The Evidence Has Been There All Along

Enforcement actions are not isolated failures. Collectively, they are a map of where governance repeatedly falls behind change.

Opening illustration for Chapter 2: The Evidence Has Been There All Along.

EXECUTIVE INSIGHT

Regulatory enforcement actions are often studied as individual events: a particular institution, a specific control failure, a remediation programme and a financial penalty. Viewed collectively, however, they reveal something more valuable. Across jurisdictions and business models, regulators repeatedly identify the same underlying weaknesses: outdated assumptions, fragmented ownership, delayed escalation and governance that reacts after risk has already changed.

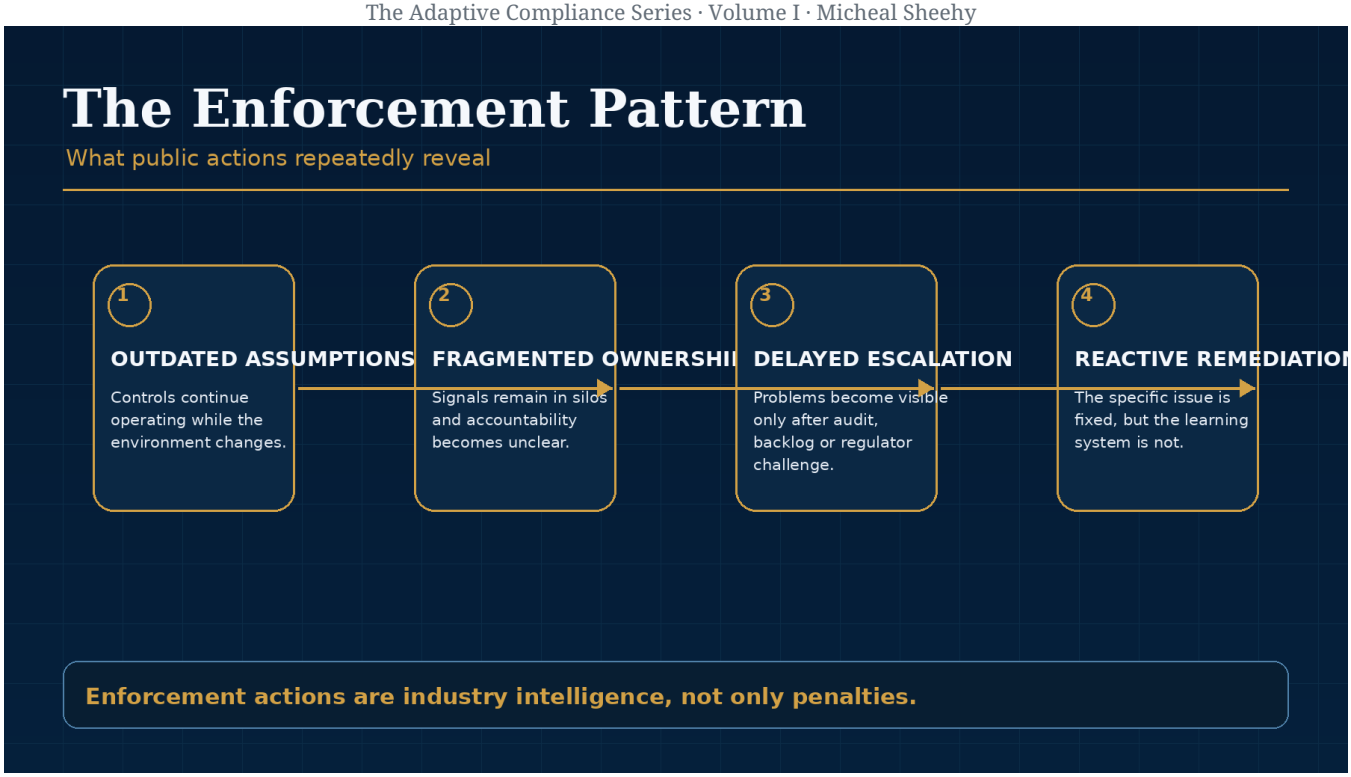

Figure 2.1: The Evidence Has Been There All Along - key framework.

