Network Security Audit Checklist

OPENVPN

A practical, zero-trust-aligned checklist for IT and security teams

Use this checklist to work through a network security audit end to end. Check off each item as you confirm it, note any gaps as you go, and use the results to build your audit report. For a walkthrough of each section, see the full guide at blog.openvpn.net/network-security-audit-checklist.

1 Classify Asset Inventory

Know what's connected before you try to secure it.

- ☐ Inventory all servers, endpoints, IoT devices, and cloud instances
- ☐ Flag unmanaged or unauthorized (shadow IT) devices
- ☐ Rank assets by data sensitivity and business impact
- ☐ Document an owner for every asset on the list

2 Review Access Controls & User Permissions

Confirm the right people have the right access — and no one else does.

- ☐ Audit user roles against current job functions
- ☐ Enforce least-privilege access across systems and data
- ☐ Flag unused, orphaned, or excessive permissions
- ☐ Confirm offboarded employees' access was fully revoked

3 Review Network Configurations & VPN Policies

Check how traffic actually moves through your network.

- ☐ Confirm MFA is enforced for all VPN and remote access
- ☐ Review firewall and router rule sets for outdated entries
- ☐ Audit site-to-site VPN connections and encryption standards
- ☐ Verify split-tunneling and access policies match current needs

4 Assess Vulnerability & Patch Status

Unpatched software is one of the most preventable causes of a breach.

- ☐ Run vulnerability scans across servers, endpoints, and network devices
- ☐ Confirm patch coverage for OS, firmware, and third-party software
- ☐ Flag end-of-life or unsupported systems for replacement

- [ ] Schedule recurring automated scans, not one-off checks

5 Monitor Log Management

You can't investigate what you never logged.

- [ ] Centralize logs from network devices, servers, and applications
- [ ] Set alerting thresholds for anomalous or suspicious activity
- [ ] Confirm log retention meets your compliance requirements
- [ ] Test that logs are usable during an incident, not just collected

6 Review Compliance Policies

Make sure documented policy matches what's actually enforced.

- [ ] Map current controls against applicable regulatory frameworks
- [ ] Identify and close documentation gaps
- [ ] Confirm evidence exists to support each compliance claim
- [ ] Schedule a follow-up review ahead of the next audit cycle

Quick Tips for Running the Audit

- Set clear goals before you start the audit
- Assign an owner and document every step
- Run this audit on a repeatable cadence — quarterly or semiannual
- Start with one department or system, then expand

Ready to move toward Zero Trust?

CloudConnexa from OpenVPN makes network security audits easier from the start, with centralized access control, logging, and zero trust network access built in. Learn more at openvpn.net/cloud-vpn.