CLOUDSWITCHED

FREE RESOURCE — AUDIT CHECKLIST

Business Internet Connectivity Audit

Assess your current business internet against ten audit areas covering speed, reliability, resilience, equipment, WiFi, remote access, security, cost and forward planning. Score each area to identify weak spots before they cost you a working day.

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

LEASED LINE · FTTP & SOGEA · FAILOVER · SD-WAN

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 whoever owns your network — an internal IT lead, your managed service provider, or your incumbent ISP. Tick every checkpoint that is **fully in place** — not partially, not "we're planning it", but live and verifiable today. 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 a connectivity gap that will cost you a working day at the worst possible moment. 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.

Current service snapshot

PROVIDER	CURRENT SPEED	MONTHLY COST
CONTRACT END	SLA	NOTES

SCORING GUIDANCE

Award one point per checkpoint where you have evidence the control is in place — a contract, a screenshot, a monitoring graph, an SLA report. Half measures 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 Current Service & Provider** — contract, technology, support boundary.
- **02 Speed & Bandwidth** — sync rate, headroom, symmetry, usage data.
- **03 Reliability & Uptime** — SLA, monitoring, MTTR, credit clauses.
- **04 Resilience & Failover** — secondary line, 4G/5G, SD-WAN, tested fallback.
- **05 Network Equipment & Cabling** — router, switches, structured cabling, UPS.
- **06 WiFi Coverage & Performance** — site survey, APs, capacity, guest separation.
- **07 Remote Access & VPN** — secure tunnels, MFA, split tunnelling, ZTNA.
- **08 Security & Filtering** — firewall, DNS, DDoS, content filtering, IDS.
- **09 Cost, Contract & Vendor Management** — pricing, renewals, escalation, billing.
- **10 Strategic Planning & Future-Proofing** — roadmap, growth, cloud, IPv6.

01

Current Service & Provider

Start with the basics — you cannot improve what you cannot describe. Every business should know exactly what service it is paying for, which technology delivers it and who picks up the phone when it breaks. Ask for the contract and the order confirmation as evidence.

- ☐ The **current provider name**, account number and primary support number are recorded and accessible offline.
- ☐ The **connection technology** is documented — FTTP, FTTC, SoGEA, leased line (EoFTTC, EFM, fibre) or fixed wireless.
- ☐ The **contracted speed** (download / upload) and any committed information rate (CIR) is documented in writing.
- ☐ A copy of the **signed contract** is on file with start date, term length and renewal date clearly marked.
- ☐ The **service is a business-grade product** with a business SLA — not a residential or "business broadband" consumer line.
- ☐ The **support boundary is clear** — you know which faults the ISP owns vs. your LAN, router or onsite cabling.
- ☐ The **account login** for the ISP portal is held by the business *(not by a single individual who could leave)*.
- ☐ A **fault-reporting runbook** exists — who calls who, what reference numbers to quote, and what to do if it is still down after 1 hour.

WHAT GOOD LOOKS LIKE

A one-page service record that any staff member can read in 30 seconds: provider, line type, speed, account number, support number, contract end date. Pinned in the comms cabinet and on the IT shared drive.

SECTION 01 SCORE _____ / **10** *Aim for 8+. Below 6 = service-knowledge gap.*

02

Speed & Bandwidth

Bandwidth is the variable everybody complains about — usually for the wrong reason. Check that the line is delivering what was sold, that you have measured real-world usage and that there is headroom for peak loads and cloud-heavy applications.

- ☐ A recent **independent speed test** has been run from a wired connection at the router during business hours.
- ☐ The measured speed is **within 10%** of the contracted speed for download *and* upload (or the leased-line CIR).
- ☐ **Upload bandwidth** is sufficient for cloud backup, video calls and SaaS uploads — not just download-heavy planning.
- ☐ A **symmetric service** (or near-symmetric) is in place if the business runs hosted phone, video conferencing or remote backup.
- ☐ **Bandwidth utilisation** is monitored — peak and 95th-percentile usage data is available for the last 30 days.
- ☐ There is at least **30% headroom** on the line at the busiest hour of the busiest day of the week.
- ☐ Bandwidth needs are **re-evaluated annually** against headcount, hybrid working patterns and cloud-app adoption.
- ☐ A **QoS / traffic shaping policy** protects voice and video traffic when the line is under pressure.

WATCH OUT FOR

"Up to" headline speeds on consumer-style products that quietly drop in the evening, on rainy days, or after the cabinet fills up. Get the SLA — if there is no committed rate, you are buying weather.

