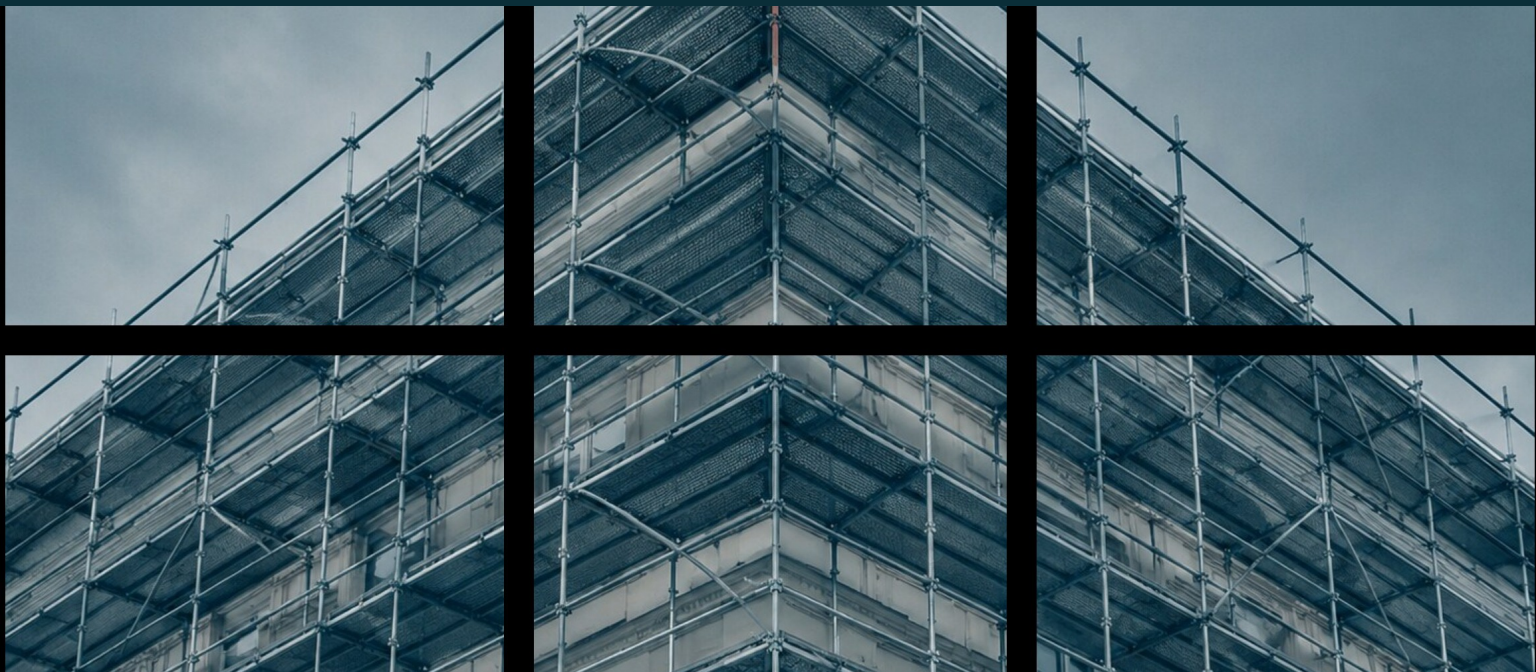


BEYOND DEMONSTRABLE COMPLIANCE

The Compliance Paradox: Why the Function Built to Enforce Change Ends Up Preventing It

How regulated organisations mistake demonstrability for safety – and freeze themselves in the name of control



Giovanni Leonardi

June 2006

The Compliance Paradox: Why the Function Built to Enforce Change Ends Up Preventing It

Transformation · No. 89

Originally written June 2006 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“It has bought the appearance of safety at the price of the very thing that makes an institution genuinely safe.”

1. The Programme That Was Never Voted Down

The programme was not voted down. That is the part worth remembering. There was no dramatic meeting where a sponsor lost their nerve or a budget was pulled at the last moment. The transformation — a genuinely sensible reworking of how the firm handled a core process — simply slowed, month by month, until it stopped being a transformation and became a standing agenda item. Each proposed change was, quite reasonably, referred to the control owners. Each control owner, quite reasonably, asked for the change to be documented, risk-assessed, and tested before it could be signed off. By the time the paperwork for the first phase was complete, the business case that justified the second had expired.

Nobody in that room was wrong. Every individual decision was defensible, several were admirable, and not one of them could have been overturned on its merits. That is precisely the problem I want to examine, because it is the signature of a paradox sitting at the centre of every regulated organisation I have watched try to change itself: the machinery built to satisfy the regulator's demand for change becomes, over time, the most reliable obstacle to it.

2. What the Regulator Asked For, and What We Built

State the paradox plainly. Regulators in our sector do not ask organisations to stand still. Read the substance of what has landed on us these past few years — the tightening of internal-control expectations in the wake of the accounting scandals, the documentation demands that came bound up with them, the operational-risk requirements now working their way through the banks — and the through-line is a demand to change: to remediate, to strengthen, to reform how the work is actually done. The regulator wants a different organisation at the end of it.

What the organisation builds in response is not a different organisation. It is a compliance apparatus. And a compliance apparatus, left to the logic of its own incentives, optimises for something that is not change and is frequently its enemy: demonstrability.

A regulator asks for a safer organisation. What it can inspect is a documented one. The gap between those two things is where the paradox lives.

The substitution happens through a chain worth walking slowly, because each link in it is individually rational.

