Network Security Audit Checklist

Comprehensive audit of firewalls, access controls, encryption, and network segmentation. Identify vulnerabilities and strengthen your network security posture with this structured checklist.

8	60+	Score	Free
SECURITY DOMAINS	AUDIT ITEMS	EACH SECTION OUT OF 10	PRINT & AUDIT

How to Use This Checklist

Work through each section with your network administrator or IT provider. Tick items that are fully in place and documented. Score each section out of 10. Any section scoring below 6 indicates a security gap that should be addressed urgently.

1 Firewall Configuration

Verify the firewall is properly configured, up to date, and following security best practices.

- [ ] Firewall **firmware is current** — check vendor site for latest stable release
- [ ] **Default admin credentials** have been changed and admin access uses strong, unique passwords
- [ ] Firewall management interface is **not accessible from the internet** (WAN side)
- [ ] All **unused ports and services** are explicitly blocked (deny-all default with allow exceptions)
- [ ] **Outbound traffic filtering** is enabled — not just inbound rules
- [ ] Firewall **rules are documented** with business justification for each allow rule
- [ ] A **rule review** has been conducted in the last 90 days to remove stale or unnecessary rules
- [ ] **Intrusion Detection/Prevention** (IDS/IPS) is enabled and signatures are up to date

Section Score: _____/10

2 Network Segmentation

Verify the network is properly segmented to contain breaches and control access.

- [ ] **VLANs** are configured to separate corporate, guest, VoIP, IoT, and server traffic
- [ ] **Inter-VLAN routing** is controlled via ACLs — only necessary traffic is permitted between VLANs
- [ ] **Guest WiFi** is on a separate VLAN with no access to internal resources
- [ ] **IoT devices** (printers, cameras, smart devices) are on an isolated VLAN
- [ ] **Server infrastructure** is on a dedicated VLAN with restricted access from user VLANs
- [ ] **Management VLAN** exists for network device administration, isolated from user traffic
- [ ] Network segmentation has been **tested with penetration tools** to verify isolation

Section Score: _____ /10

3 Wireless Security

Verify wireless networks are secured against unauthorised access and eavesdropping.

- [ ] **WPA3-Enterprise or WPA2-Enterprise** (802.1X) is used for corporate WiFi
- [ ] **Pre-shared keys** are not used for corporate WiFi (PSK is acceptable for guest networks only)
- [ ] Guest WiFi requires **acceptance of terms** and has bandwidth limitations
- [ ] **Rogue AP detection** is enabled to identify unauthorised access points
- [ ] **WiFi passwords** (if PSK is used anywhere) are changed at least quarterly
- [ ] Access points **firmware is current** and centrally managed
- [ ] **Client isolation** is enabled on guest networks to prevent device-to-device communication

Section Score: _____/10

4 Access Control & Authentication

Verify network access is properly controlled and authenticated.

- [ ] **802.1X port-based authentication** is implemented on wired network ports
- [ ] **MAC address filtering** is in place as an additional layer (not sole security measure)
- [ ] **Network device admin access** uses individual accounts with MFA, not shared credentials
- [ ] **RADIUS or TACACS+** is used for centralised network device authentication
- [ ] **SSH** is used for remote management (Telnet is disabled)
- [ ] **SNMP v3** with authentication and encryption is used (SNMPv1/v2 disabled)
- [ ] Admin **access logs** are retained and reviewed for suspicious activity

Section Score: _____/10

5 Encryption & Data Protection

Verify data in transit is encrypted and sensitive communications are protected.

- [ ] All **VPN connections** use strong encryption (AES-256, IKEv2 or WireGuard)
- [ ] **SSL/TLS certificates** are valid, current, and use TLS 1.2 minimum (TLS 1.0/1.1 disabled)
- [ ] **DNS over HTTPS (DoH)** or DNS over TLS (DoT) is configured for DNS privacy
- [ ] **Email encryption** (TLS) is enforced for email in transit
- [ ] **Remote access** to internal systems requires VPN or ZTNA — no unencrypted RDP exposed
- [ ] Sensitive **file transfers** use SFTP or HTTPS (FTP is disabled)

Section Score: _____ /10

6 Monitoring & Logging

Verify network activity is monitored, logged, and alerts are configured for security events.

- [ ] **Network monitoring** is active 24/7 with alerts for anomalies, downtime, and threshold breaches
- [ ] **Firewall logs** are collected, stored, and retained for minimum 90 days
- [ ] **DNS query logs** are monitored for indicators of compromise (C2 callbacks, malicious domains)
- [ ] **NetFlow or sFlow** data is collected for traffic analysis and anomaly detection
- [ ] **Failed authentication attempts** trigger alerts after a defined threshold
- [ ] **Bandwidth usage** by device/VLAN is monitored to detect unusual patterns
- [ ] Log data is **sent to a SIEM** or centralised logging platform for correlation and analysis

Section Score: _____ /10

#	AREA	SCORE	PRIORITY
1	Firewall Configuration	/ 10	H / M / L
2	Network Segmentation	/ 10	H / M / L
3	Wireless Security	/ 10	H / M / L
4	Access Control	/ 10	H / M / L
5	Encryption & Data Protection	/ 10	H / M / L
6	Monitoring & Logging	/ 10	H / M / L
TOTAL SCORE		**/ 60**	

Score Interpretation

80–100: Excellent — well-managed with only minor improvements needed.
60–79: Good foundation but gaps exist. Prioritise areas scoring below 6.
Below 60: Significant gaps putting your business at risk. Seek specialist review.

! Action Items & Notes

Top 3 Priority Actions:

1. _____
2. _____
3. _____

Notes

_____

_____

Need a Professional Network Security Audit?
Our engineers can conduct a thorough network security assessment and provide a prioritised remediation plan.

info@cloudswitched.com
New London House, 6 London St, London EC3R 7LP

Completed by: _____ Date: _____ Next review: _____

© 2026 CloudSwitched Limited. All rights reserved. This resource is provided for informational purposes and does not constitute professional IT advice.