RFQ–4006–12147–Network Assessment Activity Remediation

1. Scope of Work

The Service Provider's will be responsible to apply the recommended fixed identified during the network assessment activities for the following Campuses and Data Centers.

The below-mentioned locations will be part of our scope;

i. IBA Main Campus – University Enclave, University of Karachi
ii. IBA City Campus – Kiyani Shaheed Road, Garden Karachi

1.1 Remediation Activities

The scope will cover for applying the fixes for the following segments at a minimum:

Gap Identified in Network Assessment (Phase-1)	List of Activities and Required Documents (Phase-2)
Both the Main Campus (Huawei S12700E-4) and City Campus (Huawei S12800E-4) core switches are deployed as single standalone switch with no CSS clustering/HA, dual supervisor modules, or secondary failover device. A hardware or software failure on either core switch results in a complete site-wide network outage.	**Activities:** Rack and cable secondary core switch at each campus Configure CSS domain, device priority, and CSS link ports on both units Verify all existing VLAN SVIs, routing config, and access switch uplinks are intact post-CSS formation Test failover **Required Documents:** Method of Procedure (MoP) — CSS clustering (one per campus) Rollback plan
At Main and City Campus, the same Sangfor NGFW is used to enforce policy for both internal network traffic and for DMZ/internet traffic. There is no dedicated DC firewall isolated from the DMZ network perimeter device. SPOF for internal and internet segment and also becoming single layer of defence from advanced threats.	**Activities:** Design zone-based firewall architecture Map all existing traffic flows that need to be migrated to the new dedicated DC firewall Rack and cable dedicated DC firewall at each campus Verify all DC-hosted services are reachable post-migration Verify internal DMZ traffic on existing NGFW is unaffected **Required Documents:** Method of Procedure (MoP) — dedicated DC firewall deployment Rollback plan
The Top-of-Rack switches in the City Campus are deployed as a standalone device with no stacking or redundancy. All City Campus Data Center & DMZ traffic passes through this single device — its failure would isolate all DC & DMZ servers from the internet and NGFW simultaneously.	**Activities:** Rack and cable second ToR switch in City Campus DC and DMZ Configure CSS clustering between the twog Test failover **Required Documents:** Method of Procedure (MoP) — ToR CSS clustering Rollback plan
	Activities:

The WAN aggregation switches at both the Main Campus and City Campus are deployed as single standalone devices with no stacking or redundancy. All internet traffic at each site passes through one device — its failure causes a complete internet outage at that campus regardless of how many ISPs are provisioned on this switch.	Rack and cable secondary WAN switch at each campus Configure stacking between primary and secondary WAN switches Verify ISP links are distributed across both WAN switch units Test failover **Required Documents:** Method of Procedure (MoP) — WAN switch HA deployment WAN switch stack design and cabling diagram Rollback plan
Single Sangfor IAM-5400 inline in bridge mode at Main and City Campus — no redundancy at hardware level. Its failure silently blackholes all traffic between core and NGFW even though both those devices are still up	**Activities:** Cable secondary IAM unit inline parallel to primary at both campuses Configure HA heartbeat link between primary and secondary IAM units Set primary/secondary roles and failover trigger thresholds Test failover **Required Documents:** Method of Procedure (MoP) — IAM HA deployment Rollback plan
The IPSec site-to-site VPN tunnel configured between Main Campus and City Campus is not using AES (Advanced Encryption Standard) for data encryption method. The current configuration relies on a weaker cipher, which is considered cryptographically weak by modern standards and is no longer recommended for protecting sensitive data in transit.	**Activities:** Audit current IKE Phase 1 and IPSec Phase 2 proposals on both campus NGFWs Schedule coordinated maintenance window for both campuses simultaneously **Required Documents:** Method of Procedure (MoP) — IPSec re-keying Pre/post NGFW configuration backup Change Request Rollback plan
An "Allow All" firewall policy rule has been identified on the Sangfor NGFW at Main and City Campus Firewalls. In both sites, this rule eliminates the intended security, posture of the firewall and permits unrestricted traffic flows that have not been explicitly reviewed or approved.	**Activities:** Export and review full firewall rule base from both campus NGFWs Analyze traffic logs to enumerate all flows currently hitting the Allow All rule Categorize flows by source zone, destination zone, port, protocol, and business purpose Build explicit least-privilege permit rules for each legitimate traffic flow Peer review all new rules with security team before deployment Deploy new explicit rules in test/staging order Demote Allow All rule to bottom of policy base once all flows are covered Verify zero hits on Allow All rule over a 24-hour monitoring period **Required Documents:** Method of Procedure (MoP) — firewall rule base cleanup Firewall policy design document (zone matrix — Untrust/DMZ/Trust) Rollback plan
	Activities:

