CLOUDSWITCHED

FREE RESOURCE — AUDIT CHECKLIST

Network Security Audit Checklist

Stress-test your network defences against ten audit areas covering firewalls, segmentation, wireless, remote access, encryption, monitoring, vulnerability management, device hardening, identity and incident response. Score each area to surface the gaps an attacker would find first.

10	75+	/10	Fillable
AUDIT AREAS COVERED	AUDIT ITEMS TO CHECK	SCORE EACH SECTION	TICK & TYPE IN ANY VIEWER

FIREWALL · SEGMENTATION · ENCRYPTION · VULN MGMT

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this checklist

Work through each of the ten sections with your network team, your MSP, or whoever owns the network and security stack. Tick every checkpoint that is **fully in place** — not partially, not "we're scoping it", but in production with evidence (a config, a screenshot, a scan report, an SLA log). Then award each section a score out of 10 based on how many checkpoints you can confidently tick.

A score **below 6 in any section** is the kind of gap an attacker, an insurer, or a Cyber Essentials Plus assessor will land on. Use the action items page at the back to capture your top three priorities. This is an **interactive PDF** — tick the boxes and type your scores and notes directly in any modern PDF viewer.

WHAT THIS CHECKLIST IS

A baseline self-assessment for UK SMEs covering the network-security hygiene controls a competent IT or security function should be running — firewall and perimeter, segmentation, wireless, remote access, encryption, monitoring, vulnerability management, device hardening, identity / NAC and incident response. It is not an ISO 27001 audit and does not certify Cyber Essentials Plus, but it surfaces the gaps those regimes — and a real-world intrusion — will pick up first.

SCORING GUIDANCE

Award one point per checkpoint where you have evidence the control is in place — a config, a scan, a policy, a SIEM rule, a contract. Half-measures and "on the roadmap" do not score. Round each section to the nearest whole number out of 10 and carry it forward to the summary on page 13.

The ten sections

- **01 Firewall & Perimeter Defence** — NGFW, rule review, IDS/IPS, geo-blocking, DDoS.
- **02 Network Segmentation & VLANs** — guest/IoT/server isolation, inter-VLAN ACLs.
- **03 Wireless Network Security** — WPA3, 802.1X, rogue AP detection, WIPS.
- **04 Remote Access & VPN** — ZTNA, MFA, device posture, vendor / PAM access.
- **05 Encryption (Transit & at Rest)** — TLS, IPsec, disk encryption, certificates.
- **06 Intrusion Detection & Monitoring** — SIEM, NDR, DNS logging, alerting.
- **07 Vulnerability Management & Patching** — scans, patch SLAs, EOL, pen test.
- **08 Network Device Hardening** — default creds, mgmt access, CIS benchmark.
- **09 Identity & Network Access Control** — 802.1X, RADIUS, PAW, privilege review.
- **10 Incident Response & Network Forensics** — IRP, tabletop, EDR isolation, logs.

01

Firewall & Perimeter Defence

The firewall is the front door. Audit whether it is a stateful, inspected, monitored boundary — or a box that hasn't been touched since install. Ask to see the rule base, the last change ticket, and the IDS/IPS update log.

- ☐ A **next-generation firewall (NGFW)** with deep packet inspection is deployed at every internet boundary *(not a basic ISP router)*.
- ☐ The **firewall rule base is reviewed at least quarterly**; orphaned, any-any, and shadowed rules are removed with a change ticket.
- ☐ A **default-deny outbound policy** is enforced — only required egress destinations and ports are explicitly allowed.
- ☐ **IDS/IPS signatures** are enabled in blocking mode, updated daily, and alerts feed into the SOC or MSP queue.
- ☐ **Geo-blocking** is applied to countries with no business relationship and to high-risk hosting ASNs.
- ☐ The **firewall management plane** is reachable only from a dedicated management VLAN with MFA — not from the corporate LAN.
- ☐ **Configuration backups** are taken before every change, retained 90+ days, and a restore has been tested in the last 12 months.
- ☐ **DDoS protection** (cloud-scrubbing or ISP-level) is contracted and the runbook has been rehearsed.

WHAT GOOD LOOKS LIKE

Every rule has a ticket, an owner, and an expiry. Outbound is default-deny with an allow-list of business destinations. IDS/IPS is in block mode with tuned signatures and the SOC sees the alerts within minutes — not in a weekly digest.

SECTION 01 SCORE _____ / **10** *Aim for 8+. Below 6 = perimeter is porous.*

02

Network Segmentation & VLANs

Segmentation is what stops a single compromised laptop from becoming a domain-wide incident. Check that your VLAN strategy is real, enforced by firewall ACLs, and documented — not just a colour on a Visio diagram from 2021.

