Compliance in law firms: what actually matters?

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**

Compliance is no longer about what you say. It's about what you can demonstrate.

For many law firms, compliance has become increasingly complex. There are regulatory obligations to satisfy, client requirements to meet, insurers asking tougher questions, supplier risks to manage, and an ever-growing list of cyber and operational threats to consider.

At the same time, firms are expected to continue delivering exceptional client service whilst protecting sensitive information and maintaining **operational resilience**. The challenge isn't a lack of effort. Most firms invest significant time and resources into compliance activities. Policies are written, audits are completed, certifications are achieved, and technology is deployed.

And yet a growing number of firms are discovering that having controls in place and being able to demonstrate those controls are working are two very different things. And this is where compliance is changing.

The compliance problem: everybody wants something

Today's law firms operate in an environment where compliance expectations continue to grow.

They must satisfy SRA obligations, meet UK GDPR requirements, respond to increasingly detailed client due diligence requests, comply with Cyber Essentials and cyber insurance requirements, oversee third-party suppliers, and maintain effective business continuity and information security arrangements.

Each requirement is important. Each requires attention. And the result is that many firms find themselves asking a perfectly reasonable question: What actually matters? Because when everything becomes a priority, it can be difficult to identify where the real risks sit.

The compliance illusion

One of the most common misconceptions within the **legal sector** is that compliance is defined by the things a firm possesses.

- We have policies.
- We have outsourced IT.
- We have cyber security software.
- We have completed client questionnaires.
- We have backups.
- We pass audits.

These are all positive indicators. However, none of them automatically demonstrate compliance. A policy demonstrates intent, an audit demonstrates a point-in-time assessment, and a supplier demonstrates delegation of activity. None, in isolation, demonstrate operational control. Regulators, insurers, and clients are now looking beyond what exists and focusing on how organisations operate.

Three compliance myths that still catch law firms out

Many firms don't fall short because they ignore compliance. They fall short because they rely on assumptions about what compliance looks like in practice. Some of the most common misconceptions include:

Myth one: Compliance means having policies

Policies are essential because they define responsibilities and provide consistency across the firm. But a policy sitting on a shared drive doesn't prove that anyone understands it or follows it.

Regulators increasingly want to know how those policies translate into day-to-day decision making. Can staff explain the

process? Has it been followed? Is there evidence that it has been reviewed, tested, and improved over time? Policies support compliance, but they don't demonstrate it.

Myth two: Compliance means passing audits

Passing an audit is valuable, but it only provides assurance at a specific moment in time. Between audits, systems change, suppliers evolve, people join and leave, and new risks emerge. A firm that passed an audit six months ago may still struggle to explain how it would respond to a cyber incident tomorrow. Strong compliance is reflected in everyday operational discipline.

Myth three: Compliance can be outsourced

Many firms rely on specialist providers for IT support, cyber security, hosted systems, or compliance advice, and there's nothing wrong with doing so. However, while activities can be outsourced, accountability can't.

Regulators, insurers, and clients will still expect the firm to understand what controls are in place, how suppliers are performing, and how risks are being monitored. Delegating responsibility to a third party doesn't remove the need for oversight.

The shift from intention to evidence

Historically, compliance conversations often focused on documentation. Questions tended to sound like:

- What policies do you have?
- What controls are in place?
- What processes exist?

Today, the conversation looks very different. Questions are increasingly becoming:

- How did you know there was a problem?
- What action was taken?
- Who made the decision?
- What evidence exists?
- What changed afterwards?

This represents a fundamental shift. The focus has moved from intention to evidence, from policy to behaviour, from documentation to operational reality. This shift can be summarised in a simple phrase: Show me, don't tell me. Organisations are increasingly expected to demonstrate outcomes rather than simply describe intentions. Consider the following examples.

Many firms will say "We review user access." The increasingly relevant question is: Show me the last review. Many firms will say "We have backups." The increasingly relevant question is: Show me the last successful recovery test. Many firms will say "Our supplier manages security." The increasingly relevant question becomes: Show me how you know.

The challenge facing most firms today is rarely the absence of controls, the real challenge is demonstrating those controls are operating as intended.

