Business Internet Connectivity Audit Checklist

Comprehensive audit of your business internet infrastructure covering connection performance, ISP contracts, redundancy, security, and future scalability — 60+ items across 7 sections.

7	60+	Score	Free
AUDIT SECTIONS	ITEMS TO CHECK	EACH SECTION OUT OF 10	PRINT & USE NO STRINGS

How to Use This Checklist

Work through each section with your IT team or managed service provider. Test connection performance using real-world tools before scoring. Flag any items scoring below 6 for immediate attention and create a prioritised action plan.

Need Help With Your IT?

Our team can help you implement the recommendations in this resource.

info@cloudswitched.com
+44 2030 043 450
New London House, 6 London St, London EC3R 7LP

1 Current Connection Assessment

Document and evaluate every internet connection across your business to understand your baseline before making improvements.

- [ ] Document the **primary internet connection type** at each site — FTTC, FTTP, leased line, EFM, or 4G/5G (include bearer speed and contention ratio)
- [ ] Record the **contracted download and upload speeds** for each connection and compare to actual speeds delivered
- [ ] Identify the **ISP and circuit reference numbers** for every connection to streamline support requests
- [ ] Document the **router and modem models** in use, including firmware versions and whether they are ISP-provided or owned
- [ ] Check the **physical entry point** of each internet connection into the building — note condition of cabling and termination points
- [ ] Verify the **IP addressing arrangement** — static IPs, dynamic allocation, or IP subnets provided by the ISP
- [ ] Record current **average bandwidth utilisation** during peak hours using SNMP monitoring or router statistics (target: below 70% sustained utilisation)
- [ ] Identify any **single points of failure** in the physical path from the ISP demarcation point to your core network equipment
- [ ] Check whether **IPv6 is supported** on your current connections and whether your network equipment can handle dual-stack operation

Section Score: _____/10

2 Speed & Performance Testing

Objective performance measurements reveal whether your connection is delivering what you're paying for and meeting business needs.

- [ ] Run **speed tests at multiple times** throughout the business day (9am, 12pm, 3pm, 5pm) to identify peak-hour degradation
- [ ] Test from a **wired connection directly to the router** to eliminate WiFi variables from the measurement
- [ ] Measure **latency (ping)** to key business services — aim for under 20ms to UK-hosted services and under 50ms to European
- [ ] Test **jitter** using VoIP-specific tools — jitter above 30ms causes noticeable call quality degradation (target: below 15ms)
- [ ] Measure **packet loss** over a sustained period — any packet loss above 0.5% will affect VoIP and video conferencing quality
- [ ] Run a **throughput test to your cloud services** (Azure, AWS, Microsoft 365) to measure real-world application performance
- [ ] Test **upload speeds specifically** — asymmetric connections may bottleneck video calls, cloud backups, and file uploads
- [ ] Compare results against **Ofcom's broadband performance data** for your area to determine if your speeds are typical or below par
- [ ] Document results in a **baseline performance report** for future comparison after changes or upgrades

Section Score: _____ /10

3 ISP Contract Review

Your ISP contract determines your costs, service levels, and flexibility. Review it critically to ensure it still serves your needs.

- [ ] Check the **contract end date** and notice period required for cancellation or changes (diary the notice deadline)
- [ ] Review the **SLA for uptime** — business-grade connections should guarantee 99.9% or higher with financial penalties for breaches
- [ ] Verify the **guaranteed minimum speed** in the contract and whether your connection consistently meets or exceeds it
- [ ] Review **fault repair times** in the SLA — standard is typically 7 hours for business circuits; check if you're paying for enhanced
- [ ] Check for **fair usage policies** or data caps that could throttle your connection during heavy use periods
- [ ] Review the **annual price increase clause** — many ISPs increase by RPI plus 3–5% annually; negotiate a cap
- [ ] Confirm whether **static IP addresses** are included or charged as an add-on, and how many you have allocated
- [ ] Review **early termination charges** and understand the financial implications of switching provider before contract end
- [ ] Check if the contract includes **proactive monitoring** by the ISP or whether you only find out about faults when users complain

Section Score: _____ /10

4 Redundancy & Failover

A single internet connection is a single point of failure. Assess your resilience against connection loss.

