



FCA-Regulated Firms

IT & Cyber Governance Checklist

A practical checklist for FCA regulated financial services firms

MANAGE. PROTECT. ASSURE.

Purpose of this checklist

A senior read on your IT and cyber posture

Financial firms hold sensitive data and are expected to keep their services running and recover quickly when something goes wrong. Since the FCA tightened its operational resilience rules in 2025, firms are judged on evidence, not intentions. These questions are written to help you identify the gaps between what you believe is in place and what you could actually prove.

Why this checklist matters

- Remote working, cloud services and external suppliers have widened the ground you need to defend
- The FCA now looks for evidence of resilience, not a plan on paper
- Most incidents trace back to everyday gaps, not sophisticated attacks
- Your supply chain security is only as strong as the weakest link
- Clients and insurers increasingly ask you to prove your security before they engage

How to use it

- Answer each question with evidence in mind, not good intentions
- Treat anything you cannot prove as a no
- Note the gaps, then use the roadmap near the end to decide what to tackle first

Control and visibility of your IT

Tests whether your IT is genuinely under control, or only assumed to be.

		Yes	No
1	Could you produce an accurate, current list of the systems , devices and cloud services that hold client or financial data, and say who owns each?	☐	☐
2	Does everyone have access to only what their role requires, and is that reviewed regularly rather than assumed?	☐	☐
3	When someone leaves or changes role, is their access changed the same day?	☐	☐
4	Are updates and security patches applied to a defined timescale (14 days) you could evidence?	☐	☐
5	Is a named person /persons accountable for IT and cybersecurity, with the authority to act, not only to advise?	☐	☐
6	If a key system or supplier failed tomorrow, would you quickly know which parts of the business would be affected?	☐	☐



Why this matters

You cannot demonstrate control of what you cannot see. Clear ownership and current records are what turn a good intention into evidence.

PROTECT

02

Data, identity and threat exposure

Looks past whether controls exist to whether they are switched on and working.

		Yes	No
1	Is multifactor authentication enabled, enforced and reviewed for every cloud service that offers it ?	☐	☐
2	Are administrator accounts protected and the use of them tracked across the organisation?	☐	☐
3	If someone clicked a convincing phishing email today, what would stop it becoming a breach?	☐	☐
4	Do you know where your most sensitive client data lives, and exactly who has access to it?	☐	☐
5	Would your current technical controls alert you to suspicious activity affecting your organisation?	☐	☐
6	Are the controls you pay for actually switched on and working, rather than bought and assumed?	☐	☐



Why this matters

Stolen credentials and email remain the most common way into a financial firm. The question is never whether you own a control, but whether it is doing its job.

Continuity, recovery and resilience

Maps directly to what the FCA now expects firms to evidence.

		Yes	No
1	Have you identified the main services that would harm customers most if they stopped working?	☐	☐
2	Do you know how long each service could be down before the harm becomes unacceptable, and have you tested that you can stay within that time frame?	☐	☐
3	Have you actually restored from a backup recently, rather than trusting that it would work?	☐	☐
4	Is at least one copy of your backup kept on a separate network or in a separate location, where a threat actor could not reach or delete it?	☐	☐
5	In the first hour of a serious incident, would everyone know their role and how to respond?	☐	☐
6	Could you show the FCA what happened, when, and how you responded?	☐	☐



Why this matters

The FCA expects firms to stay within agreed limits through disruption and to prove it. Untested recovery and unmapped suppliers are where most firms fall short.

CERTIFY

04

Turning trust into proof

Works whether you are certified already or only starting out.

		Yes	No
1	When a client or regulator asks you to prove your security, can you point to an independent standard, or only describe your own efforts?	☐	☐
2	Do you know which certifications your clients, insurers and regulators increasingly expect before they will work with you?	☐	☐
3	Does your security follow a recognised framework such as Cyber Essentials, the CIS Controls or ISO 27001?	☐	☐
4	If you already hold a certification, do you know exactly what it covers, and would you still pass if assessed today?	☐	☐
5	Has an independent party ever tested your defences, or has your security only been checked internally ?	☐	☐
6	Do you treat certification as a live standard to keep up, rather than a badge earned once and filed away?	☐	☐



Why this matters

Certification turns your security from a claim into something a client, insurer or regulator can verify. It is fast becoming a condition of doing business, not a nice-to-have.

Your resilience snapshot

What your answers tell you

Count the questions you could not answer yes to with evidence. You are not chasing a perfect score. You are finding the places where belief and evidence part company.

- 1** **Mostly yes.** A mature base. The task is to keep the evidence current and rehearsed.
- 2** **A mix of yes and no.** Real gaps worth closing before your next review or assessment.
- 3** **Mostly no.** Priority areas that leave the firm exposed and hard to defend.