A real-world example: DPP Law

In April 2025, the Information Commissioner's Office fined DPP Law £60,000 following a cyberattack which exposed highly sensitive client information. Attackers gained access through an administrator account that did not have multi-factor authentication enabled.

The firm became aware that client data had been exposed after being contacted by the National Crime Agency, and the ICO identified failures relating to security measures and breach notification.

The significance of this case is not simply that a cyberattack occurred. Cyberattacks can affect organisations of all sizes and sectors. The more important lesson is the question underpinning the ICO's investigation.

- How did the organisation know what had happened?
- How quickly could it identify the issue?
- How effectively could it evidence the controls that were in place?

This is a practical example of the difference between having controls and being able to demonstrate they are working.

Why good firms still get caught out

One of the biggest myths surrounding compliance is that failures occur because organisations do not care. In reality; most compliance failures occur within organisations that are trying to do the right thing.

Common themes include:

- Policies exist, but behaviours do not consistently align to them.
- Controls exist, but nobody regularly verifies they are operating effectively.
- External suppliers exist, but oversight is limited.
- Responsibilities exist, but accountability is unclear.

The result is that risk accumulates quietly over time. Most **compliance failures** begin long before an incident takes place.

What the SRA is saying

The Solicitors Regulation Authority's **Cyber Security Thematic Review** reinforces many of the challenges law firms are facing today. After reviewing firms that had experienced cyber incidents, the SRA concluded that cyber security is far more than a technology issue. People, leadership, governance, and day-to-day operational practices all play a key role in determining how resilient a firm really is.

The review found that many firms recognised staff knowledge and behaviour as their greatest cyber risk, yet 11 of 40 firms still had inadequate cyber security policies and 10 had inadequate controls. More than half did not keep records of who had completed cyber security training, and many had never tested how their processes would perform during a real incident.

Perhaps most importantly, the SRA found that firms with stronger cyber resilience shared similar characteristics. They had visible leadership, clear accountability, regular training, well-understood reporting processes, and routinely tested their controls rather than assuming they would work when needed. Cyber Essentials certification was also highlighted as a positive indicator, with firms holding Cyber Essentials Plus generally demonstrating stronger policies and technical controls.

The message is clear. Compliance isn't demonstrated by producing a folder of policies when someone asks. Instead, it's demonstrated through culture, evidence, and the ability to show that controls are understood, monitored and operating as intended.

The visibility gap

In our experience, the issue is rarely that firms have no controls in place. The issue is visibility. Many organisations have backups but cannot confidently say when they were last tested. Security tools are installed, but few people can explain what they are reporting or whether alerts are being reviewed.

External suppliers may be responsible for key services, yet performance is rarely measured beyond the contract itself. Compliance responsibilities are assigned, but incident response processes have never been tested under pressure. Most firms have controls. Far fewer have visibility across them.

The question every firm should consider

If a regulator asked questions tomorrow, could you demonstrate:

- How was the issue identified?
- Who was informed?
- What decisions were made?
- What evidence exists?
- What changed afterwards?

Those questions often reveal more about a firm's compliance posture than an entire library of policies. Because ultimately, compliance is not about saying the right things. It is about demonstrating the right outcomes.

Final thoughts

Compliance within law firms is becoming less about documentation and more about operational confidence. Policies, certifications, and technical controls all have an important role to play, but they are only part of the picture.

What we see increasingly is that regulators, insurers, clients, and supply chain partners want evidence that those controls are understood, maintained, and capable of standing up under pressure. That means looking beyond individual compliance activities and understanding how people, processes, technology, and third-party suppliers work together.

The firms that are strongest from a compliance perspective aren't necessarily those with the largest policy library. They're the firms that know how their controls operate, regularly test them, understand where ownership sits, and can clearly demonstrate why they have confidence in their approach.

Ultimately, the question every law firm should be asking is no longer, "Can we tell people what we do?" It's "Can we demonstrate it when it matters most?"

If you're unsure whether your firm's compliance arrangements would stand up to that level of scrutiny, now is the time to take a closer look. At **Net-Defence**, we help law firms strengthen cyber resilience, managed IT, Cyber Essentials certification, and more, giving you greater visibility across your controls and the confidence to evidence them when the tough questions get asked.