SECTION 02 SCORE _____ / 10 *Aim for 8+. Below 6 = bandwidth bottleneck.*

03

Reliability & Uptime

Reliability is harder to see than speed and matters more. Every hour of downtime is wages paid for staff who cannot work, plus the deals you never closed because the phone was offline. Validate the SLA you bought against the uptime you actually got.

- ☐ The contract has a **written uptime SLA** with a target percentage — e.g. 99.9% or 99.95% per month.
- ☐ The SLA specifies **mean-time-to-repair (MTTR)** targets for P1, P2 and P3 faults in hours.
- ☐ **Service credits** apply automatically (or on request) when the SLA is missed — you have the clause and the process to claim.
- ☐ An **uptime report** for the last 12 months is available from the provider *(not just a verbal "we've been pretty good")*.
- ☐ Outages are **logged internally** with date, time, duration and impact — cross-checked against ISP fault tickets.
- ☐ **Independent monitoring** (UptimeRobot, ThousandEyes, ISP probe, or router-side ping) records availability outside the ISP's own view.
- ☐ **Planned maintenance windows** are notified in advance and scheduled outside business hours wherever possible.
- ☐ Latency and packet loss are **within tolerable thresholds** for voice (<150ms, <1% loss) and video.

"NO SLA" IS THE SLA

If the small print does not commit to a number, the provider is committing to nothing. Residential and many "business broadband" packages still ship without an SLA — meaning a three-day outage is annoying for you and contractually fine for them.

SECTION 03 SCORE _____ / **10** *Aim for 8+. Below 6 = exposed to outages.*

04

Resilience & Failover

Single lines fail. The question is whether the building stops working when yours does. Verify there is a genuine secondary path — not just an idea in someone's head — and that it has been tested in the last six months.

- ☐ A **secondary internet path** is provisioned — a second leased line, a different-network FTTP, 4G/5G failover, or fixed wireless.
- ☐ The secondary path uses a **diverse carrier or last mile** — not two Openreach lines that share the same cabinet.
- ☐ **Automatic failover** is configured — SD-WAN, dual-WAN router or BGP — so users do not need to do anything when the primary drops.
- ☐ Failover has been **tested in the last 6 months** by deliberately disconnecting the primary line and timing the cutover.
- ☐ Critical applications (VoIP, video, key SaaS) are **verified to still function** on the failover path at acceptable quality.
- ☐ If the secondary is metered (e.g. 4G data SIM), there is a **plan for sustained outages** — data allowance, tariff, escalation.
- ☐ A **UPS or battery backup** protects the router, switch and any onsite phone system long enough to ride out a power blip.
- ☐ A **business continuity plan** for total internet loss exists — mobile tethering, hotspot kits, work-from-home fallback.

DIVERSITY IS THE WHOLE POINT

Two FTTC lines into the same Openreach cabinet are not resilient — they fail together. Genuine resilience means different last-mile technology, ideally a different carrier, and a tested cutover. Otherwise you are paying twice for the same single point of failure.

SECTION 04 SCORE _____ / **10** *Aim for 8+. Below 6 = single-line risk.*

05

Network Equipment & Cabling

The fastest line in the world is wasted on a tired router or a fly-lead through a wall. Audit the building-side kit your traffic actually flows through — the router, the switch, the patch panel, the structured cabling and the cabinet that hosts them.

- ☐ The **router / firewall** is a business-grade device under active manufacturer support — not an ISP hub or end-of-life model.
- ☐ The router has **throughput headroom** for the contracted speed with deep packet inspection and VPN enabled.
- ☐ All **core switches are managed**, Gigabit (or 2.5/10 Gigabit where the line demands it) and have redundant uplinks where possible.
- ☐ **Structured cabling** is Cat 5e or better, terminated to a patch panel and clearly labelled at both ends.
- ☐ The **comms cabinet** is tidy, ventilated, locked and free of dust, dead patch leads and unidentified spaghetti.
- ☐ Network equipment is **on a UPS** and the UPS is tested at least annually with a load runtime check.
- ☐ All network **firmware is current** and patched on a scheduled cycle — not "whenever someone remembers".
- ☐ A current **network diagram** exists showing routers, switches, APs, cabling runs and ISP terminations.

THE ROUTER IS THE BOTTLENECK MORE OFTEN THAN THE LINE

Cheap ISP-supplied routers throttle at 200–300 Mbps once you enable firewall, IPS or VPN features. If you have just upgraded to a gigabit FTTP service and the speed test still reads 300 Mbps, blame the box on the wall before you blame the line.

SECTION 05 SCORE _____ / **10** *Aim for 8+. Below 6 = equipment bottleneck.*

06

WiFi Coverage & Performance

To most users, WiFi *is* the internet. A perfect leased line looks broken from a meeting room with one bar. Audit coverage, capacity and configuration — not just the marketing on the side of the access point box.