Treat these as red flags whatever your score

- You could not evidence your important business services or impact tolerances
- Your backups have not been restored and tested recently
- Multifactor authentication is not enabled on every service that offers it
- You rely on suppliers whose security you have never independently checked

A simple roadmap

Where to go from here

Wherever this checklist placed you, the path forward looks similar. Find your current stage and take the next step. Most firms sit between stages one and three, and steady progress matters more than a perfect score.

1

Fix the foundations

Close the everyday gaps this checklist surfaced: access, patching, backups and multi factor authentication. Most risk lives here.

2

Prove the baseline

Achieve Cyber Essentials, then Cyber Essentials Plus, so your controls are independently verified.

3

Broaden the assurance

Grow toward IASME Cyber Assurance or ISO 27001 as client, insurer and regulatory demands increase.

4

Keep it live

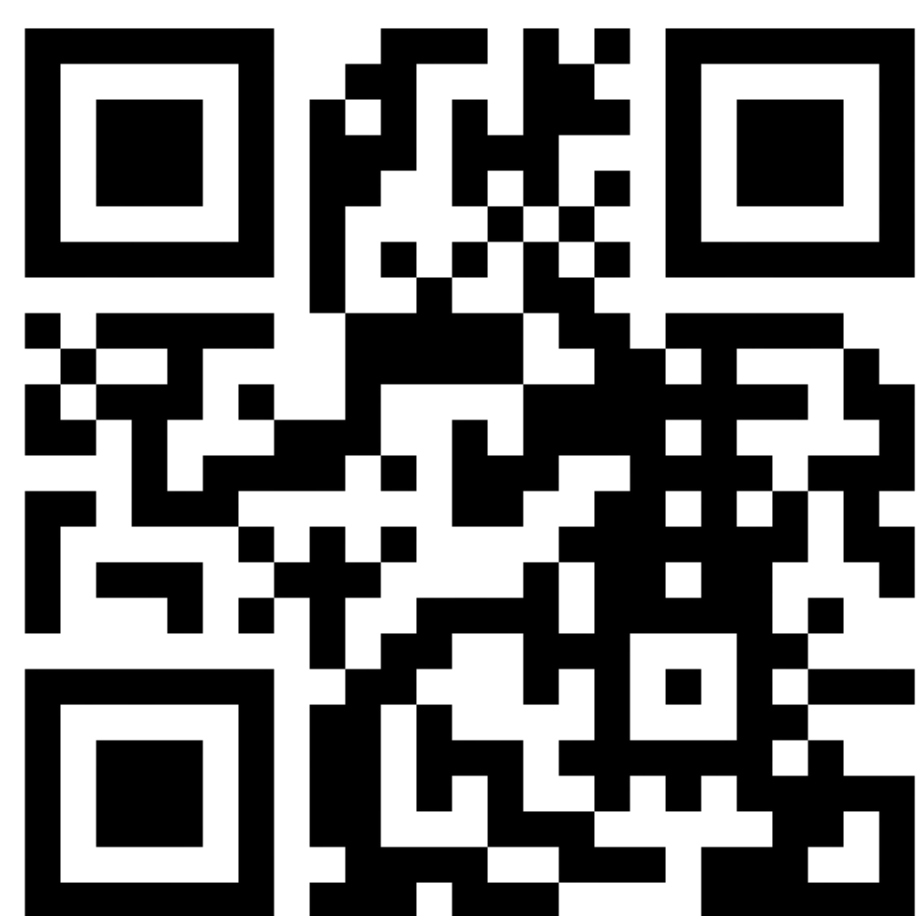
Retest, review and evidence continuously, so resilience and certification stay current.

Next step

If you would like an independent view

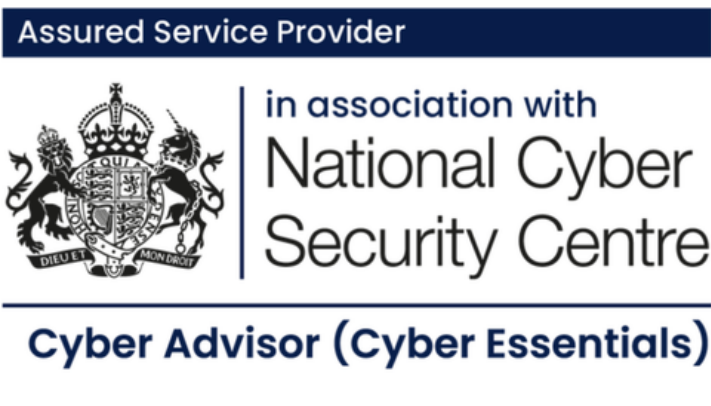
This checklist is a starting point, meant to help you see where you stand rather than to grade you. If you would like independent advice, you are welcome to request a consultation with our team.

How to get in touch



Email
info@complus-it.com

Address
107-111 Fleet St, London EC4A 2AB



This checklist reflects UK requirements in force as at August 2026, including the FCA operational resilience rules and the 2026 Cyber Essentials requirements. It is general guidance and not regulatory advice.