Cyber Security Checklist for Regulated Financial & Professional Services

BLACK SWAN
CYBER SECURITY SOLUTIONS

Protect client data. Stay compliant. Build trust.

You handle highly confidential financial and personal data every day - tax returns, investment portfolios, payroll records, ID documents and pension details.

A single breach could trigger an ICO investigation, FCA notification, or even an AML compliance review.

This checklist helps your firm benchmark its current security posture and demonstrate "appropriate technical and organisational measures" under UK GDPR, Data Protection Act 2018 and relevant FCA / Professional Body standards.

1 Access & Authentication

- [ ] Enforce Multi-Factor Authentication (MFA) for Microsoft 365, CRM, accounting and banking platforms
- [ ] Apply role-based access control (RBAC) for staff, advisers and contractors
- [ ] Keep admin accounts separate from daily-use logins
- [ ] Store passwords in an encrypted password manager (e.g. Keeper)
- [ ] Revoke access promptly when staff or partners leave
- [ ] Each user has a unique login - no shared or generic accounts
- [ ] Use unique, strong passphrases for every account (at least 12 characters or three random words)
- [ ] Apply account lockout after failed login attempts
- [ ] Use a secure password reset process - never reset via email / text without verification
- [ ] Review and update passwords immediately if compromise is suspected

2 Email & Communication Security

- [ ] Enable advanced phishing protection
- [ ] Configure and monitor DMARC, SPF and DKIM
- [ ] Encrypt all client file transfers - no plain-text attachments
- [ ] Use warning banners for external emails
- [ ] Provide ongoing phishing awareness training

3 Data Protection & Backup

- [ ] Back up all cloud and on-prem files daily with immutable copies
- [ ] Test backups quarterly for recovery speed and data integrity
- [ ] Use UK-based or UK-compliant storage
- [ ] Encrypt data at rest and in transit
- [ ] Restrict access to authorised roles only

4 Device & Endpoint Protection

- [ ] Deploy Next-Gen Antivirus / Managed EDR
- [ ] Automate patch management for all systems and apps
- [ ] Enable disk encryption (BitLocker / FileVault)
- [ ] Secure and remotely wipe mobile devices
- [ ] Maintain an asset inventory and run regular health checks

5 Network & Cloud Security

- [ ] Use secure Wi-Fi (WPA3) and separate guest networks
- [ ] Enable DNS filtering and web threat protection
- [ ] Configure and review firewalls quarterly
- [ ] Apply Microsoft 365 / Google Workspace security baselines
- [ ] Restrict sharing to named users - disable public links

6 Staff Awareness & Culture

- [ ] Run regular cyber awareness training
- [ ] Conduct phishing simulations to reinforce learning
- [ ] Maintain a no-blame incident reporting process
- [ ] Ensure staff understand data-handling and confidentiality policies
- [ ] Include GDPR, AML, FCA or professional-body compliance in staff induction

7 Governance, Compliance & Accountability

- [ ] Review Information Security and Data Protection Policies annually
- [ ] Maintain GDPR accountability evidence (Record of Processing Activities, DPIAs)
- [ ] Keep ICO registration and fees up to date
- [ ] Hold or work towards Cyber Essentials certification
- [ ] Review access logs, audit trails and configurations regularly

8 Regulatory & Sector Obligations

FCA / PRA Regulated Firms

- [ ] Ensure systems and controls meet SYSC 3 (Operational Risk) and SYSC 13 (Operational Resilience)
- [ ] Complete an annual cyber resilience review (aligned with FCA FG16/5)
- [ ] Vet outsourced IT and cloud suppliers under SS2/21
- [ ] Protect client data as part of delivering fair outcomes under the Consumer Duty
- [ ] Assess incidents for materiality and report to the FCA where required
- [ ] Test business continuity and incident response plans annually

Anti-Money Laundering (AML)

- [ ] Protect AML software with MFA
- [ ] Submit Suspicious Activity Reports (SARs) securely via the NCA portal
- [ ] Follow AML record-keeping rules (retain and delete after five years)
- [ ] Keep AML risk assessments and compliance reviews documented

Professional Bodies (ICAEW / ACCA / CISI / AAT / STEP etc.)

- [ ] Protect client data in line with the Code of Ethics
- [ ] Use secure client portals or encrypted transfer methods
- [ ] Conduct annual internal reviews of data and system security

9 Incident Response & Monitoring

- [ ] Have Managed Detection & Response (MDR) in place
- [ ] Define steps for password resets and MFA re-enrolment
- [ ] Retain Microsoft 365 audit and sign-in logs for at least 12 months
- [ ] Test your incident response plan annually
- [ ] Review cyber insurance policy wording and control requirements

Who is this for?

This checklist is designed for regulated and professional service firms handling sensitive client information, including:

» Independent Financial Advisers (IFAs)

» Accountants and Bookkeepers

» Wealth Managers and Investment Planners

» Estate and Tax Planners

» Mortgage and Protection Advisers

» Payroll Bureaus and Financial Administrators

» Compliance Consultants and Virtual Finance Offices

If your business falls under FCA, PRA, HMRC or professional-body oversight, this checklist helps you prove due diligence, meet audit expectations and reassure clients that their data is in safe hands.

BLACK SWAN
CYBER SECURITY SOLUTIONS

Need help tightening your security?

blackswancyber.co.uk

hello@blackswancyber.co.uk

01246 927142

Black Swan Cyber Security Solutions

Helping regulated firms stay secure, compliant and trusted - without the jargon.