UK Law Firm Cybersecurity Checklist (2026 Edition)

For Managing Partners, COFAs, COLPs and Practice Managers

How to Use This Checklist

This checklist is designed for managing partners, COFAs, COLPs and practice managers who want to assess whether their firm has implemented proportionate and defensible cybersecurity controls aligned with UK legal-sector expectations. It is not a certification standard. It is a practical baseline.

Information Security Governance

- ☐ Information Security Policy
- ☐ Named person responsible for cybersecurity oversight
- ☐ Defined roles and responsibilities
- ☐ Incident response plan documented and accessible
- ☐ Annual review of security policies recorded

Identity & Access Control

- ☐ Multi-factor authentication enforced on all email accounts
- ☐ MFA enforced on admin accounts
- ☐ No shared user accounts
- ☐ Least-privilege access applied
- ☐ Joiner/mover/leaver process documented

Endpoint Protection

- ☐ Modern endpoint protection deployed (EDR/AV)
- ☐ Automatic threat updates enabled
- ☐ Device encryption enabled (laptops)
- ☐ USB/storage controls defined

Backups and BCP

- ☐ Backups stored separately or immutable
- ☐ Backup access restricted
- ☐ Restore test completed within last 6 months
- ☐ Business continuity plan documented
- ☐ Recovery time objectives defined

Staff Awareness & Culture

- ☐ Annual cybersecurity awareness training completed
- ☐ Phishing simulations conducted
- ☐ Staff aware of reporting procedure for suspicious emails
- ☐ Clear internal escalation process

Risk & Asset Management

- ☐ Asset register (devices, servers, cloud services)
- ☐ Software register maintained
- ☐ Risk assessment conducted within last 12 months
- ☐ Third-party supplier risk review completed
- ☐ Cyber insurance policy reviewed/aligned

Secure Configuration & Patching

- ☐ Devices centrally managed
- ☐ Operating systems patched regularly
- ☐ Network devices (firewalls, routers) updated
- ☐ Default passwords removed
- ☐ Remote access secured

Email & Anti-Phishing Controls

- ☐ Anti-phishing filtering enabled
- ☐ SPF, DKIM and DMARC configured
- ☐ External email tagging enabled
- ☐ Mailbox forwarding rules monitored

Client Money & Conveyancing

- ☐ Written payment verification procedure
- ☐ Bank detail changes verified out-of-band
- ☐ Dual authorisation for high-value transfers
- ☐ Completion-day communication controls
- ☐ Payment confirmation logs retained

Certification & Assurance

- ☐ Cyber Essentials achieved or in progress
- ☐ Lexcel status reviewed (if applicable)
- ☐ ISO 27001 alignment assessed (if required by clients)
- ☐ Client security questionnaires template prepared

Advanced Controls

- ☐ Privileged Access Management (PAM)
- ☐ Conditional Access & Device Compliance Enforcement
- ☐ Immutable / Ransomware-Resistant Backup Architecture
- ☐ 24/7 Managed Detection & Response (MDR)
- ☐ Board-Level Cyber Incident Tabletop Exercises
- ☐ Data Loss Prevention (DLP)
- ☐ Email Impersonation & Domain Protection
- ☐ Identity Threat Protection and Response (ITDR)

Self-Assessment Score

Tick each completed control and calculate:

- **>80% completed → Strong baseline**
- **60–79% → Moderate risk exposure**
- **<60% → Significant regulatory/operational risk**

Below 80%?
Book an IT Assessment
manxtechgroup.com/itaas