NET-DEFENCE

Compliance in Law Firms: What Actually Matters?

From policies and paperwork to evidence and operational reality.

Managed Service Offerings

- IT Support
- Business Resilience as a Service
- Cyber Certifications and Resilience
- Telephony and Communication

net-defence.com

Why this conversation matters now

- Compliance expectations continue to grow.
- Evidence, visibility and accountability matter more than ever.
- This series explores what good looks like in practice.

THE COMPLIANCE PROBLEM

Everybody Wants Something!

Today's law firms are juggling:

- SRA expectations
- Client due diligence
- Cyber Essentials
- ISO certifications
- Cyber insurance requirements
- Data protection obligations
- Supplier oversight
- Business continuity expectations

The challenge: not effort or commitment – it is understanding what actually matters!

THE COMPLIANCE ILLUSION

Most Firms Believe They Are Compliant Because:

- We have policies
- We have outsourced IT
- We have cyber security tools
- We complete client questionnaires
- We have backups
- We pass audits

Having something in place and being able to evidence it are not the same thing.

WHAT HAS CHANGED?

Then vs Now

Historically - Regulators often asked:

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

Increasingly Today - The questions sound more like:

- How did you know there was an issue?
- What action was taken?
- Who made decisions?
- What evidence exists?
- What changed afterwards?

The focus has shifted from intention to evidence.

SHOW ME, DON'T TELL ME

The Regulatory Shift

Tell Me

- We review user access
- We have backups
- We monitor security
- Our supplier manages everything

  Show Me
- The last access review
- The last successful recovery test
- Evidence of monitoring
- How supplier performance is measured

The reality: the issue is rarely a lack of controls; it is evidencing they work as they were designed!

Show Me, Don't Tell Me in Practice

DPP Law (2025)

- Law firm fined £60,000 following a cyberattack exposing sensitive client information.
- An administrator account without MFA was used to gain access.
- The firm became aware of the issue when NCA notified them!
- The ICO found the firm had failed to implement appropriate security measures and delayed breach notification

The issue wasn't whether controls existed, but whether they were operating effectively.

Don't tell me security controls exist. Show me how you know they're working.

WHY GOOD FIRMS STILL GET CAUGHT OUT

Common Themes

- Policies Exist - But behaviour doesn't follow them.
- Controls Exist - But nobody checks they are operating.
- Suppliers Exist - But oversight is limited.
- Responsibilities Exist - But accountability is unclear.

Most compliance failures begin long before an incident occurs.

Cyber Security Thematic Review

What the SRA found

- The SRA reviewed firms that had experienced cyber incidents.
- Effective cyber security was found to be more than a technology issue.
- People, awareness and day-to-day practices were often the biggest vulnerability.
- Strong outcomes depended on behaviour, culture and operational discipline.

Compliance is demonstrated through operational behaviour, not simply documented control

THE VISIBILITY GAP

The Problem Isn't Always Risk - often it is visibility.

Typical Examples; a firm may have:

✅ Backups

But not know whether they are tested.

✅ Security tools

But not know what they are reporting.

✅ External suppliers

But not know how performance is measured.

✅ Compliance responsibilities

But not know who would lead during an incident.

THREE COMPLIANCE MYTHS

Myth 1: Compliance Means Having Policies

Reality:

- Policies support compliance.
- They do not prove it.

Myth 2: Compliance Means Passing Audits

Reality:

- Audits assess a point in time.
- Compliance is how the organisation operates every day.

Myth 3: Compliance Can Be Outsourced

Reality:

- Activities may be outsourced.
- Accountability cannot.

IF A REGULATOR ASKED TOMORROW...

Could You Show:

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

These questions often reveal more about compliance than a policy library ever could.

In a world that never standstill – could you recall your decision making from a cold Wednesday morning 6 weeks ago mid crisis?

THE REAL QUESTION

Compliance Is Not About Saying The Right Things

It's about demonstrating the right outcomes.

If the regulator walked into the business tomorrow, would you be relying on:

- Documents?
- Assumptions?
- Suppliers?

  Or
- Evidence?
- Visibility?
- Operational understanding?

KEY TAKEAWAYS

Remember: Compliance is not documentation; it is operational reality.

Most Firms Have Controls

The challenge is understanding whether they operate consistently.

The Biggest Risk: Often sits in the gaps between:

- People
- Processes
- Technology
- Suppliers

The New Compliance Question

"Can you show me?"

Not

"Can you tell me?"

Questions?

Secure your data.
Protect your business.
Defend against cyber threats.
Business resilience starts with us.

net-defence.com