NET-DEFENCE

‘Show me, don’t tell me’

How UK regulation has changed and what it now expects from law firms in practice

Net-Defence
Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: net-defence.com

Across the UK regulatory landscape, a consistent shift is now unmistakable. Regulators are no longer primarily interested in what organisations say they intend to do. They are increasingly focused on what organisations actually did, how they responded, and what changed as a result.

This is not isolated to a single regulator or sector. It is visible in financial services supervision, data protection enforcement, cyber resilience frameworks, anti-money laundering reform, and legal services oversight. While the language varies, the underlying message is the same: Written policy is not persuasive evidence. Operational behaviour is.

For law firms, particularly those balancing professional judgement, confidentiality, and complex risk profiles, this represents a significant change in regulatory reality.

From frameworks to outcomes: a system-wide regulatory shift

UK regulators have increasingly converged on an outcomes-based, evidence-driven model of supervision and enforcement.

Rather than asking:

- Do you have a policy?
- Is there a framework?

Regulators now ask:

- What happened when this risk materialised?
- How did you know it was happening?
- Who made decisions, on what basis, and with what information?
- What changed afterwards?

This shift is explicit in:

- The FCA and PRA's move toward assertive supervision and operational resilience testing
- The ICO's interpretation of accountability as demonstrable, ongoing compliance
- NCSC's Cyber Assessment Framework 4.0, which assesses whether controls work against real-world threats rather than whether they exist
- AML reform, which is explicitly concerned with traceability, consistency and supervisory effectiveness rather than professional discretion alone

The direction of travel is not subtle. Regulators are aligning on evidence of performance, not statements of intent.

Why this matters specifically for law firms

Law firms are exposed to this shift in multiple, overlapping ways. They are:

- Gatekeepers in AML, sanctions and fraud prevention
- Custodians of highly sensitive personal and financial data
- Operationally dependent on digital systems and third-party providers
- Profession-led businesses, where judgement, supervision and culture are central

Historically, this placed law firms in a relatively trusted regulatory space. Increasingly, that trust is being tested through

evidence, not assumed. Supervisors now look less at abstract compliance maturity and more at how controls worked on real matters, involving real clients, under real pressure.

The SRA: supervision as practice, not policy

The SRA's effective supervision guidance is often read as a policy document. In reality, it signals a practical, evidence-based supervisory approach.

When supervision is scrutinised, the regulator is typically interested in:

- How supervision operated on specific files
- Whether higher-risk matters received higher-intensity oversight
- How issues were escalated, challenged and resolved
- What happened when something went wrong

A formal supervision policy is no longer sufficient on its own. Regulators expect firms to show:

- Records of supervisory engagement
- Evidence of intervention or challenge
- Clear accountability chains
- Remedial actions and learning

In other words, the existence of supervision matters far less than its demonstrable operation.

AML: from professional judgement to auditability

AML supervision has undergone one of the clearest shifts from intent-based to evidence-based regulation.

Recent government reviews have highlighted persistent weaknesses across the professional services sector:

- Inconsistent risk assessments
- Over-reliance on client representations
- Limited transparency around decision-making
- Weak evidence of ongoing monitoring

In response, AML reform increasingly emphasises:

- Data-driven supervision
- Risk-weighted oversight
- Consistency across firms

The ability to reconstruct why decisions were taken at the time. For law firms, this reframes AML from a procedural hurdle into an audit-ready, longitudinal process, where decisions must remain defensible months or years later.

ICO accountability: 'demonstrate compliance' in action

Data protection regulation has long contained the word "accountability". Enforcement practice now gives that word clear

meaning. The ICO is explicit that organisations must be able to demonstrate compliance, which includes:

- Keeping evidence of protective measures
- Showing how risks were assessed and mitigated
- Recording incidents, near-misses and lessons learned
- Demonstrating that controls evolved over time

Crucially, this moves data protection out of static documentation and into operational reality. Investigations increasingly focus on:

- How quickly incidents were detected
- How decisions were taken
- Whether patterns were identified and addressed

For law firms, where confidentiality and trust are central, this expectation is unavoidable.

Cyber resilience: testing whether controls work

NCSC's CAF 4.0 crystallises the regulatory mindset now spreading across sectors.

Rather than asking:

- Is there a control?

CAF asks:

- Does it work against credible threat actors?
- Would it work under pressure?
- How do you know?

Evidence is drawn from:

- Incident response
- Exercises and simulations
- Monitoring and detection capability
- Third-party resilience and dependency management

For law firms, cyber resilience is no longer a technical concern. It is a regulatory, governance and client trust issue.

Third parties and time: two quiet but decisive tests

Across regulators, two factors now carry disproportionate weight.

Third-party dependency

Regulators increasingly view supplier failure as a foreseeable risk, not an external excuse. Firms are expected to evidence oversight, assurance and challenge over providers that underpin critical services.

Time as evidence

How quickly issues were identified, escalated, and addressed matters as much as what the eventual outcome was. Delays, indecision and repeated failures are increasingly treated as indicators of control weakness, not bad luck.

Both are central to 'Show me' regulation and both tend to expose gaps between paper design and operational reality.

What the regulator's question has become

Across the FCA, ICO, SRA, AML supervision and NCSC guidance, a single question recurs: 'What actually happened and how do you know?'

Firms that can answer this calmly, evidentially and consistently tend to experience:

- Collaborative supervision
- Faster issue resolution
- Lower enforcement risk

Firms that cannot often discover that their documentation is not questioned it is simply ignored.

This is not about more compliance, more paperwork or heavier process. It is about credibility under scrutiny.

The 'Show me, don't tell me' regulation rewards organisations that understand how their controls behave in the real world and who can evidence that understanding clearly, honestly and proportionately.

For law firms, that is no longer optional. It is the ground on which regulatory confidence is now built.

Building confidence in practice. As regulation increasingly focuses on evidence, behaviour and outcomes, firms need technology and security foundations that work reliably day to day.

We support law firms with practical cyber security, IT and resilience services; helping teams operate securely, confidently and without unnecessary complexity. Get in touch for support.