The Definitive South East London SME Cyber Security Audit 2026

Brought to you by Simply Solutions *Enterprise Expertise for South East London SMEs | No Jargon. No Judgment. Just Solutions.*

Overview

This audit is a comprehensive assessment based on the **NCSC Small Business Guide**, **Cyber Essentials v3.3**, and **ISO 27001** principles, updated for the 2026 threat landscape.

How to use: Work through each section. Items marked with 🚩 are **Critical Priorities**—if these aren't checked, your business is at immediate risk.

1. Firewalls, Network & The "New Perimeter"

Your first line of defense against the outside world.

- [ ] 🚩 **Active Hardware Firewall:** A business-grade firewall is installed and active on your main internet gateway.
- [ ] 🚩 **Password Security:** All default administrative passwords on routers and firewalls have been changed to complex, unique strings.
- [ ] **Documented Ruleset:** All firewall "allow" and "deny" rules are documented and reviewed at least every 6 months.
- [ ] **Disabled Remote Management:** Remote administration of the router/firewall via the internet is disabled unless using a secure ZTNA/VPN.
- [ ] **VLAN Segmentation:** Your Guest Wi-Fi and IoT devices (smart bulbs, cameras) are on a separate network from your business data.
- [ ] **Intrusion Prevention (IPS):** Active scanning is enabled to block known malicious traffic patterns automatically.

- [ ] **Inbound Port Audit:** All unnecessary inbound ports (e.g., RDP Port 3389) are closed.

2. Secure Configuration & Hardware Hardening

Reducing the "attack surface" of your office devices.

- [ ] 🚩 **Bloatware Removal:** All unnecessary pre-installed software and "trialware" has been removed from new laptops and PCs.
- [ ] 🚩 **Screen Lock Policy:** All devices are configured to auto-lock after a maximum of 5 minutes of inactivity.
- [ ] **Disabled Auto-Run:** Auto-run and Auto-play features are disabled for all USB and external drives.
- [ ] **BIOS/UEFI Passwords:** Administrative passwords are set at the hardware level to prevent unauthorized booting from USBs.
- [ ] **Approved Software Only:** Users are restricted from installing unauthorized software without administrative approval.
- [ ] **Hardware Inventory:** A full asset register exists, tracking the serial number, user, and location of every company device.
- [ ] **Secure Disposal:** A formal process is in place for the cryptographic wiping of hard drives before recycling or selling old hardware.

3. Access Control & User Management

Ensuring the right people have the right access—and nothing more.

- [ ] 🚩 **Unique Accounts:** Every single staff member has their own unique login; sharing passwords or "Office Admin" accounts is strictly forbidden.
- [ ] 🚩 **Standard User Rights:** Daily work is performed on "Standard" accounts; "Administrator" accounts are used *only* for system changes.
- [ ] **The 5-Minute Offboarding:** A process exists to revoke *all* access (Email, CRM, Building) within 5 minutes of an employee's departure.
- [ ] **Quarterly Privilege Review:** Management reviews who has access to sensitive folders (HR, Finance) every 90 days.
- [ ] **Just-In-Time (JIT) Access:** Admin rights are only granted temporarily when needed, then automatically revoked.

4. Malware Protection & EDR (Endpoint Detection)

Defending against viruses, ransomware, and AI-driven malicious code.

- [ ] 🚩 **Active Real-Time Scanning:** Anti-malware software is active and scanning files in real-time on every device.
- [ ] 🚩 **Daily Updates:** Signature definitions update automatically at least once every 24 hours.
- [ ] **Behavioral Analysis (EDR):** Your security software looks for "strange behavior" (like 100 files being renamed at once) rather than just known viruses.
- [ ] **Email Attachment Scanning:** All incoming attachments are "sandboxed" (opened in a

safe environment) before reaching the user.
- [ ] **USB Lockdown:** The use of unencrypted or unauthorized USB sticks is disabled across the company.
- [ ] **Tamper Protection:** Users are prevented from disabling or uninstalling security software without an admin code.

5. Software Updates & Patch Management

Closing the "open windows" in your software before hackers climb through.

- [ ] 🚩 **The 14-Day Rule:** All "Critical" and "High" security patches are applied to all devices within 14 days of release.
- [ ] 🚩 **Unsupported Software Audit:** No devices are running "End of Life" software (e.g., Windows 7/8, old versions of Office).
- [ ] **Automated OS Updates:** Windows, macOS, and Linux devices are set to download and install updates automatically.
- [ ] **Third-Party App Patching:** Non-Microsoft apps (Chrome, Adobe, Zoom) are included in the regular patching cycle.
- [ ] **Firmware Updates:** Router, Printer, and Switch firmware is checked and updated quarterly.