Enforcement as Industry Intelligence

Consent orders, examination findings and public enforcement notices are among the richest sources of industry intelligence available to compliance leaders. They reveal not only what regulators considered deficient, but how supervisory expectations are evolving. Yet many organisations consume these actions defensively. They ask whether the same issue exists in their own programme, complete a gap assessment and implement a tactical enhancement. That is necessary, but it is not sufficient.

An enforcement action should be read as more than a story about another institution. It should be treated as a data point in a broader pattern. The names, products and jurisdictions vary, but the recurring themes are strikingly consistent. Regulators do not simply object to isolated procedural mistakes. They regularly identify governance systems that failed to recognise that the environment had changed around the controls.

This is why enforcement actions are particularly useful for adaptive compliance. They show where real institutions lost alignment between controls, assumptions and reality. They also show how long a weakness can persist when governance is periodic, fragmented or overly focused on operational metrics.

The Recurring Pattern

Across major public actions, the pattern is rarely that a financial institution had no controls at all. More often, controls existed but were not governed with sufficient curiosity. Transaction monitoring scenarios remained unchanged despite shifts in customer behaviour. Customer risk methodologies failed to reflect new markets, new products or new channels. Data limitations were known but tolerated. Backlogs signalled operational strain, but not necessarily the deeper issue of control

effectiveness. Governance committees received extensive information without a clear view of whether underlying assumptions remained valid.

The TD Bank resolution in 2024 drew particular attention to sustained weaknesses in transaction monitoring governance and coverage. The broader lesson for the industry was not only about one institution. It was that monitoring programmes can continue to operate while material categories of activity, scenario logic or assumptions remain insufficiently challenged over time. Similar lessons can be drawn from public actions involving institutions in Europe and Australia, where regulators repeatedly pointed to delayed remediation, inadequate monitoring, poor customer understanding or failure to escalate known problems quickly enough.

The facts differ, but the governance lesson is consistent: controls rarely fail in isolation. The more important failure is the absence of a mechanism capable of recognising that the design no longer matches the risk.

Regulatory Expectations Are Moving Toward Outcomes

This pattern aligns with the direction of global standard setters. FATF's methodology explicitly assesses both technical compliance and effectiveness. The Wolfsberg Group has similarly argued that true financial crime risk management is not only about complying with laws and regulations, but about delivering useful outcomes, supporting government priorities and establishing reasonable, risk-based controls. The direction of travel is clear: institutions must demonstrate that controls work in practice, not merely that controls exist in policy.

That shift matters because it changes the burden on governance. A programme cannot simply point to the existence of a model, a validation report or a committee structure. It must be able to explain why a control exists, what assumptions support it, how those assumptions are monitored, what changed during the period and how governance responded. Evidence of effectiveness becomes dynamic rather than static.

This does not mean regulators expect perfection. Financial crime is too complex and too adversarial for that. What regulators increasingly expect is evidence that institutions understand their risks, test their controls and learn from new information before weaknesses become systemic.

From Remediation to Learning

Traditional remediation asks how to fix the finding. Adaptive remediation asks what the weakness reveals about the organisation's broader ability to learn. If a regulator identifies an outdated scenario, the answer should not end with updating that scenario. The more important question is why change was not detected earlier, which signals were missed, whether similar assumptions exist elsewhere and how governance should be redesigned to identify the next change before an external party does.

This changes the value of enforcement analysis. The goal is not merely to avoid being the next institution named in a public action. The goal is to use the public record as a collective learning system. Enforcement actions show where the industry has struggled to convert information into timely governance. Adaptive organisations use those lessons to strengthen their own capacity to identify change early.

The evidence has been there all along. The question is whether the industry has been reading it as a checklist or as a map.

From Principle to Practice

Adaptive compliance requires a disciplined way to learn from the public record. Enforcement actions, supervisory speeches, advisories and thematic reviews should not be consumed as news. They should enter a repeatable regulatory intelligence process that converts external events into internal decisions.

The objective is not to remediate every headline. It is to identify recurring failure patterns, assess their relevance to the institution, map them to controls and produce evidence that the resulting action was completed and sustained.

