NET-DEFENCE

The Role of COLPs & Managing Risk in Practice

Managed Service Offerings

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

net-defence.com

The Role of COLPs & Managing Risk in Practice

- Compliance expectations continue to grow.
- Evidence, visibility and accountability matter more than ever.
- Compliance is owned internally. Risk often lives elsewhere.

The challenge is demonstrating compliance when responsibility, authority and control sit in different parts of the business

What Actually Matters?

Four compliance pillars:

- Access & Identity
- Data Protection
- Resilience & Recovery
- Supplier Risk

Risk lives everywhere!

Who owns compliance in your firm?

- COLP
- Managing Partner
- Operations
- IT Provider/Department
- Everyone

There is no single correct answer, which is exactly the problem!

Compliance has an owner – what about risk?

Risk exists across:

- People
- Processes
- Technology
- Suppliers

Risk is everywhere, yet accountability usually sits with one of two people

Compliance has an owner – what about risk?

Risk exists across:

- People
- Processes
- Technology
- Suppliers

Risk is everywhere, yet accountability usually sits with one of two people

Why good firms still struggle

Most firms have:

- Policies
- Procedures
- IT providers
- Security Tools
- Certifications

Yet many firms still struggle to evidence compliance

The accountability gap

Responsibility Vs Accountability

Responsible for	Accountable for
Running Systems	Regulatory Compliance
Managing Users	Client Trust
Monitoring Threats	Risk Oversight
Operating Controls	Incident Outcomes

Activities can be delegated, accountability cannot!

The outsourcing myth

Can compliance be outsourced

Can be outsourced	Cannot be outsourced
IT Support	Regulatory Responsibility
Cyber Security	Governance
Cloud Hosting	Oversight
Monitoring	Accountability

A supplier or internal department can run the service;
the regulator will question and hold YOU accountable

The visibility gap

What don’t you know?

- When were backups last tested?
- When was access last reviewed?
- What risks has your supplier reported recently?
- How would you know if something failed today?

