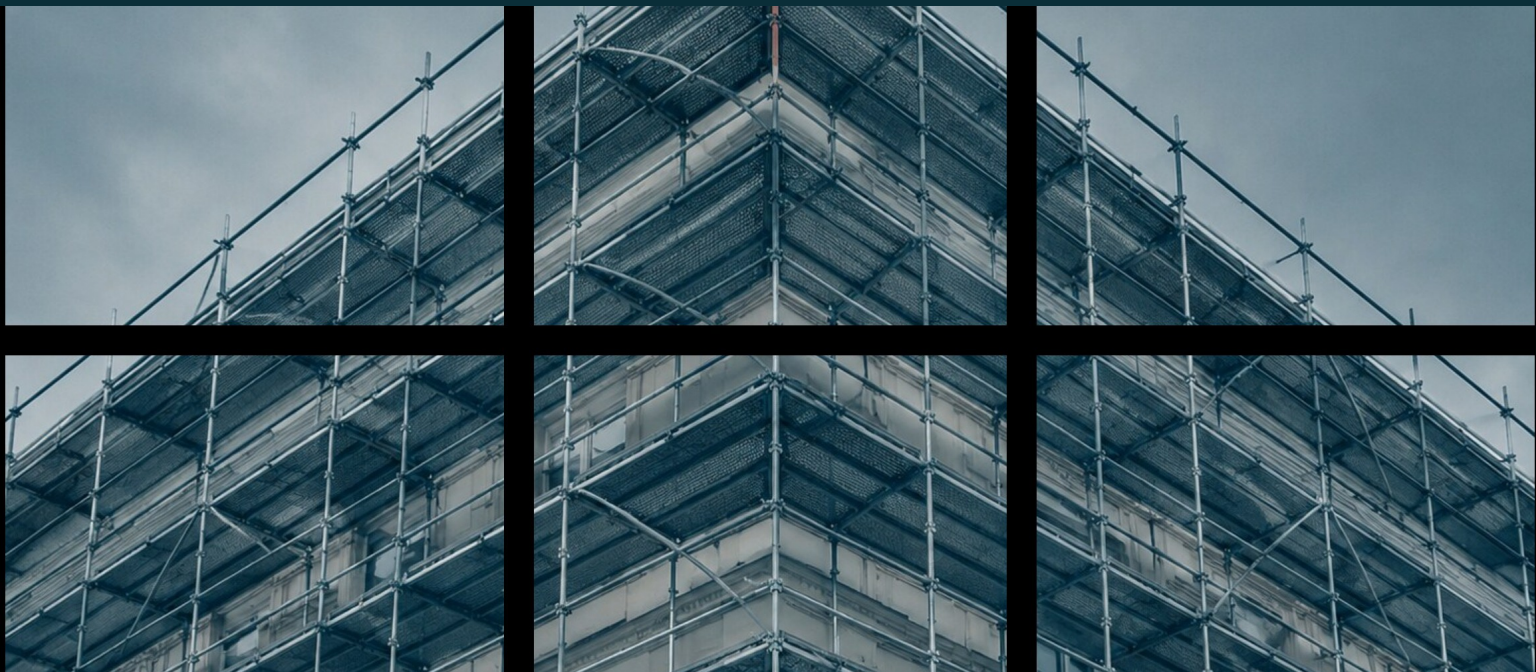


BEYOND INSPECTION

The Second Line Arrives Too Late: Why Risk and Compliance Should Design the Change, Not Just Inspect It

How regulated organisations turn their risk and compliance functions from late-stage inspectors into design partners — without surrendering the independence that makes them worth having.



Giovanni Leonardi

August 2007

The Second Line Arrives Too Late: Why Risk and Compliance Should Design the Change, Not Just Inspect It

Transformation · No. 149

Originally written August 2007 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“The function that first sees the design at the final gate is not more independent than one that helped shape it – it is merely less useful, and no less accountable when the breach it never had the chance to prevent finally surfaces.”