- ☐ A **WiFi site survey** has been carried out in the last 24 months covering every working area, meeting room and warehouse zone.
- ☐ **Coverage is documented** on a floor plan with signal-strength heatmaps and known dead zones identified.
- ☐ **Access points** are business-grade (Cisco Meraki, Aruba, Ruckus, Ubiquiti) and centrally managed — not consumer routers.
- ☐ APs support **WiFi 6 or WiFi 6E** where the line speed and device fleet justifies it.
- ☐ A **separate guest SSID** is in place on a separate VLAN with client isolation enabled and no access to corporate resources.
- ☐ The corporate SSID uses **WPA2-Enterprise or WPA3-Enterprise** with 802.1X authentication — not a shared PSK on a sticky note.
- ☐ AP **capacity is monitored** — client counts, channel utilisation, retransmit rates — and APs are added where load is hot.
- ☐ Recurring WiFi complaints are **logged and root-caused** — not parked with "try restarting the router".

A PRE-SHARED KEY IS NOT A NETWORK

If everyone in the office knows the WiFi password, so does everyone who has ever worked there, plus their plus-ones. WPA-Enterprise ties access to a user identity that you can revoke when someone leaves — no key rotation party required.

SECTION 06 SCORE _____ / **10**

Aim for 8+. Below 6 = WiFi user pain.

07

Remote Access & VPN

Hybrid working makes the home worker's laptop part of your network. Verify there is a secure, MFA-protected way back into corporate resources — and that anything still using a flat IPsec tunnel and a shared password is on a plan to die.

- ☐ A **secure remote-access solution** is in place — VPN, ZTNA (Cloudflare Access, Zscaler) or RDP gateway behind MFA.
- ☐ **Multi-factor authentication** is enforced on every remote-access login — no exceptions for "trusted" users or service accounts.
- ☐ The VPN **capacity** (concurrent users, throughput) matches the number of users likely to connect on a worst-case day.
- ☐ **Split-tunnelling** is configured sensibly — cloud traffic goes direct, internal traffic via VPN — to avoid hairpinning everything through one office line.
- ☐ Remote-access accounts use the **same identity** as everything else (Entra ID, Google) so disabling a user kills VPN access too.
- ☐ **VPN logs** are retained for at least 90 days and reviewed for unusual locations, times or session lengths.
- ☐ Remote-access concentrators run **current firmware** — CVE-rated VPN vulnerabilities are patched within 14 days.
- ☐ A **migration to ZTNA** is at least planned — legacy "VPN into the office LAN" is being retired in favour of per-application access.

VPN IS THE RANSOMWARE ON-RAMP

Every major ransomware family of the last three years has a "VPN appliance vulnerability" entry on its kill chain. If your VPN box is on its original 2019 firmware and the login is single-factor, treat it as the most exposed surface you own.

SECTION 07 SCORE _____ / **10** *Aim for 8+. Below 6 = remote-access risk.*

08

Security & Filtering

The line out of your building is also the line in. Make sure there is a firewall doing real work, that outbound DNS is filtering known-bad destinations, and that nobody is running last decade's ruleset on this year's threat landscape.

- ☐ A **business-grade firewall** sits at the perimeter with explicit deny-by-default and documented rule justifications.
- ☐ The firewall ruleset is **reviewed at least annually**; stale rules referencing decommissioned services are removed.
- ☐ **IDS/IPS** is enabled and signatures are kept current — not just licensed and switched off.
- ☐ **DNS-layer filtering** blocks malware, C2 and known-phishing domains *(Cloudflare Gateway, Cisco Umbrella, Quad9 for business)*.
- ☐ **Content filtering** prevents access to high-risk categories — with exceptions logged and reviewed.
- ☐ **DDoS protection** is in place for any public-facing service hosted at the office *(or those services are behind a CDN / cloud proxy)*.
- ☐ Inbound **port forwarding is minimised** — every open port has a documented owner and a current security reason to exist.
- ☐ Firewall and security logs are **centralised** (SIEM, cloud log store) and retained for at least 90 days.

"IT CAME WITH THE LINE"

The router the ISP sent in the box is not a firewall. It blocks unsolicited inbound, and that is all. If your only network defence is an ISP hub, you are one IoT camera away from someone using your line for things you do not want to explain to the ICO.

SECTION 08 SCORE _____ / **10** *Aim for 9+. Below 6 = perimeter exposed.*

09

Cost, Contract & Vendor Management

Connectivity contracts auto-renew. Quietly. Most businesses are still paying 2019 pricing for 2019 speeds. Audit what you actually pay, what you get for it and whether your renewal clock has already started ticking.