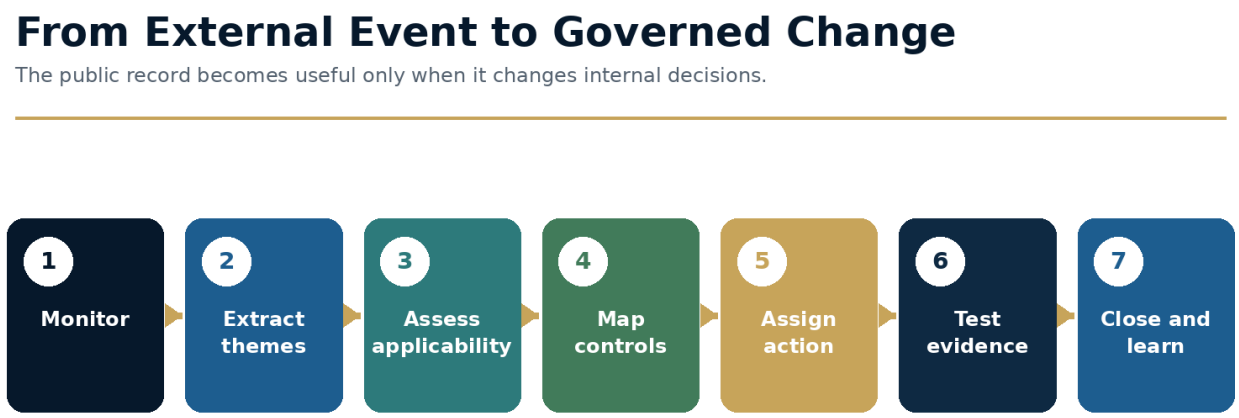

Figure 2.2 · From External Event to Governed Change

Step 1: Create a regulatory intelligence intake

The intake log should record the source, date, jurisdiction, business model, products involved, finding themes, root causes, customer or market relevance and the initial owner. A small central team can curate the information, but interpretation should involve legal, regulatory, product, operations and data specialists.

The value of the log emerges over time. When findings are coded consistently, the organization can see recurring themes such as weak data lineage, ineffective escalation, outdated risk assessments or delayed remediation rather than treating each action as unique.

Step 2: Separate applicability from severity

A severe enforcement action may have limited direct relevance to the institution; a modest action may expose a control weakness that is highly applicable. The assessment should therefore score both dimensions. It should also consider indirect applicability: the institution may not offer the same product, but may rely on the same data architecture, governance model or third party.

The conclusion should be recorded, approved and revisited if the theme recurs. A decision that no action is required is still a governance decision and should be supported by evidence.

Step 3: Close the loop with sustainable evidence

Remediation should not close when a policy is updated or a project milestone is marked complete. Closure evidence should show that the control was implemented, users were trained, data and systems changed where necessary, the control operates as intended and the underlying root cause is unlikely to recur.

Independent testing is particularly important where the lesson relates to governance weakness. The same management team that designed the response should not be the only source of assurance that the problem is solved.

Working Template

Root-cause category	Typical symptom	Appropriate response
Design gap	The control never addressed the relevant risk.	Redesign the framework or introduce a new control.
Execution gap	The control is sound but inconsistently performed.	Clarify procedure, capacity, training and quality assurance.
Data gap	Required information is missing, late or unreliable.	Fix lineage, validation, ownership and compensating controls.
Governance gap	Warning signals existed but did not trigger action.	Change thresholds, escalation rights, forum cadence or accountability.
Change-management gap	Business or regulatory change was not translated into controls.	Create formal impact assessment and implementation tracking.
Sustainability gap	Remediation was completed but not embedded.	Test outcomes, repeat performance and ownership after closure.

