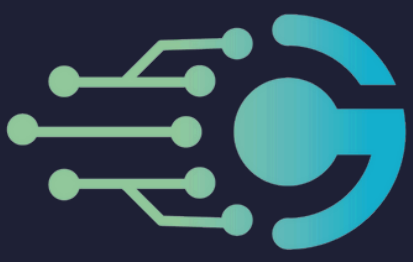
GUIDE

A Practical IT Checklist for FCA-Regulated Firms



Chapman Technology Partners

Ensure regulatory compliance, and maintain business continuity

In today's financial landscape, IT isn't just about keeping the computers on - it's about protecting sensitive client data, ensuring regulatory compliance, and maintaining business continuity.

For FCA-regulated firms, the stakes are even higher. The Financial Conduct Authority (FCA) places clear expectations on the financial services sector when it comes to operational resilience, cybersecurity, and data protection.

This practical IT checklist is designed specifically for financial advisors, mortgage brokers, wealth managers, and accountants who must meet FCA requirements while maintaining robust, efficient IT systems.

Why FCA-Regulated Firms Need an IT Checklist

Regulatory Compliance

The FCA expects firms to have adequate systems and controls to protect data and deliver services without undue interruption.

Client Trust

Protecting client data is essential to maintaining long-term relationships.

Operational Resilience

Your IT infrastructure must be able to withstand, absorb, and quickly recover from cyber-attacks, system failures, and external threats.

Cyber Security Risk

FCA-regulated firms are prime targets for cyber crime.

FCA-regulated firms were fined over £50 million in 2023 for failings related to systems and controls.

Source: FCA Enforcement Annual Performance Report, 2023

The Essential IT Checklist for FCA-Regulated Firms

Use this checklist to assess whether your IT and cybersecurity practices align with FCA expectations and industry best practice.

1. Cyber Security Controls

- [ ] Up-to-date antivirus and endpoint protection on all devices
- [ ] Firewalls configured and regularly tested
- [ ] Multi-Factor Authentication (MFA) enforced across all systems
- [ ] Secure password policy in place and monitored
- [ ] Regular vulnerability scans and penetration testing
- [ ] Device encryption for laptops and mobile equipment

FCA Guidance: Firms "must establish and maintain appropriate systems and controls to manage their information security risks"

---

2. Data Protection & Privacy

- [ ] GDPR-compliant data storage and processing practices
- [ ] Documented data-retention and deletion policies
- [ ] Secure client communication channels (email encryption, secure portals)
- [ ] A clear data-breach response plan, tested periodically
- [ ] Access controls based on roles and responsibilities to restrict data access

FCA Guidance: FCA expects firms to minimise risk to information assets via systems and controls

3. Backup & Disaster Recovery

- [ ] Daily, automated backups of critical systems and data
- [ ] Backups stored securely offsite or in the cloud
- [ ] Regularly tested disaster recovery (DR) and business continuity (BCP) plans
- [ ] Clear Recovery Time Objectives (RTO) and Recovery Point
- [ ] Objectives (RPO) defined

FCA Guidance: Firms must demonstrate operational resilience and the ability to continue critical services in the event of disruption.

---

4. Software & System Updates

- [ ] All systems, software, and security patches updated promptly
- [ ] Decommission unsupported software
- [ ] Maintain an accurate hardware and software asset register

FCA Guidance: Adequate systems and procedures to safeguard security and operational integrity are required.

---

5. Staff Training & Awareness

- [ ] Regular cyber security awareness training for all staff
- [ ] Phishing simulations conducted at least quarterly
- [ ] Clearly defined incident and phishing-reporting procedures

FCA Guidance: Firms must ensure staff understand their responsibilities in managing IT and cyber security risks.

---

6. Third-Party Vendor Management

- [ ] IT providers and other third parties assessed for security posture
- [ ] Contracts reviewed for data security and FCA compliance obligations
- [ ] Continuous monitoring of critical third-party systems

FCA Guidance: Firms must ensure third-party providers meet appropriate security standards

7. IT Governance & Policy

- [ ] Documented IT policies: Acceptable use, InfoSec, backup, change management
- [ ] Regular IT and cyber security risk assessments aligned with FCA guidelines
- [ ] Senior management oversight of IT and cybersecurity risks with clear individual and board-level accountability

FCA Guidance: Firms must have strong governance and clear accountability for IT risks.

---

8. Incident Response Planning

- [ ] Documented incident-response and escalation plan
- [ ] Assigned incident-response roles and communication strategies
- [ ] Regular incident simulations and root-cause review

FCA Guidance: In line with operational resilience, firms must test for, respond to, and learn from severe but plausible operational disruptions

---

9. Operational Resilience & Scenario Testing

- [ ] Identify Important Business Services (IBS) and map key supporting resources
- [ ] Define impact tolerances, and set/monitor RTO/RPO thresholds
- [ ] Conduct scenario testing using "severe but plausible" scenarios
- [ ] Document metrics and results in a self-assessment report for the Board

FCA Guidance: Firms are required to remain within impact tolerances during severe-but-plausible disruptions and scenario-testing of IBSs

---

10. Monitoring & Continuous Improvement

- [ ] Programmes for ongoing monitoring of resilience controls
- [ ] Annual reviews, plus updates when systems or third-parties change
- [ ] Lessons learned processes and update cycles for DR/IR plans

FCA Guidance: Senior management must oversee continuous resilience improvements, supported by self-assessments

Final Thoughts

FCA-regulated firms cannot afford to treat IT and cyber security as a secondary concern. Having a structured IT checklist in place ensures you're not only meeting regulatory expectations but also protecting your business and your clients.

Regular reviews, ongoing staff education, and proactive risk management are critical to staying one step ahead.

Next Step: Book a Free IT Review

At Chapman Technology Partners, we specialise in supporting financial services firms with fully managed IT and cybersecurity solutions that align with FCA requirements.

Book your free 15 minute intro call here – let's make sure your IT is working for you, not against you.

www.chapmantechnologypartners.co.uk

Chapman Technology Partners

Strategic IT, Cyber Security & AI Solutions
for Regulated Industries

Strawberry Fields Digital Hub,
Chorley, PR7 1PS

greg@gregorychapman.co.uk
01257 542388

CYBER ESSENTIALS CERTIFIED