- ☐ The **monthly cost** of every connectivity line and add-on is documented — primary, failover, static IPs, public DDoS, SD-WAN.
- ☐ Each invoice is **checked against the contracted price** — not auto-paid into oblivion.
- ☐ The **renewal date** is logged in a calendar that someone owns, with a reminder set 90 days before expiry.
- ☐ **Auto-renewal clauses** are understood — you know how and when to issue notice of non-renewal.
- ☐ **Like-for-like quotes** have been gathered from at least two alternative providers in the last 24 months.
- ☐ The **cost per Mbps** is roughly market-rate — check against current FTTP, leased-line and SoGEA UK averages.
- ☐ A **vendor relationship review** happens at least annually — service usage, fault history, billing accuracy, account-manager response.
- ☐ A documented **escalation contact** beyond first-line support exists — you know who to call when it has been down for two hours.

OUT-OF-CONTRACT PRICING IS A SILENT TAX

Many ISPs roll out-of-contract lines onto inflated month-to-month tariffs that quietly outpace inflation. A renewal date that came and went six months ago can mean you are paying 30–50% over an equivalent new-customer quote on the same product.

SECTION 09 SCORE _____ / **10** *Aim for 8+. Below 6 = overpaying / locked in.*

10

Strategic Planning & Future-Proofing

The internet is not a fixed input — it is the substrate the rest of the business runs on. Audit whether someone is paying attention to where it has to be in 18 months, not just whether it works today.

- ☐ A **connectivity roadmap** for the next 18–24 months exists — upgrades, sites, technology transitions and renewals on a single page.
- ☐ Bandwidth growth is **forecast against headcount, cloud spend and hybrid working** — not just guessed at renewal time.
- ☐ The line type is **future-proof** — FTTC is being phased out by 2027 (UK PSTN switch-off) and is on a transition plan to FTTP or fibre leased line.
- ☐ **Hosted VoIP / UC** readiness is verified — line speed, jitter, QoS and failover suitable for cloud telephony.
- ☐ **SD-WAN, SASE or ZTNA** options have been evaluated against current cost and growth plans.
- ☐ **IPv6 readiness** has been assessed — even if not enabled today, the network can support dual-stack when needed.
- ☐ Any **new office, expansion or relocation** has a connectivity workstream started at least 90 days before move-in.
- ☐ Senior leadership has **visibility of the connectivity risks** — not just the bill — in the form of a short annual review.

THE PSTN SWITCH-OFF IS NOW

Openreach has begun retiring the analogue PSTN and copper-derived broadband across the UK, with full migration to all-IP services by 2027. If your line is still FTTC or relies on a PSTN voice circuit, it has a hard expiry date — plan the migration, do not wait for the letter.

SECTION 10 SCORE _____ / **10** *Aim for 8+. Below 6 = drifting toward an upgrade emergency.*

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	Current Service & Provider	_____ / 10	☐ H ☐ M ☐ L
02	Speed & Bandwidth	_____ / 10	☐ H ☐ M ☐ L
03	Reliability & Uptime	_____ / 10	☐ H ☐ M ☐ L
04	Resilience & Failover	_____ / 10	☐ H ☐ M ☐ L
05	Network Equipment & Cabling	_____ / 10	☐ H ☐ M ☐ L
06	WiFi Coverage & Performance	_____ / 10	☐ H ☐ M ☐ L
07	Remote Access & VPN	_____ / 10	☐ H ☐ M ☐ L
08	Security & Filtering	_____ / 10	☐ H ☐ M ☐ L
09	Cost, Contract & Vendor	_____ / 10	☐ H ☐ M ☐ L
10	Strategic Planning & Future-Proofing	_____ / 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	**Excellent.** Your IT setup is well-managed. Focus on continuous improvement and emerging threats.
60–79	**Good foundation, gaps exist.** Prioritise any area scoring below 6 with owners and deadlines.
Below 60	**Significant gaps.** Consider an urgent review with an external IT specialist or MSP.

Top 3 priority actions

01 _____

02 _____

03 _____

Additional notes

_____

_____

_____

_____

AUDIT COMPLETED BY _____ DATE _____ NEXT REVIEW DUE _____

Need help closing the gaps?

Cloudswitched runs full connectivity audits for UK SMEs — line specification, resilience design, SD-WAN, vendor renegotiation and PSTN-switchoff migration plans.

info@cloudswitched.com

cloudswitched.com/services/connectivity

CLOUDSWITCHED

BUSINESS INTERNET & NETWORK SERVICES

info@cloudswitched.com

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