CLOUDSWITCHED

FREE RESOURCE — AUDIT CHECKLIST

IT Support Audit Checklist

Assess your current IT support setup against ten audit areas covering response times, hardware, software, network, security, backup, cloud, compliance, user experience and strategic planning. Score each area to identify gaps and prioritise improvements.

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

SERVICE DESK · CYBERSECURITY · BACKUP & DR · STRATEGY

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 IT team or your managed service provider. Tick every checkpoint that is **fully in place** — not partially, not "we're working on it", but in production 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** indicates a gap that should be addressed before it becomes an incident, an audit finding, or a board-level question. 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 everyday hygiene controls a competent IT support function should have running — ticketing and SLAs, asset and software management, network, cybersecurity, backup, cloud, compliance, user experience and strategic planning. It is not an ISO 27001 audit and it does not certify Cyber Essentials, but it is a fast way to surface the gaps that those formal regimes will pick up.

SCORING GUIDANCE

Award one point per checkpoint where you have evidence the control is in place — a configuration, a report, a policy, a screenshot, a contract. 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 Service Desk & Response Times** — ticketing, SLAs, escalation, out-of-hours cover.
- **02 Hardware & Device Management** — asset register, lifecycle, MDM, encryption.
- **03 Software & Licensing** — inventory, renewals, patching, shadow IT.
- **04 Network & Connectivity** — diagrams, monitoring, failover, VLANs, VPN/ZTNA.
- **05 Cybersecurity & Access Control** — MFA, EDR, email, leaver process.
- **06 Backup & Disaster Recovery** — 3-2-1, test restores, M365 backup.
- **07 Email & Cloud Services** — Conditional Access, DLP, sharing, admin.
- **08 Compliance & Documentation** — GDPR, breach response, Cyber Essentials.
- **09 User Experience & Satisfaction** — surveys, onboarding, training, self-service.
- **10 Strategic IT Planning** — roadmap, budget, vendor reviews.

01

Service Desk & Response Times

Your IT helpdesk is the front line of support. Evaluate whether tickets are being raised, tracked and resolved efficiently with clear communication to end users. Ask for the last three months of SLA reports as evidence.

- ☐ A **dedicated helpdesk system** is in place for logging and tracking all IT support requests *(not just email or phone)*.
- ☐ All support requests are assigned a **unique ticket number** and tracked from creation to resolution.
- ☐ **Response time targets** are defined and documented — e.g. P1 critical: 15 min, P2 high: 1 hour, P3 standard: 4 hours.
- ☐ Response time targets are **consistently met** and reported on monthly *(ask for the last 3 months of SLA reports)*.
- ☐ Users receive an **automatic acknowledgement** when a ticket is logged, with expected response time.
- ☐ There is a **clear escalation process** for unresolved or overdue tickets with defined time triggers.
- ☐ **Out-of-hours support** is available for critical issues, with a documented on-call process or emergency line.
- ☐ Users can **track the status** of their open tickets via a self-service portal or regular updates.

WHAT GOOD LOOKS LIKE

Every request lives in a ticketing system with a unique ID. Users get an automatic acknowledgement, then a real human update within the SLA window. Out-of-hours is documented — not "whoever picks up the phone".

SECTION 01 SCORE _____ / **10** *Aim for 8+. Below 6 = ticketing / SLA gap.*

02

Hardware & Device Management

Unmanaged devices are a security and cost risk. Check that all hardware is inventoried, maintained, and on a clear lifecycle replacement schedule. An asset register that lives in someone's head does not count.

- ☐ A **complete asset register** exists covering all PCs, laptops, monitors, printers and peripherals with serial numbers.
- ☐ Each device has a recorded **purchase date and warranty status** — expired warranties are flagged for replacement.
- ☐ A **hardware refresh cycle** is in place (typically 3–5 years) with a documented replacement schedule and budget line.
- ☐ All devices are **encrypted** (BitLocker, FileVault or equivalent) and can be remotely wiped if lost or stolen.
- ☐ **Mobile Device Management (MDM)** is in place for company phones and tablets *(e.g. Intune, Jamf)*.
- ☐ Spare equipment is available for **rapid swap-outs** to minimise downtime during hardware failures.
- ☐ Decommissioned devices are **securely wiped or destroyed** with documented chain of custody and a disposal certificate.

WATCH OUT FOR

"Bring your own device" arrangements where personal laptops handle company data with no MDM, no encryption enforcement and no leaver wipe. This is a common — and often unintentional — data breach vector.

SECTION 02 SCORE _____ / 10 *Aim for 8+. Below 6 = asset / lifecycle gap.*

03

Software & Licensing

Software sprawl and unlicensed applications create legal, security and cost risks. Every application should be authorised, licensed and up to date — with the paperwork to prove it if a vendor audit lands.

