Annex 2.2. Technical specification for the Microsoft HCI Hyperconverged Infrastructure Deployment Services for the Central Election Commission (CEC) of Ukraine

1. Preparatory work

Analyse the existing IT infrastructure and document the configurations of components (virtual machine, service, etc.), including hardware specifications, software versions and network connections, which need to be migrated to the newly created infrastructure based on Microsoft Windows Server Datacenter software.

Analysis of the current state of the server and network infrastructure:

- Assessment of the capacity and performance of existing network switches and servers, network connections, software versions, BIOS, etc;
- Checking the configuration of switches for compatibility with the requirements of the software to be implemented;
- Assessment of network security and availability of redundant channels.

Checking the availability of backup and recovery:

- Assessment of the current state of data backup and recovery systems;
- determining the need for additional measures to ensure fault tolerance.

2. Deployment and configuration of the Commission's data centre infrastructure

2.1. Preparation of servers and network equipment:

Update the BIOS and other software of the servers and network equipment (if necessary).

Connect each server to two switches to ensure network resilience.

Configure the switches to ensure high availability and fault tolerance.

Install the software:

- Install Microsoft Windows Server Datacenter on each physical server;
- Setting up Hyper-V on each server to create virtual machines.

Setting up the cluster:

- Setting up Storage Spaces Direct (S2D) to provide highly available shared storage for various components of the CEC's IT infrastructure;
- setting up the necessary network connections for each server, including VLANs for the cluster and management networks.

Verification of settings:

Testing the cluster settings.

Verify S2D and network connections.

Verify fault tolerance and availability.

2.2.Specification of existing server and network equipment, for the deployment of hyperconverged infrastructure, is provided in Table 1.

Table 2 Existing physical servers Lenovo and network equipment

Manufacturer of server equipment	Lenovo;
Number of servers per cluster:	8 servers;
Server model:	ThinkSystem SR645 V3;
Number of engaged CPU sockets per 1 server:	2 sockets;
Model of CPU:	AMD EPYC 9354, 32 cores, 3.25 GHz, 256 Mb L3-cash;
Number of engaged DIMM sockets RAM per 1 server:	16 sockets;
Model of RAM modules:	ThinkSystem RDIMM-A 32 GB ThruDDR5 4800 MHz;
Number of storage devices for the OS per 1 server:	2;
Model of storage devices for the OS:	ThinkSystem SSD M.2 5400 PRO 480 GB SATA 6 Gbps;
RAID-controller for the storage devices for the OS:	ThinkSystem Raid 5350-8i for M.2 SATA boot Enablement;
Number of storage devices for S2D per 1 server:	8 board;
Model of storage devices for S2D:	ThinkSystem SSD 2.5'' U.2 P5620 3.2 TB NVMe;
Number of network adapter cards per 1 server:	2 boards;
Model of board of network adapters:	ThinkSystem MellanoxConnectX-6 Lx 2-port 10/25 GbE SFP28 in OCP and PCIe form-factors;
Number of network adapters per 1 server:	4 adapters;
Number of power supplies per 1 server:	2;
Model of power supplies:	ThinkSystem Gen2 Platinum 1800 W 230 V;

Manufacturer of ToR-switches:	NVIDIA;
Number of ToR-switches:	2;
Model of ToR-switches:	SN2410 48 ports – 25 GbE 8 ports – 100 GbE Managed Switch with Cumulus OS.

2.3.Specification of other existing server equipment to ensure the availability and fault tolerance of the CEC IT-infrastructure (for the deployment and/or migration of Microsoft AD DS, Microsoft CA and other services), is provided below Table 2 and Table 3:

Table 3 Other CEC existing server equipment

Manufacturer of server equipment:	Dell;
Number of servers:	2 servers;
Server model:	Dell PowerEdge R550;
Number of engaged CPU sockets per 1 server:	2 sockets;
Model of CPU:	Intel(R) Xeon(R) Silver 4314 CPU @ 2.40GHz, 16 cores, 24 MB L3-cash;
Number of engaged DIMM sockets RAM per 1 server:	12 sockets;
Model of RAM modules:	DRAM DDR4 32 GB 2666 MT/s;
Number of storage devices for the OS per 1 server:	2;
Model of storage devices for the OS:	SSD SATA 223Gb;
RAID-controller for the storage devices for the OS:	BOSS-S2, max capable speed 6Gbps;
Number of storage devices for S2D per 1 server:	6 board;
Model of storage devices for S2D:	SAS SSD 893Gb;
Number of network adapters per 1 server:	3 adapters;
Number of power supplies per 1 server:	2;
Model of power supplies:	0C8T2PA04 800Wt;