- ☐ A **documented segmentation strategy** exists naming every VLAN, its purpose, and its trust zone.
- ☐ **Guest WiFi** is on a dedicated VLAN with internet-only egress; no route to corporate, server, or printer networks.
- ☐ **IoT, OT, and printer VLANs** are isolated; outbound is restricted to required cloud services only.
- ☐ **Server and database VLANs** are only reachable from defined client segments and admin jump hosts.
- ☐ Inter-VLAN traffic is enforced by **firewall ACLs** — not routed open at L3 with a permissive switch.
- ☐ **Micro-segmentation** or host-firewall policy is applied for crown-jewel servers (DCs, finance, file servers).
- ☐ The **network diagram** with VLANs, IP ranges and firewall zones has been updated in the last six months.

WATCH OUT FOR

A flat /24 where laptops, servers, printers and the CCTV NVR all share the same broadcast domain. One ransomware foothold then has direct line-of-sight to every asset on the network — no lateral movement skill required.

SECTION 02 SCORE _____ / **10** *Aim for 8+. Below 6 = flat network risk.*

03

Wireless Network Security

Wireless is the easiest place to put a foot wrong — a single misconfigured SSID or stale PSK opens the LAN to anyone in the carpark. Audit your APs, controllers and SSIDs against the modern WPA3 / 802.1X baseline.

- ☐ Corporate APs use **WPA3-Enterprise** (or WPA2-Enterprise minimum) with 802.1X / RADIUS authentication.
- ☐ **Pre-shared keys** (WPA-PSK) are used only for guest / IoT SSIDs and rotated at least quarterly.
- ☐ Separate **SSIDs for corporate, guest and IoT** exist; cross-SSID client isolation is enforced.
- ☐ **Rogue access point detection** is enabled and alerts on unknown SSIDs and MAC addresses.
- ☐ Wireless **controller and AP management** require MFA and live on the management VLAN.
- ☐ A **wireless site survey** has been performed in the last 18 months; no client-side coverage gaps or hidden APs.
- ☐ **Wireless intrusion prevention (WIPS)** is active, including deauth-flood, evil-twin and karma-attack detection.

PSK ROTATION REALITY

Any single staff leaver, contractor handover, or guest who jots the PSK on a sticky note effectively breaks your guest WiFi forever. Quarterly rotation — or moving to 802.1X — is the only reliable answer.

SECTION 03 SCORE _____ / **10** *Aim for 8+. Below 6 = wireless is the soft spot.*

04

Remote Access & VPN

Remote access is no longer a perk — it is a permanent expansion of your attack surface. Check that VPN / ZTNA is gated by MFA and device posture, not just a username and password that survived the move from the old office.

- ☐ A **VPN or ZTNA** solution is in production; split-tunnel policy is documented and justified.
- ☐ **MFA is enforced** on every remote access account, including service and admin identities.
- ☐ Remote access is gated by **device posture** — compliant, patched, encrypted, EDR healthy.
- ☐ **Always-on VPN or ZTNA** is enforced for managed devices; users cannot opt out of corporate inspection.
- ☐ Remote access **logs are retained 12+ months** and reviewed for anomalies (impossible travel, off-hours, geo).
- ☐ Decommissioned VPN accounts and shared credentials are **removed within 24 hours of departure**.
- ☐ Vendor and third-party remote access uses **time-bound, audited PAM sessions** (jump host, recorded).

THE LEAVER GAP

The 24-hour leaver SLA is the single most-failed control in every audit. If the question "can the person who left last Friday still VPN in?" makes you check — you have a gap. Tie remote access to your HR offboarding event, not to a calendar reminder.

SECTION 04 SCORE _____ / **10** *Aim for 9+. Below 6 = remote access is exposed.*

05

Encryption (Transit & at Rest)

Encryption is binary: it either works on every link and every disk, or you have a hole. Audit your cipher suites, certificate inventory, and disk-encryption posture — including the boring corners (printer queues, backup tapes, internal management interfaces).