- ☐ A **software inventory** is maintained listing all applications, versions, licence types and renewal dates.
- ☐ All software is **properly licensed** — licence counts match installed instances *(audit-ready at all times)*.
- ☐ **Licence renewals** are tracked with at least 60 days advance notice to avoid lapses or auto-renewals at inflated prices.
- ☐ **Unused licences** are identified and reclaimed or cancelled to reduce costs *(e.g. departed staff accounts)*.
- ☐ Application **patching is automated** with a defined cycle — critical patches within 48 hours, standard within 14 days.
- ☐ Users cannot install **unauthorised software** without admin approval *(local admin rights are restricted)*.
- ☐ **SaaS applications** are inventoried and access is managed centrally *(no shadow IT)*.

SHADOW IT DETECTION

Pull the last three months of expense-card and direct-debit data and grep for SaaS domain names — you will almost always find subscriptions IT has never been told about.

SECTION 03 SCORE _____ / **10** *Aim for 8+. Below 6 = licence / shadow IT gap.*

04

Network & Connectivity

Your network is the backbone of everything. Check that it is properly documented, monitored and performing to meet business demands — and that you have a documented fallback when your primary connection fails.

- ☐ A **network diagram** exists showing all switches, routers, firewalls, access points and ISP connections.
- ☐ **Network monitoring** is active with alerts for downtime, high latency, packet loss and capacity issues.
- ☐ **Internet bandwidth** meets current demand and there is a documented plan for scaling if the business grows.
- ☐ A **secondary internet connection** or failover is in place for business continuity *(4G/5G backup or dual ISP)*.
- ☐ **WiFi coverage** is adequate across all working areas with no dead zones *(a site survey has been conducted)*.
- ☐ **VLANs** are configured to segment guest, IoT and corporate traffic for security and performance.
- ☐ **VPN or ZTNA** is available for secure remote access, with multi-factor authentication enforced.
- ☐ All network equipment **firmware is current** and on a scheduled update cycle.

SECTION 04 SCORE _____ / **10** *Aim for 8+. Below 6 = network / failover gap.*

05

Cybersecurity & Access Control

Security is not optional. Assess whether your organisation has the right protections in place to defend against modern threats — phishing, ransomware, credential stuffing, business email compromise.

- ☐ **Multi-Factor Authentication (MFA)** is enforced on all cloud services, email, VPN and admin accounts.
- ☐ A **password policy** is enforced — minimum 12 characters, complexity requirements and no password reuse.
- ☐ **Endpoint protection** is installed and centrally managed on all devices *(EDR or next-gen antivirus)*.
- ☐ **Email filtering** is configured with anti-phishing, anti-malware and safe links/attachments scanning.
- ☐ **SPF, DKIM and DMARC** records are configured for all company email domains to prevent spoofing.
- ☐ **User access reviews** are conducted at least quarterly — leavers are disabled within 24 hours of departure.
- ☐ **Admin access** is limited to authorised IT staff only, using separate admin accounts *(not day-to-day logins)*.
- ☐ **Security awareness training** is provided to all staff at least annually, covering phishing, social engineering and data handling.

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

06

Backup & Disaster Recovery

If your backups fail, your business is at risk. Verify that data is being backed up correctly, stored securely, and that recovery has been tested in the last 12 months — an untested backup is a guess, not a plan.

- ☐ A **documented backup policy** exists covering what is backed up, how often and where it is stored.
- ☐ The **3-2-1 rule** is followed — 3 copies, 2 different media types, 1 offsite or cloud copy.
- ☐ **Backup success/failure** is monitored daily with alerts for any failed jobs.
- ☐ **Test restores** are performed at least quarterly to verify data can actually be recovered.
- ☐ **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)** are defined and documented.
- ☐ **Microsoft 365 data** (email, SharePoint, OneDrive, Teams) is backed up by a third-party solution *(Microsoft does not back up your data)*.
- ☐ A **disaster recovery plan** exists and has been tested within the last 12 months.
- ☐ Backups are **encrypted** both in transit and at rest, with access restricted to authorised personnel.

COMMON GAP: MICROSOFT 365 BACKUP

Many organisations assume Microsoft backs up their email and files. It does not. Microsoft's retention policies are designed for short-term recovery, not long-term backup. A third-party solution (Veeam, Datto, Acronis) is essential against accidental deletion, ransomware and compliance demand.

SECTION 06 SCORE _____ / **10** *Aim for 8+. Below 6 = recovery is unproven.*

07

Email & Cloud Services

Cloud services are central to modern business. Ensure your Microsoft 365 or Google Workspace environment is properly configured, secured and managed — with a tight grip on who has admin rights.

- ☐ **Microsoft 365 or Google Workspace** is configured with appropriate licence tiers for each user role.
- ☐ **Conditional Access policies** are configured to restrict access by device, location and risk level.
- ☐ **Data Loss Prevention (DLP)** policies are in place to prevent sensitive data leaving the organisation.
- ☐ **Shared mailboxes and distribution lists** are regularly reviewed and updated as staff change roles.
- ☐ **Email retention policies** are configured to meet legal and compliance requirements.
- ☐ **SharePoint and OneDrive** permissions are audited to ensure no over-sharing of sensitive files.
- ☐ A **global admin audit** has been conducted — only 2–3 trusted accounts should have global admin rights.

