CLOUDSWITCHED

FREE RESOURCE — ASSESSMENT CHECKLIST

Cybersecurity Assessment Checklist

A multi-domain self-assessment for UK SMEs covering identity, endpoint, network, data, application, email, vulnerability, backup, monitoring and governance controls. Score each domain, set a maturity rating, assign an owner and a target date — and find the gaps an attacker, an insurer, or a Cyber Essentials Plus assessor will hit first.

10	80+	1-5	Fillable
CONTROL DOMAINS COVERED	CONTROL CHECKS TO TICK	MATURITY RATING PER DOMAIN	TICK & TYPE IN ANY VIEWER

IDENTITY · ENDPOINT · DATA · CLOUD · GOVERNANCE

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this checklist

Work through the ten domains with whoever owns IT, security and risk in your organisation — in-house, MSP, vCISO, or all three. Tick every checkpoint that is **fully in place** with evidence: a config, a screenshot, a policy, a SIEM rule, a contract, a scan report. Half-measures and "on the roadmap" do not score.

For each domain, award a **score out of 10** based on how many checkpoints you can tick, then set a **maturity rating 1-5** using the CMMI-style scale below. Anything scoring below 6 — or sitting at maturity 1-2 — is the kind of gap an attacker, an insurer, or a Cyber Essentials Plus assessor will land on. This is an **interactive PDF**: tick the boxes and type your scores, owners, target dates and notes directly in any modern PDF viewer.

WHAT THIS CHECKLIST IS

A multi-domain cybersecurity self-assessment for UK SMEs spanning identity & access, endpoint, network, data, application & cloud, email & phishing, vulnerability & patch, backup & recovery, monitoring & incident response, and governance, risk & compliance. It maps to the controls Cyber Essentials, ISO 27001, NIST CSF and most UK cyber-insurance questionnaires assume you are running — without being any one of those audits.

MATURITY RATING — 1 TO 5

1 Initial — ad-hoc, no documentation. **2 Managed** — repeatable, undocumented. **3 Defined** — documented and consistently applied. **4 Quantified** — measured, with metrics and KPIs. **5 Optimised** — continuously improved with formal review. Aim for 3+ across every domain; 4+ on identity, endpoint and incident response.

The ten domains

- **01 Identity & Access Management** — MFA, conditional access, privilege, joiner/mover/leaver.
- **02 Endpoint Security & EDR** — EDR/XDR, disk encryption, MDM, application control.
- **03 Network Security & Perimeter** — firewall, segmentation, WiFi, remote access, NAC.
- **04 Data Protection & Encryption** — classification, DLP, encryption, retention, GDPR.
- **05 Application & Cloud Security** — SaaS posture, IaC, SBOM, secrets, web app firewall.
- **06 Email & Phishing Defence** — SEG, DMARC, awareness training, BEC controls.
- **07 Vulnerability & Patch Management** — scans, patch SLAs, EOL, penetration testing.
- **08 Backup & Recovery** — 3-2-1-1-0, immutability, restore testing, BCP / DR.
- **09 Security Monitoring & Incident Response** — SIEM/XDR, IRP, tabletop, retainer, ICO.
- **10 Governance, Risk & Compliance** — policies, risk register, training, supplier assurance.

01

Identity & Access Management

Identity is the new perimeter and the most-attacked control in every modern intrusion. Audit the basics — MFA on everyone, conditional access on every app, privileged separation, and a working joiner/mover/leaver process tied to HR.

- ☐ **MFA is enforced on 100% of user accounts** — staff, contractors, admin, service principals — with phishing-resistant methods where possible.
- ☐ **Conditional Access policies** gate every cloud app on device compliance, location and sign-in risk — not just password + MFA.
- ☐ **Privileged identities are separated** from day-to-day accounts (no admin@ doing email or browsing) and use PAWs or jump hosts.
- ☐ **Joiner / mover / leaver** is automated from HR; access is provisioned, role-changed and removed within 24 hours of event.
- ☐ **Privileged access is reviewed quarterly**; orphaned admin rights and dormant accounts are revoked with sign-off.
- ☐ **Password / passphrase policy** follows NCSC guidance: length over rotation, breached-password screening, no forced expiry without cause.
- ☐ **SSO covers all SaaS** in scope; shadow-IT logins (local app passwords) are inventoried and being retired.
- ☐ **Privileged Identity Management (PIM)** or equivalent enforces just-in-time, time-bound elevation for admin roles.