- ☐ **TLS 1.2+** is enforced on every public service; TLS 1.0 / 1.1 and SSL are disabled everywhere.
- ☐ Internal east-west traffic is encrypted (**IPsec, MACsec, or TLS**) wherever it crosses untrusted links.
- ☐ **Disk encryption** (BitLocker, FileVault) is enforced on every endpoint and verified centrally each week.
- ☐ **Server disks and SAN/NAS volumes** are encrypted at rest; key management is documented and tested.
- ☐ TLS certificates are **auto-rotated** (ACME / managed CA); no manual renewals on critical services.
- ☐ An **internal CA / certificate inventory** exists; expired or weak (SHA-1, <2048-bit RSA) certs are replaced.
- ☐ Wireless and VPN tunnels use only **modern ciphers** (AES-GCM, ChaCha20); legacy ciphers blocked.
- ☐ **Backups are encrypted** in transit and at rest; key-recovery procedure tested in the last 12 months.

SECTION 05 SCORE _____ / **10** *Aim for 9+. Below 6 = data exposure risk.*

06

Intrusion Detection & Monitoring

You cannot defend what you cannot see. Verify that critical logs land in a SIEM or managed XDR, that alerts route to someone who is awake, and that detection use-cases are tuned beyond the vendor defaults.

- ☐ A **SIEM or managed XDR/MDR** ingests logs from firewall, AD, M365, EDR and key servers.
- ☐ **Log retention** is at least 12 months online for hot search, with cold archive beyond.
- ☐ Critical alerts route to a **24/7 monitored channel** (SOC, MSP, or on-call rota).
- ☐ Detection use-cases are tuned for **impossible travel, password spray, lateral movement** and data exfiltration.
- ☐ **Network detection and response (NDR)** is deployed on critical segments; PCAPs captured for incidents.
- ☐ **DNS logging** is on for every endpoint; sinkholing of known C2 domains is enabled.
- ☐ **Threat-intelligence feeds** enrich alerts; IoC blocklists update automatically.

DETECTION VS ALERT NOISE

A SIEM that fires 500 medium-severity alerts a day is functionally the same as no SIEM — nobody reads them. Tune for fewer, higher-fidelity detections tied to MITRE ATT&CK techniques relevant to your stack, and review the noise quarterly.

SECTION 06 SCORE _____ / **10**

Aim for 8+. Below 6 = blind to intrusion.

07

Vulnerability Management & Patching

Vulnerability management is not a quarterly Nessus scan that nobody reads. Audit your scan cadence, your patch SLAs, your exception register, and the number of EOL systems still in production with no replacement plan.

- ☐ **Authenticated vulnerability scans** run at least weekly across servers, endpoints and network gear.
- ☐ Internet-facing assets are **scanned externally at least weekly** with continuous attack-surface monitoring.
- ☐ **Patch SLAs** are defined and met: critical 14 days, high 30 days, medium 90 days (CIS-aligned).
- ☐ A documented **exception process** exists for unpatched systems, with compensating controls and an owner.
- ☐ **End-of-life software** is identified; replacement dates and budget assigned, with formal risk acceptance.
- ☐ Patch deployment is **automated** for endpoints (WSUS / Intune / Jamf / MDM) with compliance reporting.
- ☐ Network device **firmware** (firewalls, switches, APs) is on a managed update cycle with rollback plans.
- ☐ An **annual penetration test** (external + internal) is commissioned; findings tracked to closure.

CVE DOESN'T CARE IF YOU'RE BUSY

Cyber Essentials v3.3 requires high/critical patches within 14 days of vendor release — and your cyber-insurance underwriter increasingly asks for the same. Treat the patch SLA as a hard contract, not a stretch goal.

SECTION 07 SCORE _____ / **10** *Aim for 8+. Below 6 = patch debt is critical.*

08

Network Device Hardening

Default credentials, open management protocols and stale configs are the classic findings in any external penetration test. Audit every switch, router, firewall and AP against the boring — but mandatory — hardening baseline.

- ☐ **Default vendor credentials** are removed from every device, switch, AP and console port.
- ☐ Admin access uses **centralised auth** (TACACS+ / RADIUS) with MFA — not local accounts.
- ☐ Management protocols are **SSH and HTTPS only**; Telnet, HTTP and SNMPv1/v2c are disabled.
- ☐ **Configurations are version-controlled**, backed up nightly, with file-integrity checks against drift.
- ☐ **Unused physical ports** are administratively shut down or in a quarantine/black-hole VLAN.
- ☐ A **CIS or vendor hardening benchmark** is applied; deviations are documented and risk-accepted.
- ☐ **Time synchronisation (NTP)** is hardened: trusted sources, authenticated, monitored for drift.

THE 30-MINUTE WIN

Removing default credentials, disabling Telnet/HTTP/SNMPv1, and forcing SSH-key auth on management interfaces is a half-day exercise per site — and closes the three findings every external pen-tester will surface in their report.

