CLOUDSWITCHED

FREE RESOURCE — CHECKLIST

Cybersecurity Assessment Checklist

Comprehensive security posture assessment across networks, endpoints, identity, data, and governance. Identify vulnerabilities and strengthen your defences with this structured audit.

6	50+	Score	Free
SECURITY DOMAINS	ASSESSMENT ITEMS	EACH DOMAIN OUT OF 10	SECURITY ASSESSMENT

How to Use This Checklist

Work through each section with your IT team or security provider. Tick items that are fully in place with evidence. Score each section out of 10. Results can be used to prioritise security investments and support Cyber Essentials or ISO 27001 preparation.

1 Identity & Access Management

- [ ] **MFA is enforced** on all cloud services, VPN, email, and admin accounts
- [ ] **Password policy** requires minimum 12 characters with complexity or passphrase approach
- [ ] Separate **admin accounts** are used for administrative tasks (not day-to-day user accounts)
- [ ] **Privileged access** is limited — users do not have local admin rights on workstations
- [ ] **User access reviews** are conducted quarterly — leavers disabled within 24 hours
- [ ] **Service accounts** are inventoried with strong passwords and no interactive logon
- [ ] **Single Sign-On (SSO)** is implemented where possible to reduce credential sprawl
- [ ] **Conditional Access** restricts sign-ins by device compliance, location, and risk level

Section Score: _____ /10

2 Endpoint Protection

- [ ] **EDR (Endpoint Detection & Response)** is deployed and centrally managed on all endpoints
- [ ] All devices have **full disk encryption** (BitLocker on Windows, FileVault on Mac)
- [ ] **OS patching** is automated — critical patches within 14 days, all others within 30 days
- [ ] **Application patching** covers third-party apps (Adobe, Chrome, Java) not just OS
- [ ] **USB device control** restricts unauthorised removable media
- [ ] **Mobile Device Management (MDM)** is in place for all company and BYOD devices accessing data
- [ ] Endpoint **firewall** is enabled and configured on all devices
- [ ] Devices that fail compliance checks are **blocked from corporate resources**

Section Score: _____ /10

3 Network Security

- [ ] **Firewall** is configured with deny-all default and documented allow rules
- [ ] Network is **segmented** with VLANs separating corporate, guest, IoT, and server traffic
- [ ] **Intrusion Detection/Prevention** (IDS/IPS) is active and signatures updated
- [ ] **DNS filtering** blocks known malicious domains and categories
- [ ] **VPN or ZTNA** is required for all remote access with MFA enforced
- [ ] No **unnecessary services** are exposed to the internet (RDP, SMB, FTP blocked inbound)
- [ ] **WiFi security** uses WPA3/WPA2-Enterprise with guest isolation
- [ ] **Network monitoring** detects and alerts on anomalous traffic patterns

Section Score: ____ /10

4 Email & Data Protection

- [ ] **SPF, DKIM, and DMARC** are configured on all company email domains
- [ ] **Anti-phishing** and anti-malware protection is active on email (Defender for O365 or equivalent)
- [ ] **External email tagging** visually flags emails from outside the organisation
- [ ] **Data Loss Prevention (DLP)** policies prevent sensitive data leaving via email or cloud sharing
- [ ] **Sensitivity labels** or classification is applied to confidential documents
- [ ] **Email archiving** meets retention and compliance requirements
- [ ] **Backup** covers all critical data including M365 (email, OneDrive, SharePoint, Teams)

Section Score: ____ /10

5 Incident Response & Recovery

- [ ] A documented **incident response plan** exists with defined roles and procedures
- [ ] **Backup restore tests** are conducted monthly with documented results
- [ ] **Disaster recovery plan** exists with defined RTO and RPO targets
- [ ] DR plan has been **tested** within the last 12 months
- [ ] **Cyber insurance** is in place with adequate coverage limits
- [ ] **ICO breach notification** process is documented (72-hour deadline)

Section Score: ____ /10

6 Security Governance

- [ ] **Security policies** cover acceptable use, BYOD, remote working, and data handling
- [ ] **Security awareness training** is provided to all staff annually with phishing simulations
- [ ] **Cyber Essentials** certification is current
- [ ] A **risk register** documents IT risks with likelihood, impact, and mitigations
- [ ] IT security is discussed at **board level** at least quarterly
- [ ] **Third-party/vendor security** is assessed before granting access to systems or data

Section Score: ____ /10

#	AREA	SCORE	PRIORITY
1	Identity & Access	/ 10	H / M / L
2	Endpoint Protection	/ 10	H / M / L
3	Network Security	/ 10	H / M / L
4	Email & Data	/ 10	H / M / L
5	Incident Response	/ 10	H / M / L
6	Security Governance	/ 10	H / M / L

TOTAL SCORE	**/ 60**

Score Interpretation

80–100: Excellent — well-managed with only minor improvements needed.
60–79: Good foundation but gaps exist. Prioritise areas scoring below 6.
Below 60: Significant gaps putting your business at risk. Seek specialist review.

! Action Items & Notes

Top 3 Priority Actions:

1.

2.

3.

Notes

Need a Professional Security Assessment?

Our security team conducts thorough cybersecurity assessments and helps you build a prioritised remediation roadmap.

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

Completed by: Date: Next review:

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