WHAT GOOD LOOKS LIKE

Every login goes through SSO with phishing-resistant MFA. A leaver is locked out before they reach the carpark. Admin elevation is a 4-hour PIM activation with a ticket, not a permanent role. Conditional Access blocks legacy auth and risky sign-ins automatically.

DOMAIN 01 SCORE _____ / **10** *Aim for 9+. Below 6 = identity is your weakest link.*

02

Endpoint Security & EDR

Every laptop, desktop, server and mobile is a foothold. Modern endpoint security is not anti-virus — it is EDR with behavioural detection, full-disk encryption, MDM, application control, and a clean view of what is on the estate.

- ☐ **EDR or XDR** (Defender for Endpoint, CrowdStrike, SentinelOne or equivalent) is deployed on 100% of endpoints and servers, with central reporting.
- ☐ **EDR is in block mode**, not detect-only; tamper protection is on; the agent health dashboard is reviewed weekly.
- ☐ **Disk encryption** (BitLocker / FileVault) is enforced and recovery keys escrow to Azure AD / Intune / MDM.
- ☐ **MDM** (Intune, Jamf, Kandji) manages every corporate device; personal BYOD is gated by app-protection policy or denied.
- ☐ **Application control** (AppLocker, WDAC, Smart App Control or equivalent) blocks unsigned executables in user-writable paths.
- ☐ **Local admin rights are removed** from standard users; privileged tasks use LAPS or a privilege-elevation product with ticketing.
- ☐ **USB / removable media policy** is enforced (block by default, allow by exception, write-protected if allowed).
- ☐ **Asset inventory** reconciles MDM, EDR, AD and procurement; unmanaged devices are flagged and remediated within 7 days.

THE UNMANAGED ENDPOINT

The riskiest device in any SME is the one nobody knows about — a leaver's laptop, a contractor BYOD, a server in a closet someone forgot to enrol. Reconcile your inventories monthly. If EDR coverage is under 98%, you do not have EDR — you have a partial deployment.

DOMAIN 02 SCORE _____ / **10** *Aim for 9+. Below 6 = endpoint blind spots.*

03

Network Security & Perimeter

The network still matters — even in a cloud-first SME. Verify the basics across firewall, segmentation, wireless, remote access and NAC, with central management and modern protocols.

- ☐ **Next-generation firewall** with IDS/IPS in blocking mode is deployed at every internet boundary; rules reviewed quarterly with change tickets.
- ☐ **Default-deny outbound policy** with an allow-list of business destinations and ports — not wide-open egress.
- ☐ **Network segmentation** separates guest, IoT, server, OT and corporate VLANs, enforced by firewall ACLs, not just L3 routing.
- ☐ **Wireless uses WPA3 (or WPA2-Enterprise)** with 802.1X for corporate SSIDs; guest is PSK-rotated and isolated.
- ☐ **Remote access via VPN or ZTNA** requires MFA and device-posture checks (compliant, encrypted, EDR healthy).
- ☐ **802.1X port-based authentication** is enforced on wired and wireless corporate ports; unknown devices land in a quarantine VLAN.
- ☐ **Network device hardening** applied: no default credentials, SSH/HTTPS only, SNMPv3, centralised auth (TACACS+/RADIUS) with MFA.
- ☐ **DNS filtering / Protective DNS** (NCSC PDNS, Cisco Umbrella or equivalent) blocks known C2 and phishing domains.

DEFENCE IN DEPTH, NOT PERIMETER ONLY

Modern attacks bypass the perimeter via a phished credential or a SaaS token, then move laterally inside a flat network. Segmentation, 802.1X and outbound default-deny are what limit blast radius — treat them as load-bearing, not optional.

DOMAIN 03 SCORE _____ / **10** *Aim for 8+. Below 6 = perimeter and lateral-movement risk.*

04

Data Protection & Encryption

Data protection is what survives the perimeter being breached. Know where your sensitive data lives, classify it, encrypt it everywhere, and have a working retention and deletion regime that is consistent with UK GDPR and your sector regulations.

- ☐ **Data classification scheme** exists (Public / Internal / Confidential / Restricted) and is applied via labels or DLP rules in M365 / Google Workspace.
- ☐ **Data inventory** records where Personal, Special Category, financial and IP data lives — SaaS, file shares, databases, backups.
- ☐ **Encryption in transit**: TLS 1.2+ everywhere; TLS 1.0/1.1 and SSL disabled; modern ciphers only (AES-GCM, ChaCha20).
- ☐ **Encryption at rest**: endpoints, servers, SAN/NAS, database backups and SaaS data are encrypted with documented key management.
- ☐ **Data Loss Prevention (DLP)** rules block or quarantine outbound sensitive data over email, browser uploads and removable media.
- ☐ **Retention & deletion schedules** are defined per data category and enforced — not just documented in a policy nobody applies.
- ☐ **UK GDPR alignment**: RoPA maintained, lawful bases documented, DPA / SCCs in place with processors, subject-rights workflow tested.
- ☐ **Secure data disposal** (cryptographic erasure, certified destruction) is contracted for retired drives, devices and media.

WATCH OUT FOR — ICO 72-HOUR REPORTING

Under UK GDPR a personal-data breach “likely to result in risk” must be reported to the ICO within 72 hours. If your data inventory and incident playbook cannot answer “whose data, how much, what categories?” inside an hour, the clock will beat you.

DOMAIN 04 SCORE _____ / **10** *Aim for 8+. Below 6 = data exposure and ICO risk.*

05

Application & Cloud Security

Most SMEs are now SaaS-first — M365, Google Workspace, Salesforce, dozens of line-of-business apps. The attack surface is your tenant configuration, your OAuth grants and your developer pipeline, not the rack in the cupboard.

- ☐ **SaaS security posture management** covers M365 / Google Workspace / key SaaS tenants — baseline configs, secure-score, drift alerts.
- ☐ **OAuth consent grants** are governed: admin consent for risky scopes, third-party app inventory and quarterly review.
- ☐ **Cloud Security Posture Management (CSPM)** or equivalent monitors Azure / AWS / GCP for misconfigurations and exposed assets.
- ☐ **Secrets management** uses a vault (Azure Key Vault, AWS Secrets Manager, HashiCorp); no hard-coded secrets in repos or CI logs.
- ☐ **Secure SDLC**: code review, SAST / SCA in CI, container/IaC scanning, dependency updates tracked, SBOM produced for critical apps.
- ☐ **Web Application Firewall (WAF)** protects public web apps; rules tuned; bot management enabled for high-value endpoints.
- ☐ **Public cloud storage** (S3, Blob, GCS) defaults to private; public-bucket alerts fire and are remediated within 24 hours.
- ☐ **Shadow IT** is discovered via CASB / SaaS-discovery; unsanctioned apps are blocked, sanctioned, or risk-accepted with an owner.

THE OAUTH BACK DOOR

A phished user who clicks “Accept” on a malicious OAuth app gives the attacker persistent mailbox / Drive access that survives password resets and MFA. Lock down user consent, alert on risky grants, and review the third-party app inventory quarterly.

DOMAIN 05 SCORE _____ / **10** *Aim for 8+. Below 6 = SaaS / cloud posture gaps.*

06

Email & Phishing Defence

Over 90% of intrusions start with email. Verify your secure email gateway, your authentication records (SPF / DKIM / DMARC), your awareness training, and the controls that catch a Business Email Compromise before it costs you six figures.

- ☐ **Secure Email Gateway (SEG)** or built-in Defender / Google equivalent is configured with anti-phishing, anti-spoofing, attachment sandboxing and safe-link rewriting.
- ☐ **DMARC at p=reject** on every sending domain, with SPF aligned, DKIM signing on, and BIMI optional for brand protection.
- ☐ **External sender banner / warning** is on; impersonation protection covers VIPs and finance roles.
- ☐ **Phishing awareness training** is mandatory at induction and at least annually; metrics reviewed by leadership.
- ☐ **Simulated phishing** runs at least quarterly with reporting; click-rate and report-rate trended over time.
- ☐ **Report-phish button** is deployed in Outlook / Gmail; reported messages are triaged with an SLA.
- ☐ **Wire-transfer / supplier-change process** requires out-of-band verification (callback to known number) before any payment or bank-detail change.
- ☐ **Mailbox forwarding rules** are alerted on creation; auto-forward to external domains is blocked by tenant policy.

BEC — THE SILENT LOSS

Business Email Compromise is now the highest-loss attack type for UK SMEs — fewer headlines than ransomware, but the cheques are larger. The defence is procedural: a callback rule on every supplier-change and every payment over a threshold, with no exceptions for “the boss is in a hurry”.

DOMAIN 06 SCORE _____ / **10** *Aim for 9+. Below 6 = phishing & BEC exposure.*

07

Vulnerability & Patch Management

Vulnerability management is the unglamorous baseline that catches the threats every other control assumes are gone. Audit your scan cadence, your patch SLAs, your EOL register and the date of your last penetration test.

- ☐ **Authenticated vulnerability scans** run at least weekly across endpoints, servers, network gear and containers.
- ☐ **External attack-surface scans** run continuously; new exposed services trigger an alert and a ticket.
- ☐ **Patch SLAs** defined and met: critical 14 days, high 30 days, medium 90 days (Cyber Essentials v3.3 / CIS aligned).
- ☐ **Endpoint patching is automated** via Intune / WSUS / Jamf / MDM with compliance reporting and non-compliance alerts.
- ☐ **Firmware and network device updates** are on a managed cycle with documented rollback plans.
- ☐ **End-of-life software inventory** is maintained; replacement date and budget assigned, with formal risk-acceptance signature.
- ☐ **Exception register** tracks every unpatched system with a compensating control, an owner and a review date.
- ☐ **Annual penetration test** (external and internal) is commissioned by a CREST / CHECK firm; findings tracked to closure with retest.

PATCH SLA = CONTRACT

Cyber Essentials v3.3 and most UK cyber-insurance policies now require high / critical patches within 14 days of vendor release. The day a known-exploited CVE is published, the SLA clock starts — with or without a maintenance window.

DOMAIN 07 SCORE _____ / **10** *Aim for 8+. Below 6 = patch debt is critical.*

08

Backup & Recovery

Backup is your last line against ransomware, accidental deletion, malicious insider, and SaaS provider failure. Audit against the 3-2-1-1-0 model and the question that matters: when did you last successfully restore the data you actually need?

- ☐ **3-2-1-1-0 strategy**: 3 copies, 2 media, 1 offsite, 1 immutable / air-gapped, 0 errors on the last restore test.
- ☐ **Immutable backups** (object-lock, WORM, append-only) protect at least one full copy from ransomware deletion.
- ☐ **SaaS data is backed up independently** (M365 / Google Workspace / Salesforce) — the provider's redundancy is not your backup.
- ☐ **Backup job success** is monitored daily; failed jobs trigger a ticket and an SLA, not a silent log entry.
- ☐ **Restore testing** is performed at least quarterly on a sample of systems; results documented with timings.
- ☐ **Recovery Time / Point Objectives (RTO / RPO)** are defined per system tier, approved by the business and met in test.
- ☐ **Disaster Recovery plan** exists with named roles, dependencies, runbooks and a full DR exercise within the last 12 months.
- ☐ **Business Continuity Plan** covers people, premises, comms, suppliers and finance — not just the IT stack.

THE RESTORE TEST IS THE BACKUP

A backup that has never been restored is a hope. Pick one critical workload this quarter, restore it to an isolated environment, time the restore, and compare to the RTO. If you have not done this in the last 90 days, you do not know whether your backups work.

DOMAIN 08 SCORE _____ / **10** *Aim for 9+. Below 6 = ransomware-survival risk.*

09

Security Monitoring & Incident Response

You will face an incident; the question is whether you can detect and respond in hours, not days. Audit your SIEM, your retainer, your forensic log retention, and the date of your last tabletop — "someone wrote a plan in 2022" does not score.

- ☐ **SIEM or managed XDR/MDR** ingests logs from identity, firewall, EDR, M365 / Workspace and key servers; coverage map is current.
- ☐ **Log retention** is at least 12 months online for hot search, with cold archive beyond for forensics.
- ☐ **Critical alerts route 24/7** to a SOC, MSP or on-call rota with a defined response SLA.
- ☐ **Detection use-cases** are tuned for impossible travel, password spray, lateral movement, OAuth abuse and data exfiltration.
- ☐ **Written Incident Response Plan** with named roles, contact tree, decision authority and severity tiers is maintained and accessible offline.
- ☐ **Tabletop exercise** has been run in the last 12 months; gaps documented and closed with owners.
- ☐ **Incident Response retainer** with an external DFIR firm is contracted; the number is in the contact tree and has been tested.
- ☐ **ICO 72-hour breach reporting** process is documented; legal, PR and cyber-insurance contacts are in the contact tree.

THE RETAINER TEST

Pick up the phone right now and call your incident-response number. If it rings out, goes to voicemail, or you do not have a number to call — you do not have an incident-response capability, you have a hopeful spreadsheet.

DOMAIN 09 SCORE _____ / **10** *Aim for 9+. Below 6 = blind / no IR capability.*

10

Governance, Risk & Compliance

The controls above do not survive without governance behind them. Audit your policies, your risk register, your staff training, your supplier assurance and the alignment with the standards your customers and insurers ask about.

- ☐ **Information Security Policy suite** is approved by leadership, reviewed annually, accessible to staff, and version-controlled.
- ☐ **Risk register** exists with named risk owners, scored impact / likelihood, treatment plans and review cadence.
- ☐ **Cyber Essentials (Plus)** or ISO 27001 / SOC 2 certification is held current; gap-analysis tracks any control debt.
- ☐ **Supplier / third-party assurance** requires security questionnaires, certifications and contractual security clauses for material vendors.
- ☐ **Security awareness** training is mandatory at induction and annually; specialist training for finance, IT and developers.
- ☐ **Board / leadership reporting**: a quarterly cyber-risk dashboard covers incidents, KPIs, risk acceptances and audit findings.
- ☐ **Cyber insurance** is held with cover sized to the business; the policy schedule has been read and the warranties are achievable.
- ☐ **Regulatory alignment**: UK GDPR, sector-specific (FCA, NHS DSPT, PCI-DSS, NIS2) requirements are mapped to controls.

GOVERNANCE CLOSES THE LOOP

Every control above this section eventually fails without governance — someone notices, escalates, owns the fix, and proves it landed. The risk register, the board pack and the policy-review cycle are what turn a one-off audit into a security function.

DOMAIN 10 SCORE _____ / **10** *Aim for 8+. Below 6 = the rest will not hold.*

Σ

Scorecard summary

Transfer the score for each domain into the table. Add a maturity rating (1-5) using the scale on the intro page, then set a priority (H/M/L) based on the gap to target. Anything below 6, or sitting at maturity 1-2, is a candidate for the top-3 actions overleaf.

#	CONTROL DOMAIN	SCORE / 10	MATURITY 1-5	PRIORITY
01	Identity & Access Management	_____ /10	_____	☐ H ☐ M ☐ L
02	Endpoint Security & EDR	_____ /10	_____	☐ H ☐ M ☐ L
03	Network Security & Perimeter	_____ /10	_____	☐ H ☐ M ☐ L
04	Data Protection & Encryption	_____ /10	_____	☐ H ☐ M ☐ L
05	Application & Cloud Security	_____ /10	_____	☐ H ☐ M ☐ L
06	Email & Phishing Defence	_____ /10	_____	☐ H ☐ M ☐ L
07	Vulnerability & Patch Management	_____ /10	_____	☐ H ☐ M ☐ L
08	Backup & Recovery	_____ /10	_____	☐ H ☐ M ☐ L
09	Security Monitoring & Incident Response	_____ /10	_____	☐ H ☐ M ☐ L
10	Governance, Risk & Compliance	_____ /10	_____	☐ H ☐ M ☐ L
Σ	**TOTAL SCORE**	_____ /100	_____	—

SCORE INTERPRETATION

80–100 Strong. Posture is mature; focus on detection tuning, drills and emerging threats. **60–79** Foundational, gaps exist; prioritise any domain scoring below 6. **Below 60** Material risk; commission a formal security review and remediation plan.

Control owners & target dates

Every domain needs an accountable owner and a target date for the next review or remediation milestone — otherwise nothing moves. Assign one named person per domain, agree the target, and revisit at the cadence agreed on the next page.

#	CONTROL DOMAIN	OWNER (NAMED PERSON)	TARGET DATE
01	Identity & Access Management	_____	_____
02	Endpoint Security & EDR	_____	_____
03	Network Security & Perimeter	_____	_____
04	Data Protection & Encryption	_____	_____
05	Application & Cloud Security	_____	_____
06	Email & Phishing Defence	_____	_____
07	Vulnerability & Patch Management	_____	_____
08	Backup & Recovery	_____	_____
09	Security Monitoring & Incident Response	_____	_____
10	Governance, Risk & Compliance	_____	_____

NAMING THE OWNER IS THE WORK

A control without an owner is a hope. Pick one person per domain — the head of IT, the MSP account lead, a department head — with the authority to commission the fix. “Everyone” and “the team” do not score; a name does.

Priority actions & sign-off

Commit to a small number of next steps. The goal is one page of decisions, not a wish list. Sign and date the assessment so it can be carried into the next quarterly review.

Top 3 priority actions

01 _____

02 _____

03 _____

Additional notes & risk acceptances

_____

_____

_____

_____

Sign-off

ASSESSMENT COMPLETED BY	ROLE / TITLE	DATE

APPROVED BY (SPONSOR)	SIGNATURE	NEXT REVIEW DUE

CLOUDSWITCHED

CYBERSECURITY & MANAGED DEFENCE

info@cloudswitched.com

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