Table 4 Other CEC existing server equipment

Manufacturer of server equipment:	Dell;
Number of servers:	1 servers;
Server model:	Dell PowerEdge R740;
Number of engaged CPU sockets per 1 server:	2 sockets;
Model of CPU:	Intel(R) Xeon(R) Gold 6134 CPU @ 3.20GHz, 24 MB L3-cash;
Number of engaged DIMM sockets RAM per 1 server:	6 sockets;
Model of RAM modules:	DRAM DDR4 32 GB 2666 MT/s;
Number of storage devices for the OS per 1 server:	1;
Model of storage devices for the OS:	SSD SATA 223Gb;
RAID-controller for the storage devices for the OS:	PERC H740P Adapter;
Number of storage devices for S2D per 1 server:	2 board;
Model of storage devices for S2D:	SAS HDD 558Gb;
Number of network adapters per 1 server:	2 adapters;
Number of power supplies per 1 server:	2;
Model of power supplies:	900W, 230V.

3. ***Deployment and configuration of virtual servers of System Centre and WAC components to manage the Commission's IT infrastructure:***

   – Deploy and configure SCVMM to manage virtual machines and physical servers;

   – Deploy and configure SCOM for infrastructure monitoring;

   – deploying and configuring SCCM/MECM for centralised deployment, configuration management, software suites, updates on workstations, computers and servers;

   – WAC deployment and configuration - for centralised management of local and remote servers without the need to install agents;

   – configuring RBAC in System Centre and WAC components;

   – Configuring System Center component clustering for fault tolerance and availability.

Verification of settings:

Test the configuration of System Center and WAC components.

Verify the fault tolerance, availability, and access rights features.

4. ***Deployment (migration) and configuration of authorisation systems, access rights and other services required for the CEC IT infrastructure***

The CEC data centre infrastructure uses 3 separate ADDS domains based on Windows server:

- for LOM 1 environment - LOM1.GOV.UA;
- for LOM 2 - LOM2.GOV.UA;
- for LOM 3 environment - LOM3.GOV.UA.

The ADDS domain of the LOM1 environment is the highest in the hierarchy. One-way non-transitory trust links are built from it:

- LOM1.GOV.UA→LOM2.GOV.UA;
- LOM1.GOV.UA→LOM3.GOV.UA.

As part of this project, it is necessary to

- Provide the necessary network settings for server and switching equipment, deployment and configuration of Microsoft Windows Server Datacenter software and Microsoft System Centre tools, integration with cyber defence systems (if necessary);
- deploy a Microsoft Hyper-V virtual environment on a dedicated physical server;
- deploy a fault-tolerant and highly available AD DS and CA infrastructure using a separate physical server and Microsoft Windows Server Datacenter software cluster;
- ensure migration of virtual servers (AD DS, CA, Exchange, dhcp, IIS, MsSql, Oracle, PostgreSQL, terminal farms and application software) based on Windows Server (2012, 2016, 2019) from the existing virtual infrastructure running VMware Vshpere 7 to Microsoft Hyper-V;
- ensure migration of AD DS and CA virtual servers to provide a higher level of availability from the existing virtual infrastructure running VMware Vshpere 7 to a dedicated physical server;
- ensure the upgrade of existing Windows server versions to Windows Server 2022, where possible.

The migration and configuration of these systems shall be carried out without disruption, or with minimal disruption, to the Commission's existing IT infrastructure.

Verification of settings:

Testing of the AD DS and CA configuration.

Verification of the resilience and availability of the AD DS and CA services.

5. ***Integration with existing systems and data migration***

In the existing virtual infrastructure running VMware Vsphere 7, 50 Microsoft Server 2016 and 2019 virtual machines with various application information systems are running.

