



BONUS TOOLKIT · THE AI FORWARD BROKER

The Broker Financial Crime Evidence Pack

Three artefacts that turn the FCA's multi-firm review into a one-afternoon job, not a six-week scramble. Build them before the next round of insurer due diligence lands.

Chris Matthews

AI Strategist, Speaker & Author

Making AI practical for business



How this worksheet works

This is a working document, not a policy. It is for principals, compliance leads, and senior managers at general insurance brokers. Run it now, before an insurer asks you to evidence your financial crime controls, not after.

Why this exists

The FCA published a multi-firm review on financial crime controls across insurance firms. If you run a broker, do not read that as an insurer problem. Read it as: an evidence request is coming.

When insurers tighten their own controls, they push the pain downstream: through onboarding, bordereaux, TOBA scrutiny, delegated authority checks, and post-bind sampling.

The review flagged three recurring weaknesses in general insurance. Group-level policies that are not specific enough at the business unit level. Limited evidence of structured, risk-based monitoring and testing. Uneven oversight of third parties. That is the regulator telling the market what it expects to see written down, not what it expects to see said.

This worksheet helps you build the three artefacts that answer all three weaknesses: a financial crime control map, a risk-based monitoring log, and a third-party oversight register. Being 'mostly effective' is not a defence when you cannot evidence it.

How to use it

- Run it with whoever owns compliance and at least one person who actually does the onboarding and checking day to day.
- Start with Section 1, the control map. You cannot test or oversee what you have not first owned.
- Be specific. Name people, name systems. Vague answers fail an insurer's due diligence.
- Where you cannot answer, write "unknown". Unknown is itself a finding, and it goes straight into the action log.

Key terms

The terms used through this worksheet, in the order they matter.

Term	Stands for	What it means here
RACI	Responsible, Accountable, Consulted, Informed	A grid showing who does the work, who owns the outcome, and who must be told.
TOBA	Terms of Business Agreement	The contract between you and your capacity provider that sets out your obligations.
Bordereaux	n/a	The periodic data reports you send insurers on policies bound and claims handled.



Term	Stands for	What it means here
Delegated authority	n/a	Permission an insurer grants you to bind, price, or handle claims on their behalf.
Post-bind sampling	n/a	An insurer checking a sample of your bound policies after the fact to test your controls.



SECTION 1

01

The financial crime control map

One page. A clean RACI matrix mapping who owns sanctions, fraud, bribery and corruption, and the due diligence activities your capacity providers demand. Named people, named systems. This comes first because you cannot test or oversee a control you have not first assigned.

Control area	Responsible (does it)	Accountable (owns it)	System / tool	Capacity provider requirement
Sanctions screening				
Fraud detection				
Bribery & corruption				
Customer due diligence (onboarding)				
Ongoing / enhanced due diligence				

What each control area means

Sanctions screening. Checking customers, beneficial owners, and counterparties against sanctions lists at onboarding and on an ongoing basis.

Fraud detection. How you spot and act on application fraud, claims fraud, and internal fraud.

Bribery and corruption. Controls over gifts, hospitality, introducer payments, and conflicts that could constitute a bribe.

Customer due diligence. The identity and risk checks you run before binding, and the records you keep.

A note. One page means one page. If your control map needs three pages to explain, the controls are not clear enough yet. The insurer will reach the same conclusion.



SECTION 2

02

The risk-based monitoring log

This is the heart of the document. The review flagged limited evidence of structured, risk-based monitoring and testing. The fix is a log: what you test, how often, and what changed as a result. If the honest answer is “we do it when something goes wrong”, write that down first. Then fix the cadence.

What we test	Risk (H/M/L)	Frequency	Last tested	What changed as a result

What each column means

What we test. The specific control, not the area. “Sanctions screening on new commercial clients”, not “sanctions”.

Risk rating. High, medium, or low. This is what makes it risk-based. High-risk controls get tested more often.

Frequency. How often you actually test, not how often you intend to.

What changed. The point of the whole log. A test that changes nothing was not a test, it was a tick.

Honesty first. If a control has never been tested, write “never” in the last-tested column. That single word is more useful to you than a confident blank.



03

SECTION 3

The third-party oversight register

The review flagged uneven oversight of third parties. List everyone who touches customer data or claims documentation: introducers, outsourcing partners, software vendors, anyone in the chain. What you rely on them for, what you check, and what you would show an insurer if asked.

Third party	Type	What we rely on them for	What we check	Evidence we could show

What each column means

Type. Introducer, outsourcing partner, software vendor, data processor, claims handler.

What we rely on them for. The actual dependency. Be honest about how critical they are.

What we check. Due diligence at onboarding and on an ongoing basis. If the answer is nothing, write nothing.

Evidence we could show. What lands on the table if an insurer asks tomorrow. A contract, a check, a report, or "nothing yet".

The data test. If a third party touches customer data or claims documentation and they are not on this register, the register is not finished.



SECTION 4

04

The action log

Every gap, every “unknown”, and every “never” from the three sections above lands here. This is where the worksheet turns into work.

#	Gap / finding	Owner	Action	Target date	Status



SECTION 5

05

Self-score

Score each pillar honestly out of 10. The first run is usually lower than expected. That is the point.

Pillar	Score 0 to 10	Evidence	Top priority to fix
Control map is written, named, and current			
Monitoring is risk-based and logged			
Third-party oversight is complete			
Group policy is specific at business-unit level			
You could evidence all of it within 48 hours			

Total: ___ / 50

- 40 to 50: you could survive insurer due diligence this week.
- 25 to 39: you have started. Close the gaps in the action log.
- Below 25: this is the work for the next 90 days. Start now, before the request lands.



SECTION 6

06

The next 90 days

A working sequence, not a project plan.

Days 1 to 14

- Build the one-page control map. Name every owner and system.
- Fill the gaps you can fill in a fortnight.

Days 15 to 45

- Stand up the monitoring log. Set a risk-based cadence.
- Run the first round of tests on your highest-risk controls.

Days 46 to 75

- Complete the third-party register.
- Request evidence from your most critical introducers and vendors.

Days 76 to 90

- Pressure-test the lot. Pretend an insurer asked yesterday.
- Whatever you cannot put on the table in 48 hours goes back into the action log.



ABOUT THIS WORKSHEET

About this worksheet

This worksheet maps to the FCA's multi-firm review on financial crime controls in insurance. It helps you build the three artefacts that answer the three recurring weaknesses the regulator flagged: a control map, a risk-based monitoring log, and a third-party oversight register.

Reviewed before every round of insurer due diligence. Refreshed whenever your capacity providers, your third parties, or the regulatory expectations change.

If you want a working session to build these three artefacts alongside your team, book a strategy call.

Prepared for general insurance brokers. Not legal, compliance, or regulatory advice. The FCA's expectations and your capacity providers' requirements change. Verify the current position for your firm before you rely on this. Use it alongside your own compliance and legal advisers.