You can’t govern what you can’t see

The regulatory shift

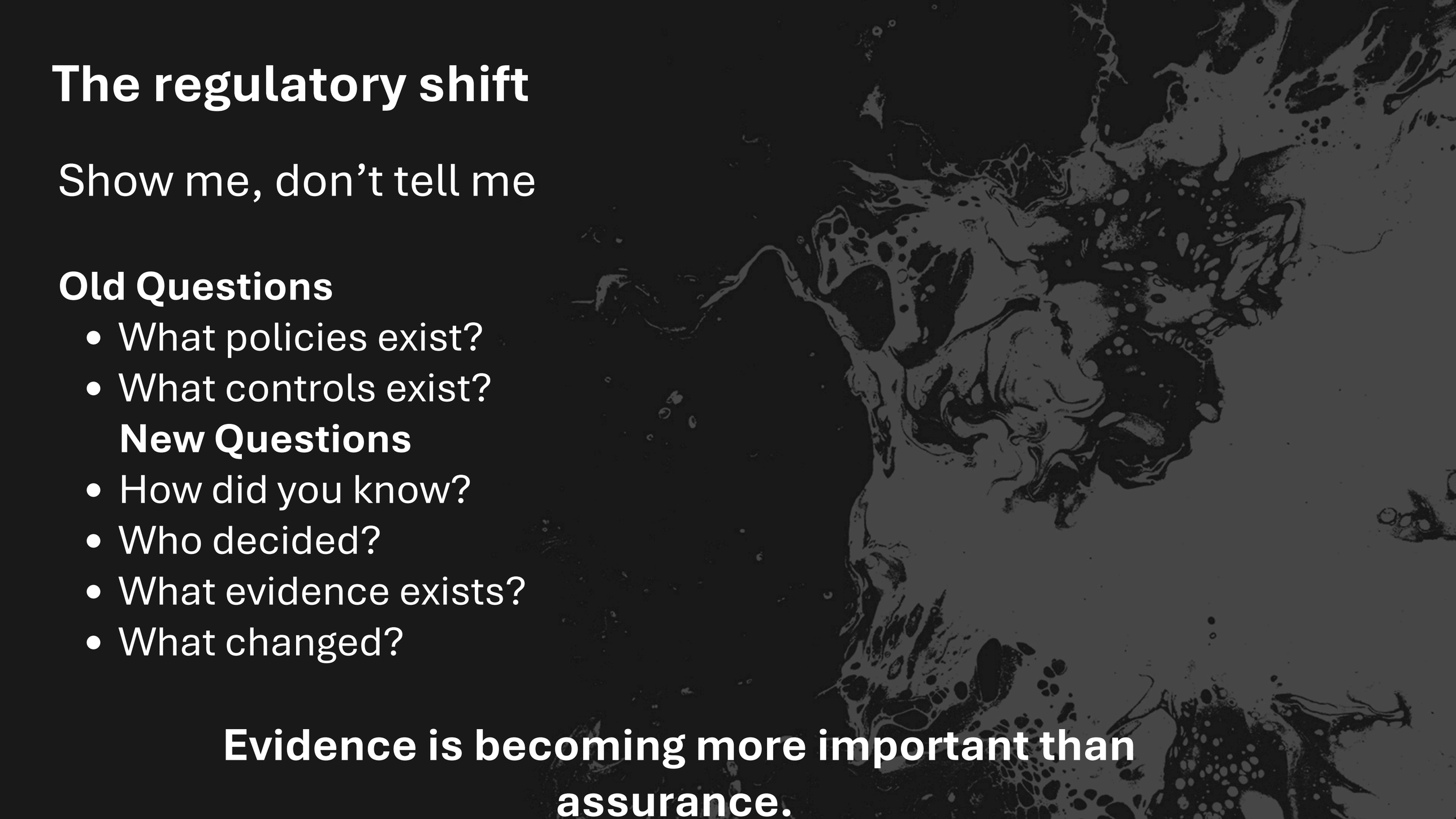
Show me, don’t tell me

Old Questions

- What policies exist?
- What controls exist?

New Questions

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



Evidence is becoming more important than assurance.