1. The veto at the eleventh hour

Eleven weeks before go-live, at the final gate review of a programme that had been running for the better part of two years, the compliance lead raised her hand and said the one word the room had spent those two years quietly arranging never to hear. No. The new authorisation workflow, she explained, would let the same user both raise a payment and approve it above the sign-off threshold – a segregation-of-duties conflict that an auditor would find in an afternoon and the regulator would find rather less amusing than we did. She was right. She had also seen the design for the first time that morning.

The fix cost a little over four hundred thousand pounds and pushed go-live into the following quarter, because the authorisation logic was woven through the new finance platform rather than sitting on top of it. Had she been in the room at the start, the same rule would have been a line in a requirements document – a morning's analysis, not a re-architecture. Nobody in that programme had set out to exclude her. We had simply built the whole enterprise, with the best intentions in the world, so that she would arrive last.

I have sat through enough of these gate reviews to know that the scene is not an accident and not a one-off. It is the predictable output of how we position risk and compliance in times of change. We cast the second line as the brake – the business prevention department, the people whose job is to find the reason you cannot do the thing you have already decided to do. And then we are surprised, and a little aggrieved, when that is exactly what they do.

The textbooks, and the model of three lines of defence that risk managers have lately begun to talk about, get the important half of this right: the function that assures the business must be independent of the business it assures. That is not in dispute here. What the textbooks leave out is the harder truth sitting next to it – that independence practised as distance turns the second line into an auditor of failure rather than a partner in success, and that the cost of the distance lands not on the compliance department but on the programme, the balance sheet, and eventually the customer.

“Independence practised as distance turns the second line into an auditor of failure rather than a partner in success.”

2. Why we keep them out of the room

If late, adversarial engagement were merely a mistake, it would have corrected itself long ago. It persists because the structures around it reward it. Four forces hold it in place:

- The incentives are asymmetric. A second-line function is judged on the breaches it catches and, more sharply, on the ones it misses. It is almost never judged on the programmes it helped to land. Given that scorecard, standing back and inspecting is the rational posture; getting involved early is unpaid risk.
- The timing is inverted. Risk and compliance are typically invited at the gate, not at the drawing board — asked to assure decisions that have already been taken, budgets already committed, architectures already chosen. By then the only moves left are to bless or to block. We hand them a binary and then complain that they are binary.
- Independence has been misread as arm's length. The build-out of compliance headcount that followed Sarbanes-Oxley gave many organisations a large checking layer bolted onto the side of the business. Somewhere in that expansion, independent quietly came to mean at a distance. They are not the same word, and the confusion is expensive.
- There is no shared language. The programme speaks in milestones, benefits and critical paths; the second line speaks in likelihood, exposure and control. Each hears the other as obstruction because neither has learned to translate. A control requirement sounds like a delay; a delivery deadline sounds like a corner about to be cut.

3. The objection that keeps them out

There is a serious argument for the distance, and it deserves to be stated at its strongest rather than waved away. It runs like this. The entire value of a second line is that it can look at what the business has built and judge it without fear or favour. If the same people help design the change, they cannot then objectively assess it — they are marking their own homework. Separation of duties is the oldest control we possess; the Turnbull guidance, the whole post-Sarbanes edifice, rests on the assurer being separate from the assured. A compliance function that has been co-opted into the delivery it is meant to police is worse than an absent one, because it launders risk with a signature and calls it assurance.

That objection is real, and anyone who dismisses it has not understood what the second line is for. But it conflates two things that are not the same: designing the control environment and owning the business decision. Partnership is not ownership. A second line that helps shape how a change will be controlled, while retaining the standing authority to escalate and to withhold its sign-off, has not been captured. It has been informed.