6. Data Backup, Recovery & Residency

Your ultimate insurance policy against total business failure.

- [ ] 🚩 **The 3-2-1-1-0 Strategy:**
  - [ ] 3 Copies of data
  - [ ] 2 Different media types
  - [ ] 1 Offsite copy
  - [ ] 1 **Air-Gapped/Immutable** copy (cannot be deleted/changed)
  - [ ] 0 Errors (verified daily)
- [ ] 🚩 **Restoration Testing:** A full data restore is successfully tested and documented at least every 6 months.
- [ ] **Cloud-to-Cloud Backup:** Your Microsoft 365 or Google Workspace data is backed up to a *separate* provider.
- [ ] **Encryption at Rest:** Backups are encrypted so that stolen backup drives or cloud accounts are useless to thieves.
- [ ] **Data Residency Compliance:** You have confirmed that sensitive client data is stored in UK-based data centers (or GDPR-compliant regions).

7. Password, Identity & Biometrics

Strengthening the weakest link in the security chain.

- [ ] 🚩 **Multi-Factor Authentication (MFA):** MFA is active on *every* cloud service, without exception.
- [ ] 🚩 **Password Length:** Your company policy requires a minimum of 12-14 characters

for all passwords.
- [ ] **Password Manager:** Every staff member is provided with a secure password manager (e.g., Bitwarden, 1Password) to prevent password reuse.
- [ ] **Passkey Adoption:** High-risk accounts have migrated to Biometric Passkeys (FaceID/Fingerprint) or FIDO2 hardware keys.
- [ ] **Account Lockout:** Accounts are automatically locked for 30 minutes after 5 failed login attempts.

8. Email, Phishing & AI-Deepfake Defense

Email is the #1 attack vector for 90% of SME breaches.

- [ ] 🚩 **Domain Authentication:** SPF, DKIM, and DMARC are correctly configured for your email domain to prevent spoofing.
- [ ] 🚩 **Deepfake Verification Protocol:** A strict "verbal verification" policy is in place for any bank transfer or sensitive data request, regardless of "who" asks via email/voice note.
- [ ] **Spam/Phishing Filtering:** An advanced cloud filter is active to block malicious links before they reach the inbox.
- [ ] **External Mail Flagging:** All emails arriving from outside the organization are clearly marked with an [EXTERNAL] banner.
- [ ] **Dangerous File Blocking:** Files like .exe, .js, and .zip are blocked or heavily scrutinized by the email gateway.

9. Physical, Device & PSTN Security

Securing the tangible assets of your South East London office.

- [ ] 🚩 **Full-Disk Encryption (BitLocker/FileVault):** All laptops are encrypted so that data is unreadable if the device is stolen.
- [ ] 🚩 **Remote Wipe:** You have the ability to "nuke" any lost or stolen device remotely via MDM (Mobile Device Management).
- [ ] **PSTN/ISDN Audit:** All legacy hardware (Alarms, Elevator phones, Fax machines) has been identified for the 2027 PSTN switch-off.
- [ ] **Secure Hardware Storage:** Servers and network switches are kept in a locked room or rack with restricted access.
- [ ] **CCTV & Physical Alarms:** The physical office is secured with monitored alarms and clear CCTV coverage.

10. Staff Awareness & AI Governance

Building a culture of security.

- [ ] 🚩 **Induction Training:** Every new hire receives 30 minutes of cyber security training before receiving their login details.
- [ ] **Annual Refresher:** All staff undergo formal security awareness training at least once a year.
- [ ] **AI Acceptable Use Policy:** A signed document exists stating which company data is

strictly forbidden from being put into public AI tools.

- [ ] **Simulated Phishing:** The company conducts "friendly" phishing tests twice a year to identify staff who need extra training.
- [ ] **Incident Reporting:** Every employee knows exactly who to call (and how) the moment they think they've clicked a bad link.

📈 Your Resilience Score

Total Items Checked: _____ / 72

Critical (🚩) Items Checked: _____ / 22

Score	Rating	Action Required
60-72	**Excellent**	You are "Cyber Essentials Plus" ready. Maintain and document.
45-59	**Good**	Solid foundations, but you have gaps that professional hackers will exploit.
30-44	**Vulnerable**	You have significant weaknesses. Prioritize all 🚩 items immediately.
Under 30	**Critical Risk**	Your business is statistically likely to suffer a breach within 12 months.

🆘 Need an Expert Review?

Simply Solutions brings **30 years of Silver Circle expertise** to your high street. We don't just find the gaps; we close them.

Contact the Simply Solutions Team:
📍 Serving Bromley, Greenwich, Lewisham & Beyond
🌐 simplysolutions.tech

✉️ info@simplysolutions.tech

No jargon. No judgment. Just solutions.