The regulatory shift

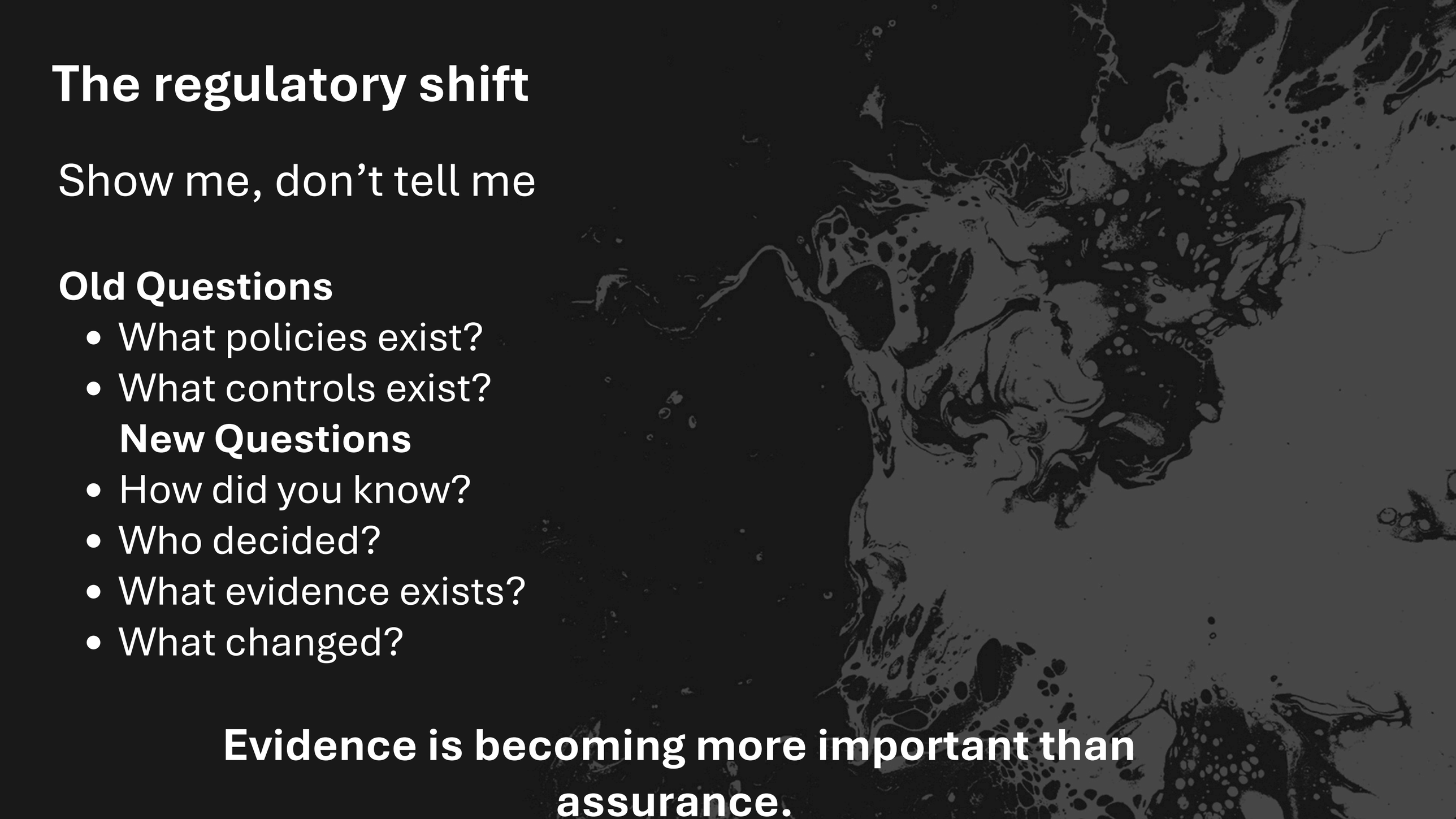
Show me, don’t tell me

Old Questions

- What policies exist?
- What controls exist?

New Questions

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



Evidence is becoming more important than assurance.

It’s Tuesday morning….

Show me, don’t tell me

A supplier reports suspicious activity.
Potential client data involved.
Questions:

- Who is leading?
- Who decides?
- Who informs clients?
- Who informs regulators?

Most firms believe they know, but have you tested it?

The accountability Test

- A Simple Exercise for COLPs, Partners and Compliance Leaders
- Most firms can identify who is responsible for compliance.
- Far fewer can clearly identify who controls the activities that support it.

Compliance risk often emerges when accountability sits in one place and operational control sits somewhere else.

The accountability Test

Who owns compliance?
Who controls systems?
Who leads incidents?
Who makes decisions?
Who provides evidence?

If answers vary across the business, compliance risk exists.

Three questions every COLP should ask

Before your next management meeting, ask these three questions.

How Would We Know?
How is risk detected?
Who sees issues first?
Who Would Decide?
Who leads?
Who escalates?

Three questions every COLP should ask

How Would We Prove It?
What evidence exists?
Could we demonstrate it months later?

These questions reveal more than any policy library

What good looks like

High-performing firms have:

- Clear ownership
- Defined decision making
- Supplier oversight
- Regular reporting
- Tested response plans
- Evidence-based governance

Good structures support great people and reduce risk

Compliance is an operational outcome

Compliance is delivered through:

- IT systems
- Cyber controls
- Operational processes
- Supplier management

The strongest firms view compliance as a business-wide discipline, not a compliance-team activity

Key Takeaways

- Compliance does not fail because people fail
- Responsibility and control are often disconnected
- Accountability remains with the firm
- Visibility is essential
- Evidence matters

Great people cannot succeed in bad structures

Webinar 3 – preview

The Regulator in the Room
Understanding the questions regulators ask and the evidence they expect to see when an incident occurs.

The 72-Hour Reality Check
A practical walkthrough of the critical decisions, actions and records required during the first 72 hours of a significant incident.

Testing Compliance Under Pressure
Discover whether your governance, accountability and evidence processes would stand up to real-world scrutiny when risk becomes reality.

Closing Question

If a regulator asked tomorrow:
How would you know?
Who would decide?
How would you prove it?

Those three questions are the foundation of modern compliance.

Questions?

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

net-defence.com