- [ ] Confirm whether a **secondary internet connection** exists at each site and whether it uses a different ISP and technology
- [ ] Verify the secondary connection enters the building via a **different physical path** — not the same duct or cabinet as the primary
- [ ] Test **automatic failover** by disconnecting the primary connection and measuring how quickly traffic switches to the backup
- [ ] Confirm the **secondary connection bandwidth** is sufficient to maintain critical services during a primary outage
- [ ] Check whether **4G/5G backup** is available as a tertiary failover path for critical sites (ensure adequate signal strength)
- [ ] Verify that **DNS resolution** continues to work during a connection failover — test with external DNS queries
- [ ] Confirm that **VPN tunnels re-establish automatically** when traffic fails over to the secondary connection
- [ ] Document the **last failover test date** and schedule regular testing at least quarterly

Section Score: ____/10

5 Network Security at the Edge

Your internet connection is the entry point for most cyber threats. Verify your edge security is robust.

- [ ] A **business-grade firewall** is deployed at the internet edge with active threat intelligence subscriptions (not a consumer router)
- [ ] Firewall firmware is **current and on a scheduled update cycle** with change management procedures in place
- [ ] All **unnecessary inbound ports are blocked** — only explicitly required services are exposed to the internet
- [ ] Outbound traffic is **monitored and filtered** to detect data exfiltration, command-and-control traffic, and policy violations
- [ ] **Intrusion Detection/Prevention (IDS/IPS)** is enabled on the firewall with up-to-date signatures
- [ ] Remote access is secured via **VPN with multi-factor authentication** — no RDP or SSH exposed directly to the internet
- [ ] **DNS filtering** is configured to block access to known malicious domains, phishing sites, and inappropriate content
- [ ] The ISP-provided router is configured in **bridge or modem-only mode** to avoid double-NAT issues and hand security control to your firewall
- [ ] Regular **external vulnerability scans** verify no unintended services are exposed on your public IP addresses

Section Score: _____ /10

6 Business Continuity & Uptime

Assess how well your internet connectivity supports business continuity objectives and operational resilience.

- [ ] Internet connectivity is included in the **business continuity plan** with defined recovery procedures for total connection loss
- [ ] An **incident response procedure** exists for internet outages, including ISP escalation contacts and internal communication plans
- [ ] The business has quantified the **cost of internet downtime per hour** to justify investment in redundancy and better SLAs
- [ ] Critical cloud services have been identified and **alternative access methods** documented (e.g., mobile tethering, remote working)
- [ ] Staff can **work remotely** if the office internet fails — VPN access, cloud applications, and collaboration tools are accessible from home
- [ ] An **internet outage has been simulated** within the past 12 months to test the effectiveness of failover and continuity plans
- [ ] ISP **planned maintenance windows** are communicated in advance and scheduled outside business hours wherever possible
- [ ] Historical **uptime data** from the ISP and internal monitoring is reviewed quarterly to track reliability trends

Section Score: ____/10

7 Future-Proofing & Scalability

Assess whether your current internet infrastructure can support growth, new technologies, and evolving business needs.

- [ ] Current bandwidth utilisation trends have been **analysed over the past 12 months** to forecast future requirements
- [ ] The impact of planned **cloud migration, SaaS adoption, or remote working expansion** on bandwidth requirements has been assessed
- [ ] The availability of **higher-speed connections** (FTTP, leased line, or Ethernet) at your location has been investigated
- [ ] A **technology roadmap** includes internet connectivity upgrades aligned with business growth plans
- [ ] The potential for **SD-WAN deployment** has been evaluated to optimise traffic routing across multiple connections
- [ ] Emerging requirements for **IoT, AI, or real-time data** applications have been considered in bandwidth planning
- [ ] The current ISP can **scale bandwidth on demand** or within a reasonable timeframe without requiring a new circuit installation
- [ ] Budget has been allocated for **connectivity upgrades** in the next 12–24 months based on growth projections

Section Score: ____ /10

8 Audit Summary & Action Plan

#	AUDIT AREA	SCORE	PRIORITY
1	Current Connection Assessment	/ 10	H / M / L
2	Speed & Performance Testing	/ 10	H / M / L
3	ISP Contract Review	/ 10	H / M / L
4	Redundancy & Failover	/ 10	H / M / L
5	Network Security at the Edge	/ 10	H / M / L
6	Business Continuity & Uptime	/ 10	H / M / L
7	Future-Proofing & Scalability	/ 10	H / M / L
TOTAL SCORE		**/ 70**	

Score Interpretation

80–100: Excellent. Your IT setup is well-managed. Focus on continuous improvement and emerging threats.
60–79: Good foundation but gaps exist. Prioritise areas scoring below 6 and create an action plan.
Below 60: Significant gaps that put your business at risk. Consider an urgent review with an IT specialist.

Top 3 Priority Actions:

1. _____
2. _____
3. _____

Additional Notes

_____

_____

_____

_____

_____

_____

Audit completed by: _____ Date: _____ Next review due: _____