Incorrect STP root bridge placement and mode mismatch in Recommendation a large-scale multi-vendor access layer creates a fragile Layer 2 foundation that is prone to loops, suboptimal forwarding paths, and slow convergence during failures. This must be corrected systematically across both campuses. The core switch STP priority has not been explicitly set to the lowest value.	Audit current STP mode on all switches at both campuses Identify current root bridge per VLAN across all switches **Required Documents:** Method of Procedure (MoP) — STP MSTP migration Rollback plan (revert to previous STP mode per switch)
Default routes (0.0.0.0/0) are configured on both the Main and City core switches and the DMZ switches, pointing toward the Sangfor NGFW as the next hop. The absence of more specific routing policy, route summarization, and any routing protocol or failover mechanism means that if the NGFW becomes unreachable, due to failure, maintenance, or interface flap and all traffic from both the core and DMZ is immediately blackholed with no automatic failover or re-routing capability. Additionally, a single static default route provides no path diversity, no load balancing, and no ability to influence routing decisions based on traffic type or destination, certainly optimal routing is missing.	**Activities:** Document current default route configuration on core and DMZ switches at both campuses Design Huawei / IP SLA Cisco probe targeting NGFW gateway IP Review and clean up any unnecessary static routes on switches **Required Documents:** Method of Procedure (MoP) — default route tracking
The trunk interface on the core switch connecting to the WLC is configured to allow all VLANs rather than being restricted to only the required wireless VLANs and the WLC management VLAN. This means every VLAN in the network including data centre server VLANs is advertised and accessible over the WLC trunk link.	**Activities:** Identify exact VLAN IDs required on the WLC-facing trunk. Document current trunk allowed VLAN list on core switch port connected to WLC at both campuses Restrict allowed VLANs on WLC trunk to only required VLANs **Required Documents:** Method of Procedure (MoP) — WLC trunk restriction Rollback plan
Multiple physical links and VLAN configurations exist across the switching infrastructure at Main and City Campus that are no longer in active use. May cause harm to create a Layer-2 loop in the network. It is also observed during the assessment phase that many Layer-2 trunk and access ports are cascading that may create a loop in the network	**Activities:** Cross-reference each candidate port with the network team to confirm no active purpose Administratively shut down candidate ports Physically remove confirmed unused patch cables Remove confirmed unused VLANs from VLAN database and trunk allowed-VLAN lists Update physical connectivity diagram and VLAN register **Required Documents:** Method of Procedure (MoP) — link and VLAN cleanup Rollback plan
SNMPv2c is a community-based protocol that lacks encryption and	**Activities:** Audit all devices at both campuses for active SNMPv2c community strings

strong authentication mechanisms, making it vulnerable to unauthorized access, interception, and potential misuse. The coexistence of SNMPv2c alongside SNMPv3 introduces a security risk, as less secure protocols remain accessible.	Confirm SNMPv3 is already configured and functional on all devices Disable SNMPv2c community strings on all devices **Required Documents:** Method of Procedure (MoP) — SNMP hardening
The current network design does not follow the standard hierarchical model (Core–Distribution–Access). The absence of a Distribution/Aggregation layer results in direct dependency on the Core for access-level connectivity, not following the standard network design best practices. Also, consuming the expensive ports or core switches	**Activities:** Design three-tier hierarchical network model — Core / Distribution / Access for both campuses Define distribution layer switch placement, VLAN assignment, and uplink design per campus zone/floor/building **Required Documents:** Method of Procedure (MoP) — distribution layer deployment (phased, one MoP per zone)
The wireless controller and VLAN configuration are not properly optimized, leading to failures in client association, authentication, or IP address assignment. This indicates gaps authentication mechanisms, or controller-level configurations.	Method of Procedure (MoP) — DHCP and wireless remediation
The absence of a consistent and resilient NTP configuration indicates non-compliance with best practices for time synchronization across network infrastructure, also impact the troubleshooting with time co-relation	**Activities:** Audit current NTP configuration on all core, distribution, access, firewall, and WLC devices Push consistent NTP server configuration to all devices at both campuses **Required Documents:** Method of Procedure (MoP) — NTP standardization NTP server details and design document
The use of EoS/EoL devices in critical network layers violates lifecycle management and network design best practices. Additionally, placing such devices in roles connected directly to the Core increases operational and security risks due to, it may hit any vulnerability/CVE.	**Activities:** Compile full inventory of all EoL and unsupported devices at both campuses Prioritize devices by criticality Rack and cable replacement device Migrate configuration to replacement device Migrate physical cable connections from old to new device **Required Documents:** Method of Procedure (MoP) — EoL device replacement Rollback plan
It is identified during the assessment phase that many interfaces has either no description, improper description or wrong/old description, that may lead to bring up or down any connected devices by taking decision on the basis of interface description	**Activities:** Define a standard interface description format Cross-reference descriptions against physical connectivity map and device inventory Identify interfaces with no description, wrong description. Update descriptions on all interfaces across ~230 switches at both campuses. **Required Documents:**

1.2 Deliverable

The scope of work defined above will be covered in the deliverable with the minimum service interruption and impact, where possible. As a deliverable of this engagement, Service Provider will carry out the fixes on the current network and security infrastructure using the industries' best practices and also IBA's technical and business requirements.

considering the following parameters;

- ✓ *High Availability*
- ✓ *Scalability*
- ✓ *Security*
- ✓ *Performance*

1.3 Related Documents:

IBA, Karachi will require the relevant documents to participate;

- ✓ Current Network Design Diagram (physical/logical)
- ✓ Current list of Business critical / non-critical applications
- ✓ Current network issues (if any) identified in the past days
- ✓ Current Network devices' IP and VLAN schema
- ✓ Current Network devices' (updated) configurations
- ✓ Current Network device inventory

1.4 High-Level Project Plan

The below provides the details of the high-level project plan of Service Provider/Subject Matter Expert (SME) engagement in this project.

Phase-2	Service Description	Estimated Duration
Remediation Activity	Performing the remediation activities as described on the	30 days~40 days

1.5 Payment Terms and Conditions:

- ✓ Total project cost/price required.
- ✓ 3% Service Tax should be mentioned separately.
- ✓ 100% payment after project completion and its acknowledgment from IBA ICT department.