

Could you prove it? Why governance matters when everything goes wrong

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**

Most law firms invest significant time and effort in compliance. Policies are reviewed, controls are implemented, risks are recorded, audits are completed. Yet when a significant incident occurs, regulators rarely begin by asking about policies. Instead, they focus on decision-making, accountability, oversight, and evidence.

The issue now is whether an organisation can demonstrate what happened. This is the question at the heart of the accompanying Could You Prove It? Governance & Regulatory Readiness Review, developed to help law firms assess whether their governance, accountability, and evidence arrangements would stand up to scrutiny when it matters most.

The assessment is not designed to determine whether a firm is compliant. Instead, it is intended to encourage meaningful discussion around the operational, governance, and reporting capabilities that enable organisations to demonstrate compliance when placed under pressure.

The compliance illusion

Most firms appear compliant during normal operations. Information is available, people are accessible, processes are familiar, and decisions can be made carefully.

The real test comes when something changes. A supplier fails. An operational issue disrupts service delivery. A cyber incident impacts systems. Client data may be at risk. Information becomes incomplete. Time becomes limited. Expectations increase.

This is often the point at which organisations discover the difference between having compliance arrangements and being able to demonstrate compliance.

Many firms have:

- Policies
- Procedures
- Certifications
- Technology
- External suppliers
- Audit records

And yet, many still struggle to answer fundamental questions when operating under pressure. The challenge is a lack of visibility, ownership, or evidence.

Compliance is not tested during audits.

Audits assess preparedness, incidents assess capability. That distinction matters. A firm may be able to demonstrate that:

- Policies exist
- Controls have been implemented
- Risks have been considered
- Reviews have been undertaken

However, regulators, clients and insurers are more interested in understanding:

- What happened?
- Who knew?
- Who decided?

- What evidence exists?
- What changed afterwards?

In many cases, those questions cannot be answered by opening a policy document. They are answered through governance, accountability, and operational resilience.

The boardroom test

Imagine a significant incident has occurred. Not necessarily a cyberattack, or a data breach. Simply a serious event capable of impacting the firm, its clients or its operations. Now imagine a regulator, insurer or key client asks to meet your leadership team.

How did you know?

- How was the issue identified?
- Who became aware first?
- How quickly was it escalated?
- Were the right people informed at the right time?

Who decided?

- Who took ownership?
- Who assessed the risk?
- Who authorised key decisions?
- Who determined whether reporting obligations were triggered?

How would you prove it?

- What records exist?
- What evidence has been retained?
- Months later, could the organisation demonstrate:
    - Actions taken?
    - Decisions made?
    - Reasons for those decisions?
    - Timelines of events?

What changed afterwards?

- What lessons were identified?
- What improvements were made?
- How were those improvements tracked?
- How would the firm demonstrate learning?

If different members of your leadership team would answer those questions differently, there may be gaps in governance, accountability, or evidence management that warrant further review.

Testing assumptions

The four questions within the Boardroom Test form the foundation of the accompanying Could You Prove It? Assessment. The assessment explores six areas that influence a firm's ability to demonstrate compliance:

- Visibility
- Governance & accountability
- Evidence & decision-making
- Regulatory readiness
- Supplier oversight
- Learning & improvement

The assessment is not intended to produce a pass or fail result. Its purpose is to help leadership teams challenge assumptions, identify potential blind spots, and assess whether governance arrangements are capable of supporting effective decision-making during periods of disruption. In many firms, the discussion generated by the assessment is more valuable than the score itself.

Compliance requires joined-up thinking.

One of the recurring themes in regulatory investigations is that issues rarely originate from a single failure. More often, they emerge where responsibilities overlap.

- Compliance assumes IT is managing the risk.
- IT assumes compliance is providing oversight.
- Cyber security tools generate alerts that never reach decision-makers.
- Operational teams are unaware of emerging technical risks.
- Suppliers hold information that leadership never sees.

The result is not usually a lack of controls; more likely it is a lack of visibility. This is why IT, cyber security, risk, and compliance can no longer operate as separate disciplines. When information remains siloed, organisations often struggle to answer the very questions regulators ask:

- How did you know?
- Who decided?
- What evidence exists?
- What changed afterwards?

Strong governance depends upon the ability to bring operational, technical, and compliance information together into a single, coherent picture.

Compliance is the product of operational resilience.

Many firms think of compliance as a destination. In reality, compliance is often the visible outcome of capabilities operating effectively across the business. These capabilities include:

- Effective IT support
- Cyber resilience
- Secure access management
- Business continuity planning

- Incident management
- Supplier oversight
- Leadership reporting
- Governance and accountability

When these capabilities are working together, compliance becomes easier to demonstrate. When they operate independently, organisations frequently struggle to maintain visibility, establish ownership, and provide evidence during periods of disruption. Put simply, compliance is the visible result of governance, technology and operational resilience working together.

The Visibility challenge

One of the biggest challenges facing law firm leaders, COLPs, and Practice Managers is obtaining a clear view of risk across the business. Information is often spread across:

- IT providers
- Cyber security platforms
- Incident records
- Supplier reports
- Risk registers
- Compliance documentation

And yet, regulators assess the organisation, not the individual systems that underpin it. This is why visibility has become such a critical component of modern governance. Without visibility, organisations struggle to:

- Identify emerging risks
- Make informed decisions
- Demonstrate oversight
- Evidence compliance

Turning information into assurance

The challenge for many firms is making sense of the available information. Leadership teams need meaningful information that supports decision-making, rather than disconnected reports from different systems and suppliers.

At Net-Defence, we developed The Signal to support this challenge by bringing together operational, cyber, and compliance-related information in a way that provides greater visibility and assurance. The goal is to help firms understand:

- What is happening?
- What requires attention?
- What decisions may need to be made?
- What evidence exists to support those decisions?

Because governance becomes significantly easier when leaders have access to clear, consistent, and meaningful information.

A different question

Most firms ask, ‘Are we compliant?’, But a more useful question may be: ‘Could we demonstrate compliance if our decisions were scrutinised tomorrow?’ Because compliance is rarely judged solely by the policies that exist. It is judged by the effectiveness of

the people, processes, and systems that support those policies when they are tested.

Strong compliance is often the result of:

- Good governance
- Effective IT support
- Cyber resilience
- Operational maturity
- Clear accountability
- Meaningful management information

When these capabilities work together, organisations are better positioned to understand and manage risk, respond effectively to disruption, and demonstrate compliance when it matters most.

Taking the next step

If the Boardroom Test has highlighted uncertainty in terms of visibility, accountability, evidence, regulatory readiness, supplier oversight, or organisational learning, then the accompanying Could You Prove It? Governance & Regulatory Readiness Review provides a practical framework to explore those areas in greater detail.

The objective is to understand whether your firm could confidently explain, evidence, and defend its decisions if subjected to scrutiny by regulators, insurers, clients or other stakeholders. More importantly, it encourages discussion between those responsible for compliance, governance, IT, cyber security, and operations.

Because effective compliance is rarely delivered by one department alone. It is the product of governance, technology, operational resilience, and accountability working together.

Final reflection

If your firm experienced a significant incident tomorrow:

- Would IT, cyber security, and compliance teams be working from the same information?
- Would leadership have the visibility needed to make informed decisions?
- Would you have the evidence required to demonstrate effective governance?
- Could you confidently answer the four questions in the Boardroom Test?

The accompanying assessment provides a starting point. The real value comes from the conversations it creates between leadership, compliance, IT, and cyber security teams, because when governance, technology, and operational resilience work together, demonstrating compliance becomes significantly easier. And ultimately, that's what *Could You Prove It?* is really asking.