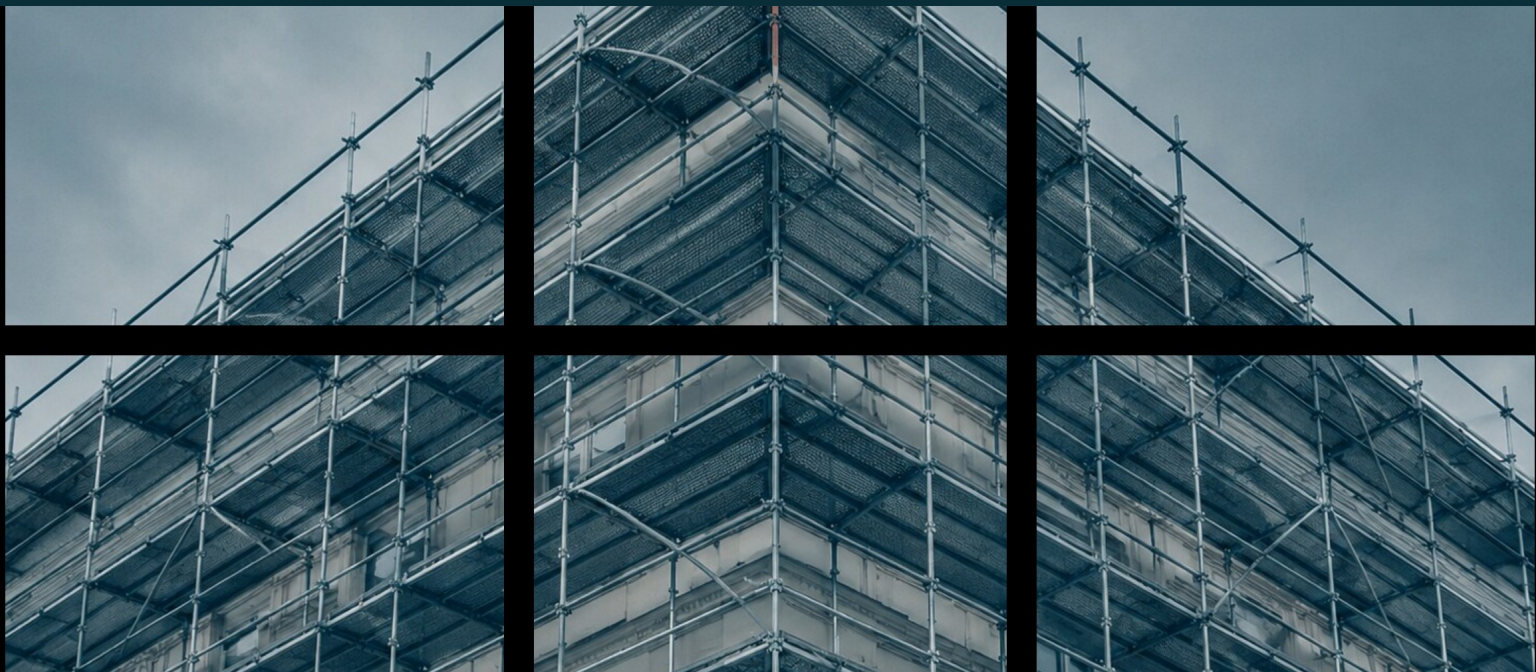


BEYOND COMPLIANCE BY FAITH

The Calculation Nobody Makes: Why Compliance Is Priced by Faith, Not by Economics

Compliance spending, non-compliance risk, and the comparison regulated organisations refuse to make



Giovanni Leonardi

March 2008

The Calculation Nobody Makes: Why Compliance Is Priced by Faith, Not by Economics

Transformation · No. 133

Originally written March 2008 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“Spend follows what can be shown, not what can be saved.”

1. The Meeting Where the Number Is Never Asked

The compliance budget is approved as the third item of a governance meeting that has already run twenty minutes over. A figure appears on the slide — larger than last year, as it is larger every year — and the committee nods it through. Someone remarks that the regulator's expectations keep climbing. Someone else notes that last year's programme is not quite finished. The number passes not because anyone has weighed it but because no one in the room is willing to be the person who argued for spending less on compliance. It carries on the strength of its own inevitability.

What never happens in that meeting is the one question that would give the figure any meaning: compared with what? We approve the cost of compliance in isolation, as an article of faith, and we almost never set it against the thing it is supposed to be buying down — the cost of non-compliance. The comparison that would turn a reflex into a decision is the calculation nobody makes.

I do not mean that firms spend too much, or too little. I mean something more awkward: that most regulated organisations have no defensible view of whether they are doing either, because they have never put the two numbers on the same page. And in the absence of that comparison they drift, reliably, to the worst of both outcomes — lavishing money on the compliance that is easiest to see while starving the compliance that would actually save them.

2. Two Ledgers in Different Currencies

The reason the comparison is so rarely made is not that the arithmetic is hard. It is that the two sides of it are kept in different currencies, on different time horizons, owned by different people.

The cost of compliance is a hard number. It is budgeted, present, and precise to the pound: the compliance headcount, the external attestation fee, the licence for the monitoring system, the programme to implement the latest rulebook. It has an owner — the compliance or risk function — whose job is to defend and grow it.

The cost of non-compliance is a soft number. It is probabilistic, deferred, and owned by no one: a fine that may or may not land, a remediation that may or may not be ordered, a past-business review whose scope is unknowable until a regulator sets it, a loss of authorisation nobody will price because pricing it feels like inviting it. It lives in the future tense and in the passive voice.

