degree) in the field of Computer Science and/or Information Technologies
- At least 7 (seven) years of professional experience in the field, as PM or Team Leader or other leading position for projects in ICT field
- Proven experience in similar projects, with similar complexity as a Project Manager
- Proven previous experience with international organizations (UNDP, WB, GIZ, EBRD, others)
- Proven previous experience as PM, Team Leader or other leading position for projects for public authorities;
- Fluency in Romanian.

Infrastructure expert

- University degree in the field of Computer Science and/or Information Technologies or related areas
- At least 5 years of progressive experience in ICT sector
- At least 5 years of work experience as managing/leading expert for complex ICT and infrastructure solution audit and/or implementation projects
- Proven experience as infrastructure expert
- Fluency in Romanian or Russian.

Network expert

- University degree in the field of Computer Science and/or Information Technologies, engineering, telecommunications or related areas
- At least 5 years of progressive experience in ICT sector as Network expert
- Certificates in relevant areas (like CCNA, CTNS, CCIE, CCMA)
- Proven experience within the public sector
- Fluency in Romanian or Russian.

Security expert

- University degree in the field of Computer Science and/or Information Technologies, engineering, telecommunications or related areas
- At least 5 years of experience in information technology on positions involving cyber security projects and/or information security management, implementation and/or assessment
- Proven experience in implementation and/or provision consultancy/advisory services related to assessment of ICT and cyber security processes and tools
- Proven experience within the public sector
- Relevant certifications (ex: MS Cyber Architect expert, CISSP, CCSP, CISM, or similar)
- Fluency in Romanian or Russian is a must.

Other experts (in accordance with proposed solutions/technologies and equipment, e.g. AD, SIEM, etc.)

All other team members should be relevant to required activities and technologies provided.

G. TIMEFRAME AND LOCATION

The expected period of implementation of the assignment is during November 2024 – February 2025. The services will be carried out in Republic of Moldova.

All packaging materials must be removed from the client's premises immediately and disposed of in an environmentally friendly manner.

H. SPECIFICATIONS FOR GOODS

Item no	Requirements	Minimum technical requirements	Unit	Quantity
1	**ENTERPRISE SERVERS FOR VIRTUALIZATION**			
	Type	Rackmount, max. 2U Enterprise Server, with rail-kit included.	Pcs	2
	Form factor	Rack mount-Kit for Industry standard 19" RETMA standard, EIA-310D Type A cabinet per section 4.1.1, cable management arm		
	CPU Included	2 x CPU; min 16 core per CPU with hyper-threading; min. 2Ghz, min. Cache 30 MB gen 5.		
	Sockets	2		
	Memory installed	min. 512GB DDR5 (16x32GB or 8x64 GB). min. 16 total RAM slots available.		
	Storage bays	min. 8 bays 2.5, Hot-Swappable.		
	Storage bays for OS installed	2 x min. 240Gb SSD SAS, hot-swappable, configurable in RAID1		
	Network cards included	dedicated 1GE for management; min 2 x 1GE; min. 2 x 10GbE SFP+, with SFP modules included.		

	OS Supported	VMware (VMware ESXi);
		Microsoft Windows Server;
		RHEL;
		Microsoft Hyper-V.		

	OS Included	2 x Microsoft Windows Server St. Ed. 16 Core License		
	Interfaces	min. 2 x USB port		
	Power supplies included	2 x hot-plug PSU with support for 1+1 redundancy, power cords c13-c14.		
	Power Input Requirements	100 to 240 VAC		
	Rated Input Frequency	50 to 60 Hz		
	Industry Standard Compliance	Min. ACPI 5.0		
	Fan Modules	hot-swappable with N+1 redundancy		

	Network cables	2 x Cisco Compatible 10G SFP+ DAC Twinax Cable (2-meter)		
	Management included	KVM with full functionality for manage and monitoring, at least view information about the state, inventory of the managed server; energy consumption, remote on/off server, remote FW update (BIOS, network, RAID), virtual console and media for remote OS install.		
	Warranty	min. 3y/3y/3y years hardware warranty (parts/labour/onsite), Next business day[3], and min 3 years software support from vendor, access to support and customer portal		
	Service requirement	Minimum one authorised service available in Chisinau for this type of products.		
2	**ALL FLASH STORAGE SYSTEM FOR VIRTUALIZATION**			
	Storage type	Dual controller, redundant, with automatic failover, rackmount with kit included	**Pcs**	**1**
	Purpose	The storage system will be utilized for infrastructure virtualization		
	RAID Type supported	10, 5, 6 or similar by performance and redundancy		
	System Cache protection	Cache saving mechanism on flash or disk drives in case of power loss		
	Storage space	Min. 30TB SSD of usable space, configured in RAID6 or another RAID type, ensuring continuous access to data in the event of a simultaneous failure of 2 disks. Disk type volume used for achieving usable space – max. 3.8TB SAS SSD. System must include spare drives for fast rebuild		
	Host ports	min. 8 x CNA ports, supporting 10Gb ethernet and 16Gb FC, with 8x included SFP+ 10Gb ethernet		
	Storage protocols included	FCP, iSCSI, NFS, CIFS, SMB		
	Efficiency and Features included	Snapshots, storage QoS, Deduplication, Compression, thin provisioning, volume migration. Licenses must cover all storage space supported by system, without restrictions on protocol used or other limitations		
	Redundancy with hot swap	Power supply and fans, controllers, disks, ports		
	OS support	Windows Server 2019-2022 Edition (21H2), Linux, Citrix XEN Server, VMware ESXi		
	Updates and upgrade	all update and patching processes (FW, controllers, disks or other) and system extension (adding or removing disk shelves) must not affect access to data or production environment.		
	Network cables	4 x Cisco Compatible 10G SFP+ DAC Twinax Cable (2-meter)		
	Management	Dedicated port for management, easy software for storage administration hosted on controllers, secured Web based GUI and CLI. Integration with 3rd party management and monitoring solutions using SMI-S, SNMP		