SECTION 08 SCORE _____ / **10** *Aim for 9+. Below 6 = device hardening gap.*

09

Identity & Network Access Control

Identity is the new perimeter, but the network still has to enforce it. Verify that 802.1X is on every port, that privileged users have separate admin accounts and PAWs, and that privilege gets reviewed — not just granted.

- ☐ **802.1X port-based authentication** is enforced on every wired and wireless corporate port.
- ☐ Unauthorised devices are routed to a **quarantine VLAN** with no corporate or server access.
- ☐ **RADIUS / NPS infrastructure** is redundant, monitored, and forwards logs to the SIEM.
- ☐ **Privileged identities** use separate admin accounts (no day-to-day login or mailbox).
- ☐ **Privileged Access Workstations (PAWs)** or jump hosts are used for all infrastructure administration.
- ☐ **Account lockout**, Conditional Access and risk-based MFA policies are enforced and tested.
- ☐ A **quarterly privileged-access review** is signed off; orphaned admin rights are revoked.

PAW DISCIPLINE

The most damaging incident in any modern intrusion chain is the moment a domain admin opens an Outlook attachment on the same workstation they use to RDP to the DC. PAWs are the single highest-leverage control you can add this quarter.

SECTION 09 SCORE _____ / **10** *Aim for 8+. Below 6 = privileged-access risk.*

10

Incident Response & Network Forensics

Every organisation will face an incident; the question is whether you can respond in hours, not days. Audit your runbooks, your retainer, your forensic log retention, and the date of your last tabletop — "someone wrote a plan in 2022" does not score.

- ☐ A written **Incident Response Plan** exists with named roles, contact tree, and decision authority.
- ☐ A **tabletop exercise** has been run in the last 12 months; gaps documented and closed with owners.
- ☐ A **24/7 escalation route** exists to an MSP, SOC, or Incident Response retainer with a defined SLA.
- ☐ **Forensic-quality logs** (firewall, DNS, NetFlow, AD, EDR) are retained for at least 12 months.
- ☐ EDR can **isolate hosts on demand**; isolation has been drilled in the last 12 months.
- ☐ The **ICO 72-hour breach reporting** process is documented; legal and PR contacts are in the contact tree.
- ☐ A **post-incident lessons-learned** process exists; findings feed back into control improvements.

THE RETAINER TEST

Pick up the phone right now and call your incident-response number. If it rings out, goes to voicemail, or you do not have a number to call — you do not have an incident-response capability, you have a hopeful spreadsheet.

SECTION 10 SCORE _____ / **10** *Aim for 8+. Below 6 = no incident readiness.*

Σ

Audit score summary

Transfer the score for each section into the table. Set a priority (H/M/L) based on the gap to target. Anything below 6 is a candidate for the top-3 actions on the next page.

#	AUDIT AREA	SCORE / 10	PRIORITY
01	Firewall & Perimeter Defence	_____ / 10	☐ H ☐ M ☐ L
02	Network Segmentation & VLANs	_____ / 10	☐ H ☐ M ☐ L
03	Wireless Network Security	_____ / 10	☐ H ☐ M ☐ L
04	Remote Access & VPN	_____ / 10	☐ H ☐ M ☐ L
05	Encryption (Transit & at Rest)	_____ / 10	☐ H ☐ M ☐ L
06	Intrusion Detection & Monitoring	_____ / 10	☐ H ☐ M ☐ L
07	Vulnerability Management & Patching	_____ / 10	☐ H ☐ M ☐ L
08	Network Device Hardening	_____ / 10	☐ H ☐ M ☐ L
09	Identity & Network Access Control	_____ / 10	☐ H ☐ M ☐ L
10	Incident Response & Network Forensics	_____ / 10	☐ H ☐ M ☐ L
Σ	**TOTAL SCORE**	_____ / 100	—

Interpretation & priority actions

Translate your total score into a risk band, then commit to a small number of next steps. The goal is one page of decisions, not a wish list.

Score interpretation

80–100	**Strong.** Posture is mature. Focus on detection tuning, drills and emerging threats.
60–79	**Foundational, gaps exist.** Prioritise any area scoring below 6 with owners and deadlines.
Below 60	**Material risk.** Commission a formal network-security review and a remediation plan.

Top 3 priority actions

01 _____

02 _____

03 _____

Additional notes

_____

_____

_____

_____

AUDIT COMPLETED BY _____ DATE _____ NEXT REVIEW DUE _____

CLOUDSWITCHED

NETWORK SECURITY & CYBER SERVICES

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom