PROVE & PROTECT

Security Posture Self-Audit Checklist

A structured diagnostic for IT Leaders.

CloudClevr

How to use: ◯ Yes - fully in place ◯ Partial - needs work ◯ No - not in place

1. VISIBILITY & ASSET MANAGEMENT

You have a current, complete inventory of all devices, users, and applications in your environment. Including cloud services, remote endpoints, and third-party access.	◯ Yes	◯ Partial	◯ No
You know exactly where your sensitive data is stored and who has access to it. Data classification and access mapping are documented and reviewed regularly.	◯ Yes	◯ Partial	◯ No
You have a unified view of your security posture across all tools and platforms. Not separate dashboards — a single, consolidated picture.	◯ Yes	◯ Partial	◯ No
Permissions and access rights are reviewed and updated at least every six months. Including ex-employees, contractors, and third-party integrations.	◯ Yes	◯ Partial	◯ No
Shadow IT (unmanaged apps and devices) is actively monitored and controlled. You know what your team is using, even if IT didn't deploy it.	◯ Yes	◯ Partial	◯ No

2. IDENTITY & ACCESS CONTROL

Multi-factor authentication (MFA) is enforced across all user accounts and remote access. Including email, VPN, cloud platforms, and admin accounts — not just some of them.	◯ Yes	◯ Partial	◯ No
Privileged access is restricted, monitored, and reviewed regularly. Admin rights are granted on a need-only basis with full audit logging.	◯ Yes	◯ Partial	◯ No
Joiners, movers, and leavers processes are consistently applied and timely. Access is removed or updated within 24 hours of a role or employment change.	◯ Yes	◯ Partial	◯ No
Password policies meet current NCSC guidance. Long, unique passwords with no mandatory rotation unless compromised.	◯ Yes	◯ Partial	◯ No
Single Sign-On (SSO) is implemented where possible. Reducing credential sprawl across multiple platforms.	◯ Yes	◯ Partial	◯ No

3. ENDPOINT & NETWORK SECURITY

Endpoint Detection & Response (EDR) or Extended Detection & Response (XDR) tools are deployed and actively monitored. Behavioural detection with a response capability — not just antivirus.	◯ Yes	◯ Partial	◯ No
Software patching is automated and applied within 14 days of release. Across operating systems, third-party applications, and firmware.	◯ Yes	◯ Partial	◯ No
Network traffic is monitored for anomalous activity. With alerts and a defined process for investigating suspicious behaviour.	◯ Yes	◯ Partial	◯ No
Remote access is secured via VPN or Zero Trust architecture. With device compliance checks enforced before granting access.	◯ Yes	◯ Partial	◯ No

4. INCIDENT RESPONSE READINESS

	Yes	Partial	No
A formal Cyber Incident Response Plan exists and is documented. Covering roles, escalation paths, communication, and ICO notification requirements.	○	○	○
The response plan has been tested in a realistic exercise in the last twelve months. A tabletop simulation or breach scenario — not just a policy review.	○	○	○
Your team knows exactly who to call in the first hour of a breach. Including out-of-hours contacts for IT, legal, PR, and executive leadership.	○	○	○
You have a defined process for communicating with customers and regulators in a breach. Including ICO notification within 72 hours where required under GDPR.	○	○	○

5. GOVERNANCE, COMPLIANCE & EVIDENCE

	Yes	Partial	No
You can produce clear, current evidence of your security posture if asked today. Not policies — documented, provable controls with recent review dates.	○	○	○
Your cyber insurance policy is current and you can evidence the controls required. Including EDR/XDR, MFA, patching cadence, and incident response documentation.	○	○	○
You are aware of and actively working toward relevant compliance frameworks. Cyber Essentials, ISO 27001, GDPR, or sector-specific requirements.	○	○	○
Security responsibilities are clearly assigned at board or executive level. Someone owns cyber risk at a governance level — not just within IT.	○	○	○
A formal security review has been completed by an independent party in the last 12 months. Not self-assessed against a checklist alone.	○	○	○

NOTES / ACTIONS

Ready to go deeper?

CloudClevr

A focused, expert-led review designed to identify gaps, risks, and areas of uncertainty across your current security posture.

Your security exposure review includes:

- Security posture review
- Incident readiness discussion
- Executive-level findings summary
- Exposure and vulnerability visibility
- Risk and control gap identification
- Prioritised remediation recommendations

Book a Free Security Exposure Review