# IT Support Audit Checklist

Assess your current IT support setup with this comprehensive audit covering response times, service desk operations, security posture, backup systems, and strategic planning. Score each area to identify gaps and prioritise improvements.

| 10 | 75+ | Score | Free |
|---|---|---|---|
| AUDIT AREAS COVERED | AUDIT 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 provider. Tick items that are fully in place. Score each section out of 10 based on how many items you can confidently tick. A score below 6 in any area indicates a gap that should be addressed. Use the notes section at the end to capture action items and priorities.

## 1 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.

- [ ] 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 **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

**Section Score:** _____ /10

## 2 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.

- [ ] 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
- [ ] All devices are **encrypted** (BitLocker 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

**Section Score:** _____ /10

## 3 Software & Licensing

Software sprawl and unlicensed applications create legal, security, and cost risks. Ensure every application is authorised, licenced, and up to date.

- [ ] A **software inventory** is maintained listing all applications, versions, licence types, and renewal dates
- [ ] All software is **properly licenced** — 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)

**Section Score:** ____/10

## 4 Network & Connectivity

Your network is the backbone of everything. Check that it is properly documented, monitored, and performing to meet business demands.

- [ ] 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 Score:** ____/10

## 5 Cybersecurity & Access Control

Security is not optional. Assess whether your organisation has the right protections in place to defend against modern threats.

- [ ] **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 Score:** ____/10

## 6 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.

- [ ] 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 backup solution (such as Veeam, Datto, or Acronis) is essential to protect against accidental deletion, ransomware, and compliance requirements.

**Section Score:** _____ /10

## 7 Email & Cloud Services

Cloud services are central to modern business. Ensure your Microsoft 365 or Google Workspace environment is properly configured, secured, and managed.

- [ ] **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

**Section Score:** _____ /10

## 8 Compliance & Documentation

Proper documentation protects you during audits, incidents, and staff changes. Check that your IT environment is properly documented and compliant.

- [ ] 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 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 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. It covers firewalls, secure configuration, access control, malware protection, and patch management. Certification costs as little as £300 and can protect your business against 80% of common cyber attacks.

**Section Score:** _____/10

## 9 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.

- [ ] **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 relying on ad-hoc messages to IT staff)

**Section Score:** _____/10

## 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.

- [ ] 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

**Section Score:** _____/10

## Σ Audit Score Summary

| # | AUDIT AREA | SCORE | PRIORITY |
|---|---|---|---|
| 1 | Service Desk & Response Times | / 10 | H / M / L |
| 2 | Hardware & Device Management | / 10 | H / M / L |
| 3 | Software & Licensing | / 10 | H / M / L |
| 4 | Network & Connectivity | / 10 | H / M / L |
| 5 | Cybersecurity & Access Control | / 10 | H / M / L |
| 6 | Backup & Disaster Recovery | / 10 | H / M / L |
| 7 | Email & Cloud Services | / 10 | H / M / L |
| 8 | Compliance & Documentation | / 10 | H / M / L |
| 9 | User Experience & Satisfaction | / 10 | H / M / L |
| 10 | Strategic IT Planning | / 10 | H / M / L |
| **TOTAL SCORE** | | **/ 100** | |

**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.

## ! Action Items & Notes

**Top 3 Priority Actions:**

1

2

3

**Additional Notes**

**Need Help With Your IT Audit?**
Our team can conduct a full IT assessment and help you address any gaps identified in this checklist.

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



Audit completed by: Date: Next review due:

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