Annex 2.3. Technical requirements for Privileged Access Manager (PAM) deployment services for the Central Election Commission of Ukraine

1. Preparations
   - Analyze the existing IT infrastructure and document the configurations of components (virtual machines, services, etc.), including hardware, software, and network.
   - 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, etc.
     - Checking the configuration of switches for compatibility with the requirements of the PAM solution.
     - Assessment of network security and availability for privileged access management.

2. Deployment and Configuration of Privilege Access Manager
   - Installation and configuration of the network environment and virtual/physical appliances.
   - Creating a fault-tolerant cluster in active/passive mode.
   - Installation and initial setup of Privileged Access Manager.
   - Configuration of the role-based access control (RBAC) model for PAM management.
   - Onboarding and Configuration of Target Systems:
     - RDP Connectivity: Configuring secure, agentless access to Windows-based assets, including terminal server setup, resolution settings, and clipboard/drive redirection controls.
     - SSH Connectivity: Configuring secure access to Unix/Linux systems and network devices, including SSH key management and command filtering.
     - HTTPS Connectivity: Integrating web-based management interfaces for secure proxied access without direct credential exposure.
     - Session Management: Enabling mandatory video/text session recording and real-time monitoring for all RDP, SSH, and HTTPS connections.
     - Credential Management: Configuring automated password rotation and vaulted storage for privileged accounts associated with the target systems.
   - Backup and Disaster Recovery:
     - Configuring automated backup policies for the PAM configuration and database.
     - Connecting target storage and verifying data recovery procedures.

3. Integration with AD, configure integration with ADFS using SAML.
4. Integration with IBM QRadar
   - Analysis of the existing SIEM infrastructure based on IBM QRadar.
   - Designing the logic of interaction between PAM and IBM QRadar.
   - Configuring PAM to forward logs and events (via Syslog/LEEF) to IBM QRadar for centralized collection, real-time threat detection, and audit analysis.

5. Testing
   - Development of a comprehensive testing program (Acceptance Test Plan).
   - Functional testing of the Privileged Access Manager (session recording, password vaulting, zero-trust access).
   - Development of the final testing report.

6. Documentation

The following documentation must be provided:

1. High-Level Design (HLD) and Low-Level Design (LLD) for the PAM solution.
2. Administrator and User Manuals tailored to the implemented environment.
3. Operational Acceptance Document (Testing Report).