telappliant

SME Cybersecurity & Infrastructure Readiness Checklist

A step by step framework to audit your own IT, security and supplier setup. Aligned to UK Cyber Essentials and NCSC guidance. Tick each item you can confirm today; unticked items are your priority list.

Last reviewed 28 September 2026. Telappliant.

STEP 1

Governance and ownership

Why it matters: Security fails quietly when nobody owns it. Clear ownership means decisions get made and risks get reviewed.

Reference: NCSC Small Business Guide

- [ ] A named person is accountable for IT and cyber security
- [ ] Leadership reviews technology risk at least once a year
- [ ] You have a written list of IT suppliers and what each one is responsible for
- [ ] Staff know who to report a suspicious email or incident to
- [ ] Key policies (acceptable use, passwords, remote working) are written and shared

STEP 2

Devices and asset inventory

Why it matters: You cannot protect what you do not know you have. An up to date inventory is the base of every audit.

Reference: Cyber Essentials: Secure configuration

- [ ] You keep a current list of laptops, desktops, phones and servers
- [ ] Every device runs a supported operating system
- [ ] Security updates install automatically within 14 days of release
- [ ] Laptops and phones are encrypted
- [ ] Default passwords and unused software are removed from new devices
- [ ] Lost or stolen devices can be locked or wiped remotely

STEP 3

Identity, passwords and MFA

Why it matters: Stolen passwords are the most common way attackers get in. Multi factor authentication blocks most of these attempts.

Reference: Cyber Essentials: User access control

- [ ] Multi factor authentication is on for email and all cloud services
- [ ] Every person has their own account, with no shared logins
- [ ] Admin accounts are separate and used only for admin tasks
- [ ] Leavers lose access on their last day
- [ ] A password manager is available to staff
- [ ] Access rights are reviewed at least every six months

STEP 4

Backup and recovery

Why it matters: Backups are your last line of defence against ransomware, mistakes and hardware failure, but only if they restore.

Reference: NCSC Small Business Guide: Backing up your data

- [ ] Critical data, including Microsoft 365 or Google Workspace, is backed up
- [ ] At least one backup copy is kept offline or separate from your main systems
- [ ] A test restore has been completed in the last six months
- [ ] You know how long you could operate without key systems
- [ ] Backup failures raise an alert that someone acts on

STEP 5

Network, firewall and Wi-Fi

Why it matters: Your network is the front door. A misconfigured firewall or open guest Wi-Fi can expose every device behind it.

Reference: Cyber Essentials: Firewalls

- [ ] A firewall protects your office and remote workers
- [ ] Firewall and router admin passwords have been changed from the defaults
- [ ] Guest Wi-Fi is separated from the business network
- [ ] Remote access uses a VPN or secure cloud access, not open ports
- [ ] Your broadband and phone lines have a backup or failover plan

STEP 6

Email and phishing protection

Why it matters: Most attacks start with an email. Good filtering and aware staff stop them before damage is done.

Reference: NCSC Phishing guidance

- [ ] Email filtering blocks spam, malware and impersonation attempts
- [ ] SPF, DKIM and DMARC records are set up for your domain
- [ ] Staff complete short phishing awareness training each year
- [ ] Payment or bank detail changes are always confirmed by phone
- [ ] Anti malware protection runs on every device

STEP 7

Cloud, licences and supplier spend

Why it matters: Unused licences and overlapping contracts waste budget that could fund real security improvements.

Reference: Telappliant supplier spend review

- [ ] You know every software subscription the business pays for
- [ ] Licences for leavers are removed or reassigned
- [ ] Contract renewal dates for IT, telecoms and connectivity are tracked
- [ ] You have compared supplier costs in the last two years
- [ ] Cloud services have security settings reviewed, not left on defaults

STEP 8

Incident response and continuity

Why it matters: A short, practised plan turns a crisis into an inconvenience and helps you meet your legal duties.

Reference: NCSC Response and recovery guidance

- [ ] A simple incident response plan is written down
- [ ] Contact details for IT support, insurers and key suppliers are stored offline
- [ ] You know when to report a breach to the ICO (within 72 hours)
- [ ] You have considered cyber insurance
- [ ] The plan has been talked through or tested in the last year

Next step

Want a specialist to review your answers and help you prioritise? Book a free, no obligation technology review at itaudit.telappliant.co.uk or call 0345 557 6100.