Setting a hard present cost against a soft future one requires somebody to convert the second into the same terms as the first and then own the comparison. Almost no one is ever asked to. So the hard number wins by default — not because it is more important, but because it is the only one on the table.

3. Why the Question Feels Forbidden

There is a deeper reason the calculation goes unmade, and it is worth naming plainly, because it is cultural rather than technical.

- Naming the price of getting caught feels like licensing the offence. To say out loud "the expected cost of this control gap is four hundred thousand pounds" sounds, in a governance forum, uncomfortably close to "and therefore we might accept it." The number itself becomes taboo, so it is never spoken, and an exposure that could have been ranked and managed is instead left unexamined.
- We buy compliance as insurance against blame, not only against loss. A great deal of what is approved in that meeting protects the people approving it as much as the organisation they serve. An unquantified "we did everything a reasonable firm would do" is personally safer than a defensible "we invested where the risk was greatest and consciously accepted residual risk elsewhere" — even though the second is the more honest, and usually the more protective, position.
- Visibility is mistaken for value. The controls that are easiest to evidence — the binders, the sign-offs, the attestations — are the ones that reassure an auditor, so they attract the money. The controls that would actually prevent the damaging event are often unglamorous, buried in operations, and invisible to anyone not looking for them. Spend follows what can be shown, not what can be saved.

The result of these three forces together is a peculiar kind of failure: not negligence, but misdirection. The firm is busy, diligent, well-audited — and exposed in precisely the place no one was incentivised to look.

The organisations that are caught out are rarely the ones that spent too little on compliance. They are the ones that spent almost the right amount on almost exactly the wrong things.

4. A Composite From the Wrong Side of a Remediation

Let me make this concrete, because the argument is too easy to nod along with in the abstract. Consider a composite that will be recognisable to anyone who has sat on the wrong side of a remediation programme.

A mid-tier lender spends a little over four million pounds a year on its compliance function. The single largest line, close to a million and a half, goes on the annual documentation and testing of its financial controls in the style the post-Enron world now demands: the process narratives, the control matrices, the evidence files assembled for external attestation. The work is diligent, it is auditable, and almost none of it changes a decision anyone makes. It exists to be shown.

Meanwhile, an operations manager has for three consecutive years requested ninety thousand pounds to automate a reconciliation between two settlement systems that are currently married up by hand. Each year the request is deferred as "not this year's priority." Each year the manual workaround holds — until the year it does not, and a discrepancy opens in exactly that gap. The remediation, the past-business review, the skilled-person report the regulator commissions, and the customer redress together run to something well north of three million pounds, before anyone counts the management time or the supervisory attention the firm has now permanently earned.

Where the money went	Annual cost	What it bought
Control documentation and attestation	~£1.5m	Auditability; reassurance; no change in outcomes
Deferred reconciliation control	£0 (declined)	A £3m+ remediation and a supervisory relationship

The firm was not under-spending on compliance. It was spending close to the right amount on close to the wrong things — because it had priced its compliance by visibility and comfort rather than by exposure. Ninety thousand pounds of unglamorous prevention lost, every year, to a million and a half pounds of highly visible reassurance. No one made a bad decision. No one made the comparison at all.

5. But Some Things You Simply Must Do

The strongest objection to everything above deserves to be stated at full strength, not waved away. It runs like this: some obligations are absolute. You do not perform a cost-benefit analysis on whether to prevent money laundering or to safeguard client money; the duty is categorical, the law is not optional, and the very habit of asking "what would it cost us if we didn't?" is the corner-cutting mindset that produced the last decade's scandals in the first place. On this view, compliance economics is not just distasteful; it is dangerous.

It is a serious argument, and it is half right. There are bright lines that must never become line items — obligations you meet because they are obligations, full stop. But notice what the objection quietly assumes: that the alternative to explicit calculation is principled non-calculation. It is not. The alternative, as the composite shows, is implicit calculation — pricing by neglect. The firm that never asks the question is not honouring every duty equally; it is triaging by accident, funding whatever is most visible and starving whatever is quietest, and calling the result principle.

“Every organisation already prices its compliance. The only real question is whether it does so on purpose.”

Making the calculation is not the same as deciding to breach. It is the discipline of directing finite money and attention to where they buy down the most real exposure — which is the opposite of corner-cutting, because it takes prevention seriously enough to fund it where it matters rather than where it shows.

6. The Calculation, Made on Purpose

None of this requires a grand model or a new risk-quantification cult. What it requires is the willingness to hold both ledgers open at once and rank honestly. In practice that means a handful of unglamorous habits.

1. For the small number of genuinely material exposures — the ones that could draw a fine, a remediation, or a loss of permission — form an explicit view of likelihood and consequence, however rough. A defensible range beats a reverent silence.
2. Set the marginal cost of the control that would move each exposure against the reduction it buys, and rank by risk reduced per pound — not by how well the control shows up in an audit file.
3. Say out loud what is being accepted, and by whom. Residual risk that is named and owned is governed; residual risk that is merely unfunded is just an accident waiting for a date.

This is not a heavier process. In most firms it is a lighter one, because it gives permission to stop gold-plating the visible controls that passed the point of doing any good long ago, and to move that money to the exposures that have been quietly waiting three years for ninety thousand pounds.

The pressure to make this shift is only going to grow. The environment is tightening; the scrutiny of cost is sharper this year than last, and every function is being asked to show that its spend does something. Compliance will not be exempt from that question for much longer, and "the regulator expects it" will not, on its own, remain an answer. The firms that come through best will be the ones that learned to make the calculation nobody makes — not so they can spend less on compliance, though many will, but so that what they do spend is finally pointed at the thing they were always afraid of, rather than at the thing that was easiest to show the auditor.