Regulatory Intelligence Applicability Matrix

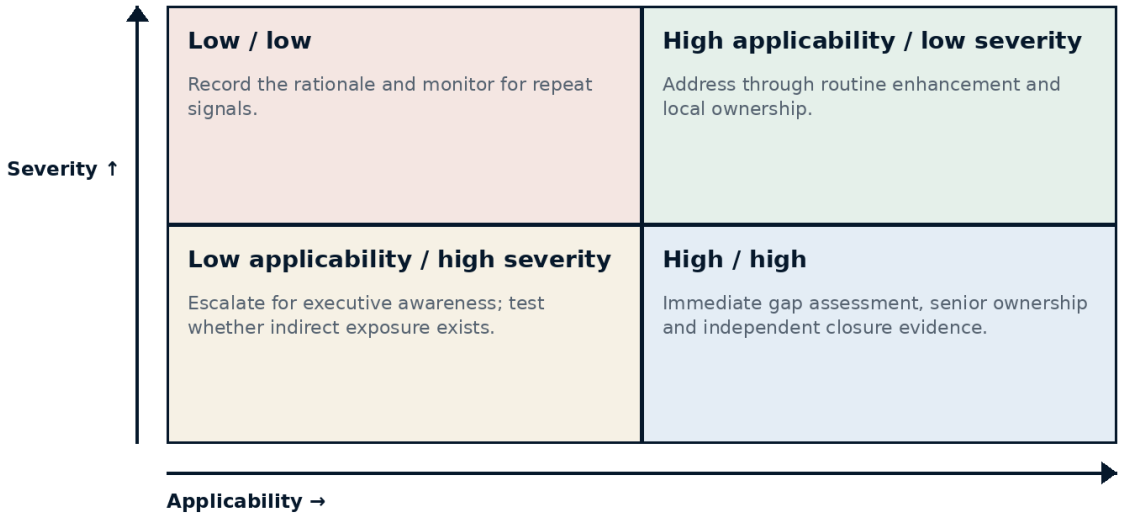

Figure 2.3 · Regulatory Intelligence Applicability Matrix

Decision Framework

Assessment question	Evidence to review	Output
Is the business model comparable?	Products, customers, channels and geography.	Direct, indirect or low applicability.
Could the same root cause exist here?	Data architecture, ownership, governance and third parties.	Control-map and gap hypothesis.
What is the potential consequence?	Regulatory, customer, financial and systemic impact.	Severity rating and escalation level.
What would prove the issue is absent or controlled?	Testing, metrics, documentation and expert challenge.	Evidence plan and accountable owner.

Executive Case Study

Turning enforcement into internal governance

A public enforcement action described static transaction-monitoring scenarios, weak escalation and delayed remediation. The institution reviewing the action did not have the same products or jurisdictional exposure, and an initial legal assessment concluded that the facts were not directly comparable.

Implementation

Instead of ending the review, the regulatory intelligence team coded the underlying themes. It identified three questions with broader relevance: whether scenario coverage changed with product growth, whether committee thresholds forced timely escalation, and whether remediation closure required evidence of sustained performance.

Governance

Those themes were mapped to the institution's own monitoring governance. The review found no equivalent misconduct, but it identified an escalation threshold that relied too heavily on backlog size and did not capture deteriorating model performance. The threshold was revised, a model-health indicator was added and the closure standard for material issues was strengthened.

Outcome and lesson

The case illustrates the purpose of regulatory intelligence. The institution did not copy another firm's remediation plan. It translated the root cause into its own operating context and used the public record to challenge assumptions before an examiner did.

Common Failure Modes

- Reviewing only the penalty and headline facts.
- Launching broad remediation without testing applicability.
- Using different root-cause language in every assessment.
- Closing actions on documentation rather than demonstrated operation.
- Failing to track repeated themes across regulators and markets.

A Practical 30 / 60 / 90-Day Plan

Period	Actions and evidence
First 30 days	Create the intake log and taxonomy; identify accountable owners; review the last twelve months of relevant public actions; select three recurring themes.
Days 31-60	Complete applicability assessments; map high-priority themes to controls; define evidence standards; establish a monthly regulatory intelligence forum.
Days 61-90	Implement the first control enhancements; independently test one closure; add recurrence and action-aging measures to executive reporting; publish lessons learned to product and regional teams.

> **Implementation checkpoint**
> At the end of the first ninety days, leadership should be able to point to at least one changed decision, one implemented control or governance improvement, and evidence that the result was tested. Activity alone is not proof of adaptation.

Executive Reflection

Regulators have repeatedly shown that the greatest weaknesses do not arise because institutions lack controls. They arise because controls, assumptions and governance fail to evolve together. Enforcement actions should therefore be read not simply as warnings, but as a collective blueprint for building organisations that adapt before external intervention becomes necessary.

Questions for Leaders

- When your organization reviews enforcement actions, does it identify only control gaps or also governance failure patterns?
- Which public regulatory findings have changed your internal assumptions in the last year?
- How would your board know whether remediation improved learning rather than simply closed an issue?
- What evidence proves your monitoring programme remains effective in practice rather than present in policy?