[3] A vendor authorized representative will arrive at the customer's site during the coverage window to begin hardware maintenance service the next business day after the call has been received and acknowledged by vendor.

	Monitoring	Dedicated software for storage system monitoring and events, at least performance IOPS, latency, throughput for controllers, data volumes, ports, disks. Performance data must be stored at least for 12 months, allowing to corelate events or analyse performance and events.		
	Warranty	min. 3y/3y/3y years hardware warranty (parts/labour/onsite), Next business day, and min 3 years software support from vendor, access to support and customer portal		
	Service requirement	Authorised service available in Chisinau for this type of products.		
3	**CORE AND AGGREGATION SWITCH**			
	Form factor	19", 1U metal rack mount network equipment chassis, with rack mounting kit included	**Pcs**	**2**
	Network Ports	min. 48x 1/10 Gigabit SFP+ ports		
	Power Supplies and fans	2x hot-swappable power supplies, redundant hot-swappable fans		
	Stacking	Switch stacking protocol or technology redundancy must be offered		
	Performance Indicators	min. 900Gbps switching capacity and min. forwarding rate 700 Mpps; min. 4000 VLANs; min. Jumbo Frame size 9000; min. 60k MAC addresses		
	Management ports	min. 1x USB; 1x serial console port, 1x 1Gbps RJ-45		
	Functional Requirements	IEEE 802.1Q VLAN; LACP; IEEE 802.3ad; Radius; TACACS+; Secure Shell; OSPFv2; FHRP; BGP; VRF; Multiple Spanning Tree Protocol (MSTP); Rapid Spanning Tree Protocol (RSTP); Virtual Interface; ACL, BPDU Guard; Remote Switch Port Analyzer (RSPAN); Uni-Directional Link Detection (UDLD - like)		
	Network cables	2 x Cisco Compatible 10G SFP+ DAC Twinax Cable (2-meter)		
	Network connectors	30 x SFP 1/10 Gbps Optic Module Juniper&Cisco Compatible for LAN aggregation connections (2 m FC LC/LC cables included)		
	Management	CLI; SNMP v2c and v3		
	Warranty	min. 3y/3y/3y years hardware warranty (parts/labour/onsite), Next business day, and min 3 years software support from vendor, access to support and customer portal		
	Service requirement	Authorised service available in Chisinau for this type of products.		
4	**NEXT GENERATION FIREWALL**			
	Form factor	19", max. 1U metal rack mount network equipment chassis, with rack mounting kit included		
	Network Ports	min. 8x 1GbE Base-T; min. 8x10GbE SFP+ ports, extension ports for future upgrade min. 8x10GbE SFP+.		
	Performance	- min. 10GbE IPS throughput - min. 1.4 M concurrent sessions - min. 85k new connections per second - min. 3Gbps TLS decryption - min. 5.4 Gbps IPSec VPN		

	Security features included	application control;
		URL filtering;
		malware protection; per user security policy.
			Pcs	**2**

	Routing protocols	BGPv4; OSPFv2		
	High availability	Active-Active, Active-Passive, Clustering		
	Management and monitoring	Centralized management that includes at least security configuration rules and policy, events logging, advanced monitoring, reporting tool		
	Hardware redundancy	2x hot-swappable power supplies, redundant hot-swappable fans		
	Network cables	2 x Cisco Compatible 10G SFP+ DAC Twinax Cable (2-meter)		
	Warranty	min. 3y/3y/3y years hardware warranty (parts/labour/onsite), Next business day, and min 3 years of vendor official hardware and software support, including features subscription		
	Service requirement	Authorised service available in Chisinau for this type of products.		
5	**RACK-MOUNTABLE UNINTERRUPTIBLE POWER SOURCE (UPS)**			
	Form factor	19-inch rackmount UPS with integrated battery pack	**Pcs**	**1**
	Topology and power	On-line double conversion with PFC with rated Power of min. 5kVA.		
	Management ports	USB, supports Network Management Module, LCD display with button interface for status and diagnostics		
	Input Specifications	Three-phase input with voltage range from 305V to 480V.		
	Nominal Voltage	380/400/415V Auto-selection for 50/60 Hz frequency with a frequency range of 40-70 Hz, with frequency converter as standard.		
	Short Circuit Current	120 A		
	Output Specifications	Single-phase output with voltages of min. 208/220/230/240/250V (+/- 1%).		
	Efficiency	Up to 98%		
	Typical recharge time	Not more than 1,5h		
	Expected Battery Life (years)	Min 3 years		
	Output Connections	- Using PDU (must be included, rack mount) - Minimum 24 x C-13 outlets		
	Battery Specifications and extended runtime	Maintenance-free, rechargeable, valve-regulated lead-acid batteries; support of a minimum of 2 extended runtime modules per UPS.		
	Environmental and Safety	Operating Temperature: 10° to 40° C Humidity (Operation): 20% to 80% (non-condensing)		
	Warranty	min. 3y/3y/3y hardware warranty, Next business day (parts/labour/onsite) (2 years for battery)		
	Service requirement	Minimum one authorised service available in Chisinau for this type of products.		