The VMware virtual environment is deployed on an HPE Synergy 12000 blade system with HPE SY 480 Gen10 servers.

As part of this project, it is necessary to ensure the migration of Windows Server virtual machines from the existing VMware virtual infrastructure to the Microsoft virtual infrastructure.

Ensure, where possible, that the versions of Windows Server 2016 and 2019 virtual machines are updated to Windows Server 2022, where applicable.

Ensure the fault tolerance and availability of these virtual machines.

Ensure the integration of the newly created virtual environment with the existing IT infrastructure of the CEC data centre and cyber security systems.

The migration and configuration of these systems should be carried out without interrupting the functioning of the existing IT infrastructure of the CEC's data centre or with minimal interruption.

6. Integration of Microsoft infrastructure with Cisco ACI Fabric and IBM QRadar SIEM system

The Contractor shall provide the Customer with the services of integration of Microsoft infrastructure with Cisco ACI Fabric and IBM QRadar SIEM system, taking into account the requirements of security, performance and event monitoring in the data centre.

Configuration services should include the following steps:

- Development of a target Microsoft cluster architecture.
- Integration of Cisco ACI into Microsoft infrastructure.
- Ensuring Cisco ACI integration with IBM QRadar.
- Ensuring the integration of Cisco ACI with Windows Admin Centre and AD.
- Providing L3Out and external access integration.
- Development of documentation.

Services for setting up the Subsystem shall include the following works:

- Requirements analysis and architectural planning:
- Analysis of the existing Microsoft server infrastructure, taking into account its current state and integration plans;
- Analysis of the Customer's network infrastructure, including Cisco ACI structure (switches, APICs, policies, topology);
- Analysis of existing or planned SIEM infrastructure based on IBM QRadar;
- Designing the logic of interaction between Cisco ACI, Microsoft infrastructure, and IBM QRadar;
- Development of a logical structure for traffic segmentation in Cisco ACI, including:

VRF - to differentiate traffic zones;

BD - for creating isolated broadcast domains;

EPG - for grouping objects with the same access policies;

Trust zoning according to traffic types: management, storage, VM, migration.

– Setting up Cisco ACI to create a segmented network infrastructure for the Microsoft cluster, where each type of traffic is isolated in its own logical zone (BD/EPG), which will ensure secure, manageable and productive interaction of infrastructure components.
– Services at this stage should include the following works:

Physical connection of Microsoft infrastructure server nodes to Cisco ACI Leaf switches;

Setting up individual EPGs (Endpoint Groups) for traffic types, including:

- Management (management: Windows Admin Centre, Cluster Services),
- VM traffic (Hyper-V virtual machines),
- Storage (storage: SMB/RDMA),
- Live Migration (virtual machine migration),
- Backup;

Configure the appropriate Bridge Domains (BD) for each EPG group;

Implementing access policies (contracts) between EPGs to regulate interaction;

Configure QoS and MTU parameters to meet the traffic requirements of the Microsoft infrastructure.

Provide integration with IBM QRadar for centralised collection of logs, telemetry and network events for further analysis and detection of potential threats in real time. Cisco ACI components should transmit SNMP, SYSLOG, and NetFlow data, and Microsoft infrastructure should transmit Windows event logs via WinRM or Sysmon.

Services at this stage should include the following work:

– Configuration of SNMP, SYSLOG, NetFlow, SPAN protocols on Cisco ACI network switches to enable telemetry and event collection;
– Organisation of logging from key components of Cisco ACI:

APIC controllers;

Nexus switches;

Bridge Domains (BD) and Endpoint Groups (EPG);

– Transmission of event logs to IBM QRadar via standard protocols and channels;
– Developing or adapting custom parsers (custom DSMs), if necessary, to support non-standard event formats;
– Setting up event correlation rules, defining security offences in the QRadar environment;
– Verification of event delivery and testing of incident detection mechanisms;
– Developing playbooks (incident response scenarios) for use by the SOC security team.

Ensure integration of Cisco ACI with Windows Admin Center and Active Directory for centralised, secure and managed administration of Microsoft infrastructure.