GLOBAL ADMIN DISCIPLINE

The fastest path from a phishing click to a tenant takeover is a service account with global admin still using a shared password. Audit who holds the keys, separate admin accounts from daily accounts, and enforce hardware MFA on every privileged identity.

SECTION 07 SCORE _____ / **10** *Aim for 8+. Below 6 = tenant hygiene gap.*

08

Compliance & Documentation

Proper documentation protects you during audits, incidents and staff changes. Check that your IT environment is properly documented and compliant with UK-specific obligations including GDPR and ICO breach reporting.

- ☐ An **IT documentation repository** exists containing network diagrams, configurations, procedures and passwords.
- ☐ **Passwords and credentials** are stored in a secure password manager *(not spreadsheets or sticky notes)*.
- ☐ A **GDPR data processing register** is maintained listing all personal data held, its purpose and retention period.
- ☐ **Privacy policies and cookie notices** on the company website are accurate and up to date.
- ☐ A **data breach response plan** exists with steps for containment, notification (within 72 hours to the ICO) and recovery.
- ☐ **IT policies** are in place covering acceptable use, BYOD, remote working and data handling.
- ☐ **Cyber Essentials** certification is current *(mandatory for many UK government contracts and increasingly expected by customers)*.

WHY CYBER ESSENTIALS MATTERS

Cyber Essentials is a UK government-backed scheme that demonstrates your organisation meets a baseline of cybersecurity controls (firewalls, secure configuration, access control, malware protection, patch management). Certification costs from around £300 and protects against the most common cyber attacks.

SECTION 08 SCORE _____ / **10**

Aim for 8+. Below 6 = audit / regulator risk.

09

User Experience & Satisfaction

IT should empower your team, not frustrate them. Assess whether your users are well supported, trained and satisfied with the IT service they receive — the cheapest measure here is a short annual survey.

- ☐ **User satisfaction surveys** are conducted at least annually to gauge the quality of IT support.
- ☐ **Onboarding processes** for new starters are documented — equipment, accounts and training are ready on day one.
- ☐ **Offboarding processes** are documented — accounts disabled, equipment returned and data backed up on the last day.
- ☐ **Self-service resources** are available — knowledge base, FAQs or guides for common issues *(password resets, VPN setup)*.
- ☐ **Training** is provided when new systems or tools are rolled out, not just a link to a help article.
- ☐ **Recurring issues** are tracked and root-cause fixes are prioritised over repeated quick fixes.
- ☐ Users know **how to report IT issues** and the expected response process *(not ad-hoc messages to IT staff)*.

ONBOARDING TELLS YOU EVERYTHING

A repeatable, day-one-ready onboarding process is the single best indicator of a mature IT function. If new starters wait three days for a laptop and a Teams login, the upstream processes are broken.

SECTION 09 SCORE _____ / **10** *Aim for 8+. Below 6 = service quality issue.*

10

Strategic IT Planning

IT should be a strategic enabler, not just a cost centre. Check whether there is a forward-looking plan for technology investment and alignment with business goals — reviewed at least annually with senior leadership.

- ☐ An **IT strategy or technology roadmap** exists and is reviewed at least annually with senior leadership.
- ☐ There is a defined **IT budget** covering BAU costs, planned investments and a contingency for unexpected needs.
- ☐ **Technology refresh cycles** are planned and budgeted — hardware, software and infrastructure have defined lifecycles.
- ☐ **Cloud migration** opportunities are evaluated — remaining on-premise systems have a documented justification.
- ☐ Regular **IT review meetings** are held between IT leadership (or your MSP) and business stakeholders.
- ☐ **Risk and capacity planning** considers business growth, new office locations and remote workforce needs.
- ☐ An **IT vendor review** is conducted annually to assess value, performance and contract terms.

STRATEGIC VS REACTIVE

The clearest signal of a strategic IT function is a written 18-month roadmap that maps technology change to business outcomes — not a backlog of tickets. If your IT conversation is dominated by yesterday's incidents, you do not have a strategy, you have a queue.

SECTION 10 SCORE _____ / **10** *Aim for 8+. Below 6 = no forward plan.*

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	Service Desk & Response Times	_____ / 10	☐ H ☐ M ☐ L
02	Hardware & Device Management	_____ / 10	☐ H ☐ M ☐ L
03	Software & Licensing	_____ / 10	☐ H ☐ M ☐ L
04	Network & Connectivity	_____ / 10	☐ H ☐ M ☐ L
05	Cybersecurity & Access Control	_____ / 10	☐ H ☐ M ☐ L
06	Backup & Disaster Recovery	_____ / 10	☐ H ☐ M ☐ L
07	Email & Cloud Services	_____ / 10	☐ H ☐ M ☐ L
08	Compliance & Documentation	_____ / 10	☐ H ☐ M ☐ L
09	User Experience & Satisfaction	_____ / 10	☐ H ☐ M ☐ L
10	Strategic IT Planning	_____ / 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 IT assessments for UK SMEs — helpdesk, security, backup, cloud and strategic planning, with fixed-price remediation plans.

info@cloudswitched.com

cloudswitched.com/services/it-support

CLOUDSWITCHED

IT SUPPORT & PROJECT SERVICES

info@cloudswitched.com

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