6	**42U UNIVERSAL SERVER RACK**			
	Width	EIA Standard 19" Rack Rails	**Pcs**	**1**
	Rack Units:	42U		
	External Width	~ 23.6" (600 mm)		
	Height	~ 78.74" (2000 mm)		
	External Depth	~ 47.24" (1200 mm)		
	Accessories	Adjustable mounting depth Casters, levelling feet included Cable pass-through in top & bottom of rack Vertical cable management bar One stationary shelves One sliding shelves		
	Warranty	min. 5 years		
7.	**SERVICES**			
	• Basic installation services • Training services • Data migration services • Services related to implementation and deployment Security services implementation and deployment • Cyber security services • Redundant interconnection of existing network devices with new equipment in the data centre • Proper documentation of all necessary/required aspects and guides/instructions or methodological documents, to ensure knowledge transfer and all necessary guidelines for ARIJ **The expected tasks are detailed in this section at C. OBJECTIVES OF THE ASIGNMENT**			

I. DELIVERY AND OTHER RELATED REQUIREMENTS

Delivery date	The entire assignment must not exceed 90 days after the contract is signed. Bidder shall deliver the goods within 60 days after contract signature and complete the services no later than 90 days after the contract is signed.
Delivery place / terms (INCOTERMS 2020)	DDP, 31 August 1989 St 82, MD-2012, Chisinau, Moldova
Customs clearance (must be linked to INCOTERM)	Shall be done by: ☒Supplier/Bidder UNDP shall provide a Tax Exemption letter for Customs clearance.
Installation Requirements	As per SECTION 5: SCHEDULE OF REQUIREMENTS
Testing Requirements	As per SECTION 5: SCHEDULE OF REQUIREMENTS
Scope of Training on Operation and Maintenance	As per SECTION 5: SCHEDULE OF REQUIREMENTS
Warranty Period	**36 MONTHS FOR ALL GOODS, EXCEPT RACK (60 MONTHS) AND UPS'S BATTERY (24 MONTHS) – WARRANTY DETAIL ARE SPECIFIED FOR EACH ITEM**
Local Service Support	Availability of authorised by manufacturer local representative/partner to handle warranty/hardware repair issues ensuring the comprehensiveness after-sales services in Chisinau, Moldova Bidder should indicate Service Centre name, address and contact details. The relationship between the Manufacturer, Service provider and the local representative/partner shall be duly documented:

	- Contract/Agreement/Letter signed by both parties confirming the relationship; - Official documentation stating that the Partner is a registered business; - A detailed profile of the local representative/partner
Technical Support Requirements	The Selected Bidder shall provide technical support through both online and on-site methods as needed. The support will be categorized into three urgency classes, each with specific response and resolution times. **Class 2** covers consulting inquiries where the client requires clarifications to implement or improve equipment and/or services. Examples include applying updates or configuring new features. For this class, the bidder is required to respond within 8 hours and provide a solution within 48 hours. **Class 1** addresses errors that do not currently affect functionality or service accessibility but could potentially lead to future incidents. For such errors, the bidder must respond within 4 hours and resolve the issue within 24 hours. **Class 0** involves incidents where the client encounters a technical or software-related issue that impacts the partial or complete functioning of equipment and/or services. In these cases, the bidder is required to respond within 1 hour and provide a solution by the next business day (NBD).
After-sale services Requirements	☒ Availability of written and signed statement of full warranty of 36 months for all goods, except rack (60 months) and UPS's battery (24 months); ☒ Availability of an authorized service center in Moldova ☒ Technical Support
Payment Terms	100% within 30 days upon UNDP's acceptance of the goods delivered as specified and receipt of invoice
Conditions for Release of Payment	☒ Inspection upon arrival at destination ☒ Installation ☒ Testing ☒ Training on Operation and Maintenance ☒ Written Acceptance of Goods based on full compliance with ITB requirements
All documentations, including catalogues, instructions and operating manuals, shall be in this language	☒ English; ☒ Others: Russian, Romanian