IT Security Audit Checklist for Network Vulnerability Assessment

Conducting an **IT security audit checklist** for network vulnerability assessment ensures comprehensive identification of potential threats and weaknesses. This process helps organizations safeguard their data by systematically evaluating network components and configurations. Regular audits enhance overall security posture and compliance with industry standards.

Checklist

1. **Network Inventory and Documentation**
   - Document all network assets (servers, routers, switches, firewalls, endpoints).
   - Verify up-to-date network diagrams.
   - Maintain an inventory of installed software and firmware versions.
2. **Configuration & Access Control**
   - Review firewall and router configurations.
   - Ensure minimal necessary open ports.
   - Check for secure configuration baselines across all devices.
   - Verify least-privilege access controls for network resources.
3. **Patch Management**
   - Check for operating system and application updates.
   - Validate timely deployment of security patches.
4. **Vulnerability Scanning**
   - Run vulnerability scans on internal and external interfaces.
   - Review and remediate any high or critical vulnerabilities.
5. **Authentication & Authorization**
   - Enforce strong password policies (length, complexity, expiration).
   - Review multi-factor authentication (MFA) implementation.
   - Check for inactive accounts and remove or disable as appropriate.
6. **Logging & Monitoring**
   - Enable logging on all critical network devices.
   - Regularly review logs for suspicious activities.
   - Confirm centralized log management and retention policies.
7. **Remote Access & VPN**
   - Audit VPN configurations and access controls.
   - Verify encryption and secure tunneling protocols.
   - Limit remote access privileges to necessary personnel.
8. **Physical and Wireless Security**
   - Check physical security of network equipment.
   - Audit wireless network configurations for encryption and access controls.
   - Disable broadcasting of unsecured SSIDs.
9. **Incident Response Readiness**
   - Verify existence of incident response plan and procedures.
   - Test communication channels for incident escalation.
   - Review backup and disaster recovery processes.
10. **Compliance & Policy Review**
    - Ensure compliance with relevant regulations (e.g., GDPR, HIPAA, PCI-DSS).
    - Update and communicate security policies to staff.

Recommendations

- Perform regular audits (quarterly or after significant changes).
- Remediate vulnerabilities as soon as identified.
- Train staff on security best practices and awareness.
- Continuously monitor threat intelligence sources for emerging risks.