The services at this stage should include the following works:

- Providing secure access to the Microsoft cluster through Cisco ACI logic (APIC and EPG);
- Restriction of access to the Microsoft cluster based on policies set in ACI (EPG, Contracts), taking into account the principles of minimum required access;
- Integration of the Microsoft cluster with Windows Admin Centre (WAC) for centralised management;
- Integration with Active Directory (AD) to implement a role-based access model and authenticate cluster administrators;
- Transfer security and access events from the Microsoft cluster to IBM QRadar for analysis;
- Setting up mechanisms for auditing user actions based on the logic of interaction between Cisco ACI and QRadar.

Integration of L3Out and external access should provide multi-level access control, filtering and inspection of traffic passing between network segments.

Services at this stage should include the following work:

- Configuring the routing of external traffic through the Firepower NGFW firewall;
- Configuring the routing of internal HCI cluster traffic through the FortiGate NGFW firewall;
- Provide integration between Cisco ACI and external NGFWs using the L3Out mechanism;
- Implementation of SSL traffic inspection, application control, and information security policy enforcement (IPS, antivirus, DLP) at the Firepower and FortiGate levels;
- Separation of traffic between isolated zones (Management, Backup, VM, Internet) through NGFW policies;
- Transfer of security events from Firepower and FortiGate to the IBM QRadar SIEM system for further processing and correlation.

7. Information security requirements for creating a hyperconverged data centre infrastructure for the Central Election Commission

The deployment of Microsoft Windows Server Datacenter software and Microsoft System Center tools in the data centre of the Central Election Commission is aimed at ensuring the functioning of the components of the Unified Automated Information and Analytical System of the Central Election Commission on a single hardware and software platform using technologies that ensure efficient use and management of computing resources and their flexible scaling.

The infrastructure resulting from the deployment of Microsoft Windows Server Datacenter software and Microsoft System Center tools is a functional extension of the platform of the

automated information system for access control and information security (hereinafter referred to as the AIS ACIS), designed to host and ensure the secure operation of the Commission's information resources, registers, systems, websites, etc.

The said system has a comprehensive information security system with confirmed compliance and received a Certificate of Conformity No. 763B registered with the Administration of the State Service for Special Communications and Information Protection of Ukraine on 01 December 2023.

Information protection and cybersecurity of the Commission's data centre infrastructure is carried out by the existing means of the integrated information security system AIS USIB, in particular:

- Integration of Cisco ACI with IBM QRadar allows detecting critical events, including changes in network policies, suspicious activity between EPGs, unauthorised access to APICs, overloading and DoS attacks on Leaf switches;
- Events from the Microsoft infrastructure are fed into IBM QRadar, which provides in-depth analysis, anomaly detection, and the creation of offsets related to user activity;
- Thanks to access policies implemented through EPGs and Contracts in Cisco ACI and the use of Active Directory as an authentication source, critical services such as management, storage, and migration are isolated;
- Through the L3Out mechanism, Cisco ACI interacts with NGFW, which allows you to centrally manage routing, apply security policies, and transmit events to IBM QRadar.

When deploying and configuring a hyperconverged infrastructure, secure administrative access channels are used using TLS 1.3, SSH 2.0, and IPsec protocols.

These measures ensure an adequate level of cybersecurity and transparency of network interaction between data centre infrastructure services.

8. Requirements for the operating modes of Microsoft Windows Server Datacenter software and Microsoft System Center tools

The time mode of operation of the Central Election Commission's data centre infrastructure after the deployment of Microsoft Windows Server Datacenter software and Microsoft System Center tools should be permanent, which means that there is no set period of its operation regardless of the timing of elections or referendums.

The Microsoft software infrastructure can operate in different modes, depending on the scale and specifics of the technological load caused by the information flows that arise during elections or referendums. These modes include day-to-day mode and high load mode.

Day-to-day mode:

- Established under normal conditions, when there are no extraordinary, peak loads on infrastructure resources or the threat of their occurrence.

– It is characterised by the normal functioning of the system, without additional measures.

Heavy load mode:

– It is set in case of unstable loads on Microsoft software infrastructure resources, which may affect its stability and fault tolerance.
– It is characterised by increased monitoring of the functioning of the Microsoft software infrastructure.

