***Technical Compliance Form***

Bidders are requested to demonstrate compliance with the following requirements and add any further information in support of their Bid. Please refer to the relevant section of the Terms of Reference (ToR) for further explanation of the requirements. The information from the below offered tables will form an integral part of the technical evaluation process. Bidders should avoid simply writing “comply” without providing further information or evidence to support the claim, as this will not generally reflect well in the evaluation. Reference can be made to annexes or other material in the Bid.

**Table no. 1 – Mandatory Requirements (Pass/Fail Criteria)**

| **No.** | **Mandatory Requirement** | **Bidder’s Response**  *Please tick applicable* | | **Bidder’s**  **Clarification** |
| --- | --- | --- | --- | --- |
| **Yes** | **No** |
| **Vendor Requirements** | | | | |
| 1. | Bidder must have at least 5 years of experience in providing Qualys solutions and support |  |  |  |
| 2. | Bidder must have ISO27001 or equivalent security certificate |  |  |  |
| 3. | Acceptance of the OSCE Non-Disclosure Agreement (sample of the template provided; the successful Bidder will be requested to sigh it at the stage of Contract signature) |  |  |  |
| 4. | Acceptance of the OSCE Declaration of Impartiality, Confidentiality and Conflict of Interest (sample of the template provided; the successful Bidder will be requested to sigh it at the stage of Contract signature) |  |  |  |
| **Solution Requirements** | | | | |
| 5. | A cloud-hosted vulnerability assessment and management platform based on Qualys Enterprise version that provides the ability to assess security vulnerabilities for 8,000 internal (including 5,500 with Cloud Agent) and 96 external IPs |  |  |  |
| 6. | Virtual scanner appliances on VMWare platform (6 appliances, support for vSphere 6.0 – 6.7 mandatory) |  |  |  |
| 7. | Cloud Agents for all endpoints and servers on internal network (at least 5,500 hosts) |  |  |  |
| 8. | Unified View of asset and vulnerability data from network and agent-based scans, without duplication of assets |  |  |  |
| 9. | Reporting capabilities as described in the Terms of Reference (point 4) |  |  |  |
| 10. | Vulnerability data export and import for custom reporting and data input (e.g., approved asset inventory) to/from the OSCE internal MS-SQL database, via API |  |  |  |
| 11. | Capability to local IT staff across the Organisation to manage their own scanning, asset management and reporting tasks |  |  |  |
| 12. | Vulnerability assessment and reporting with differentiated levels of risk per vulnerability and recommended remediation targets per vulnerability based on criticality of asset and severity of vulnerability |  |  |  |
| 13. | Authenticated/encrypted report delivery |  |  |  |
| 14. | Assignment of vulnerability remediation tasks to asset pool owners with remediation deadlines based on criticality of asset and severity of vulnerability |  |  |  |
| 15. | Unlimited number of users |  |  |  |
| 16. | Differentiated user roles by privilege level, asset pool and device access |  |  |  |
| 17. | Authenticated network scans for network devices and non-endpoint devices (e.g. printers, scanners, IoT devices, etc.) |  |  |  |
| 18. | Two-factor authentication (use of RSA token is preferred as this is already available at the OSCE) |  |  |  |
| 19. | Upgrade protection including signature updates, patches and upgrades to major releases as well for the full period of contract |  |  |  |
| 20. | Remote and on-site support, training and maintenance services on an as-requested basis for configuration, changes, reports and operational issues |  |  |  |