- The regulator mandates an outcome — better control, sound remediation, a culture that manages risk rather than hides it.
- The organisation cannot hand an examiner an outcome. It can only hand over evidence, so it builds to produce evidence: policies, procedures, control matrices, attestations, testing regimes.
- Evidence rewards what holds still. A process unchanged since it was documented is easy to attest; a process in flight is a moving target that generates findings and exceptions.
- The apparatus therefore develops a quiet institutional preference for freezing the organisation into a documented, defensible steady state. Change is reclassified, in practice if never in policy, as a source of risk to be suppressed.
- And so the regulation that began by demanding change produces a function that resists it — not through obstruction, but through the ordinary operation of its own incentives.

This is not a story about lazy or timid compliance officers. The best ones I have worked alongside understood the paradox perfectly well and disliked it more than anyone. It is a story about what an organisation measures and therefore gets. Reward a function for the completeness of its documentation and the cleanliness of its findings, and you should not be surprised when that function comes to prefer a firm that does not move.

Consider a single, ordinary improvement — the kind that ought to be the lifeblood of a well-run operation. A team wants to simplify a handoff between two processing steps that everyone agrees is clumsy. Eight weeks of work, on the face of it. But the handoff sits inside a documented control chain. Changing it means re-testing the forty-odd linked controls that reference it, refreshing three procedure documents, and securing fresh attestation from each affected owner. None of this is unreasonable in isolation. Together they turn an eight-week improvement into an eight-month one — and the next team, watching from across the floor, quietly decides that the clumsy handoff is not worth the trouble. Multiply that one decision across a firm and you have an organisation that has learned, without ever deciding to, that the safest available action is to do nothing at all.

*“The most compliant organisation and the least adaptable one
are, disturbingly often, the same organisation.”*

3. The Objection That Deserves Its Strongest Form

Here an honest version of this argument has to slow down, because there is a serious objection and it deserves its best statement rather than a caricature.

The objection runs like this. In a regulated sector the asymmetry of outcomes is brutal. A slow change costs weeks; an unmanaged one can cost a mis-selling remediation, a data breach, a regulatory censure, a place in the newspapers your chairman reads before you do. Against that asymmetry, friction is not a defect — it is the discipline that keeps the firm solvent and out of the enforcement column. A practitioner who grumbles about the control framework's drag is really grumbling about the seatbelt, and will keep grumbling

right up to the moment it saves them. Better a transformation that arrives late than a headline that arrives early.

I have made a version of that argument myself, and I do not think it foolish. But it rests on an assumption that does not survive contact with the evidence: that the friction is actually buying safety. Very often it is not. It is buying demonstrability, and the two come apart far more easily than the objection allows.

A control environment can be fully documented, exhaustively attested, and comprehensively evidenced, and still be fragile — because all of that energy went into proving that last year's controls operate rather than asking whether they still address this year's risk. Ossification is not safety. A framework frozen for the convenience of the auditor is safe against the exposure it was written for and blind to the one forming quietly outside its scope. Real safety in a regulated firm has never come from stillness; it comes from the capacity to see a new risk and adapt to it before it matures. An organisation that has traded its adaptability for demonstrability has not bought safety at the price of speed. It has bought the appearance of safety at the price of the very thing that makes an institution genuinely safe.

So the trade-off the objection presents — safety against change — is largely false. The real choice is between a control environment that can move and one that cannot, and only one of those is safe in any sense a regulator should actually care about.

4. A Different Kind of Compliance

If the paradox is not solved by less compliance — and it is not, because the regulator will not permit it and should not — then it is solved by a different kind of compliance. The practical work, in my experience, comes down to prising apart two things the apparatus habitually fuses.

1. Separate assurance from evidence. "Is this change safe?" and "can we prove this control operated?" are different questions, and the apparatus answers the second while behaving as though it has answered the first. Assurance is a judgement about risk; evidence is a record of process. Design them as separate disciplines and a change can be assured quickly even while its evidentiary paperwork takes its ordinary, unhurried course.
2. Express controls as outcomes, not procedures. A control written as a frozen sequence of steps is invalidated the instant the process improves. A control written as the outcome it must guarantee — this reconciliation is complete, this approval is genuinely independent — survives the process changing underneath it. Outcome-expressed controls are change-tolerant by construction; procedure-expressed controls are change-hostile by construction. Most of the drag I have described comes from firms choosing, without ever noticing they are choosing, the second.
3. Bring compliance to the front of change, as co-designer, not to the end, as gate. A function that meets a change only at the approval gate can do nothing but slow it or stop it. The same function, engaged while the change is still being shaped, can design the assurance in — so the change arrives already controllable. The gate manufactures friction; the partnership manufactures safe change. It is the same people and the same rigour; only the timing has moved.
4. Measure the function on safe change delivered, not on documentation held. This is the hardest of the four and the most important. As long as compliance is rewarded for the stability of its evidence and the tidiness of its findings, it will prefer a firm that

does not move. Reward it instead for the organisation's ability to change without incident, and you have quietly aligned it with the outcome the regulator wanted from the very beginning.

None of this is a relaxation of control. It is a redirection of it — away from the stillness that is easy to inspect and towards the adaptability that is hard to inspect but is the actual point of the exercise. The regulated organisation that will come through the next decade in good order is not the one with the thickest manual or the cleanest attestation file. It is the one that has made its controls able to move as fast as its risks do.

The paradox is not a law of nature. It is the predictable result of measuring a function for the wrong thing, and it loosens the moment we measure it for the right one. The regulator asked for an organisation that could change safely. The quiet tragedy of the compliance paradox is how often, in labouring to give the regulator precisely that, we construct the one thing that cannot.