9. Reliability requirements

The Microsoft software infrastructure must be available 24 hours a day, 7 days a week, 365 days a year. Secure storage and backup of all Microsoft infrastructure process data shall be provided.

Define the target indicators:

RTO (maximum allowable recovery time): no more than 4 hours;

RPO (maximum allowable data loss): no more than 15 minutes.

10. Requirements for the development and delivery of services.

The deployment of Microsoft Windows Server Datacenter software and Microsoft System Center tools in the data centre of the Central Election Commission should include the following stages:

1) development of a working draft;

2) testing of the Microsoft software infrastructure or its components;

3) conducting commissioning works;

4) conducting trial operation of the data centre infrastructure;

5) setting up the elements of the information security system with which the integration is carried out.

If necessary, the stages may be supplemented with new ones or combined depending on the specifics of the information technology tool.

Infrastructure testing is carried out jointly with the Customer's representatives.

The scope of work at the stage of preliminary testing of the information technology tool or its components, types of tests and their sequence shall be agreed with the Customer.

The results of the preliminary tests shall be documented in a test report, which shall record the fact of the infrastructure testing.

Based on the results of the tests, a test report is prepared, which indicates the results of the tests, errors and defects identified, as well as recommendations for their elimination.

The test programme and methodology shall be developed by the Contractor and approved by the Customer.

The test programme and procedure shall include:

- testing the functioning of all systems and subsystems deployed on the Microsoft software infrastructure;
- testing the fault tolerance and availability of services and services in case of failure of a part of the server or communication equipment;
- testing the speed and efficiency of shared s2d storages and virtual machines;
- testing disaster recovery scenarios in accordance with the approved DRP;
- testing the interaction of the Microsoft software infrastructure with other systems of the existing infrastructure;
- checking the distribution of access rights and security rule settings;
- modelling failures of individual cluster nodes;
- checking the compliance of logging and logging (SIEM QRadar) with detected security events.

The test programme and methodology may also include other tests proposed by the contractor.

Development of documentation

The Contractor shall develop the following working, operational and project documentation.

Indicative list of working documentation:

1) test programme and methodology;

2) plan for deployment of Microsoft Windows Server Datacenter software and Microsoft System Center tools in the data centre of the Central Election Commission;

3) data (information) migration plan to the Microsoft software infrastructure;

4) a report or protocol on the test results.

Indicative list of operational and design documentation:

1. Passport/form of the new software and hardware infrastructure based on Microsoft solutions.

2. Target architecture of the new software and hardware infrastructure based on Microsoft solutions.

Quality of services and oversees:

Technical support, including the scheduled maintenance for 1 (one) year after deployment, should include the following services:

1. Consultations on configuration and fine-tuning of Microsoft software that is part of the HCI cluster, as well as IBM QRADAR software and Cisco ACI infrastructure — limited to the scope in which they interact with the Microsoft components of this computing complex;

2. Consultations on the update processes of Microsoft, IBM, and Cisco software that are components of the HCI cluster and / or interact with it — but only in the part where such interaction involves Microsoft software;

Clear SLA should also be provided, including response time and problem resolution terms, available support channels, and a defined escalation process.

11. Conclusions

As a result of deploying Microsoft Windows Server Datacenter software and Microsoft System Center tools in the data centre of the Central Election Commission, the Customer shall receive

in terms of deploying Microsoft software*:*

- Ready-to-use, configured and tested software and hardware infrastructure based on Microsoft solutions.
- A certificate of commissioning of the software and hardware infrastructure based on Microsoft solutions.
- Approved migration plan for the information system from the VMware vSphere virtualisation platform
- Documentation: target architecture, test methodology and programme, system data sheet, migration plan.
- The system meets the Customer's requirements for reliability, scalability, support and further integration with other components of the IT infrastructure.

In terms of integrating Microsoft infrastructure with Cisco ACI Fabric and the IBM QRadar SIEM system:

- Architectural integration model;
- Configured segmented Cisco ACI network for Microsoft infrastructure;
- Integration with IBM QRadar;
- Integration with Windows Admin Centre and AD;
- Configured interaction with NGFW via L3Out.