Capture, when it happens, comes from dependency and incentive — a function that reports into the very executive whose programme it is meant to challenge, or whose

bonus rides on the go-live date. It does not come from proximity and timing. The safeguard against capture is structural: a reporting line that runs to the board or the audit committee rather than to the programme, and a preserved right to say that the residual risk is unacceptable. That safeguard is not weakened one iota by the second line having been in the room since month one. The function that first sees the design at the final gate is not more independent than one that helped shape it — it is merely less useful, and no less accountable when the breach it never had the chance to prevent finally surfaces.

Dimension	The second line as inspector	The second line as design partner
When it engages	At the gate, once the options have closed	In the design authority, while the options are still open
What it can do	Bless or block	Shape the control environment before it sets
How its independence is protected	By keeping its distance	By its reporting line and its standing right to escalate
What it optimises for	Breaches caught late	Breaches never designed in

4. Control by design, not by inspection

The alternative to inspection is not laxity; it is design. The control requirements that a programme will eventually be judged against — the segregation-of-duties rules, the audit trail, the data-handling obligations under the Data Protection Act, the customer-outcome tests that principles-based regulation now expects us to be able to evidence — are constraints on the target operating model as real as throughput or cost. They are also far cheaper to honour on a whiteboard than in production code.

This is the mechanism the "brake" framing hides. The cost of a control does not stay flat as a programme runs; it climbs by an order of magnitude at each stage it is introduced. A rule captured at design is a sentence in a specification. The same rule caught in build is a configuration change. Caught in test — as our payment conflict was — it is a re-architecture and a slipped quarter. Discovered after go-live, it is an incident, a remediation programme, and a difficult letter to the regulator. Bringing the second line to the drawing board moves every control leftward along that curve, to the point where honouring it is nearly free.

Control by design means treating the second line's requirements as design inputs, not late findings. A control is cheapest to build when it is still a sentence in a specification and most expensive when it is already an incident.

There is a second thing the second line carries that the delivery team lacks: intelligence. They know what the regulator is actually exercised about this year — the scramble to be ready for the new markets-in-financial-instruments regime, the tightening expectations on anti-money-laundering checks, the shift from box-ticking rules to demonstrable fair treatment of customers. They know where peer organisations have been burned, and how a broad principle will be read in practice when it meets a real process. That knowledge is worth a great deal before the design sets and almost nothing after it. Engaging them late does not merely raise the cost of the controls; it forfeits the very insight that would have

shaped a better design in the first place.

5. What partnership actually requires

None of this happens by goodwill or a warmer relationship. It takes a small number of deliberate disciplines, and each of them is designed to buy involvement without spending independence.

1. Embed on design; separate on judgement. The second line sits in the design authority and shapes the control environment as the change is built — but its formal sign-off is given, or withheld, through its own reporting line, not the programme's. Involvement in the how is not the same as a vote on the whether.
2. Preserve the veto, and make it rare. The right to say no must survive intact; a partnership that cannot end in refusal is a capture. But a second line that has been in the room from the start rarely needs the dramatic late no. The single catastrophic veto becomes a series of small redesigns that no one outside the programme ever notices.
3. Build literacy in both directions. Give risk and compliance people enough delivery literacy to read a critical path and know what a slipped dependency costs; give programme managers enough control literacy to understand why a requirement exists rather than merely that it does. Most of the friction between the two lines is a translation failure wearing the costume of a disagreement.
4. Measure them, at least in part, on what they enable. As long as the second line's scorecard counts only breaches caught, the incentive to stand back and wait will never die. Some portion of how we judge these functions has to reward the transformation they helped to deliver safely, not only the disasters they intercepted.

The functions we now call the second line were built to protect the organisation from itself, and after the compliance build-out of recent years, almost none of us are short of them. What we are short of is the willingness to stop treating independence and involvement as opposites. The organisations that come through this era of near-permanent change with their controls and their credibility intact will not be the ones with the largest compliance departments. They will be the ones that learned to put the second line at the drawing board — because the most valuable work it will ever do is not the no at the gate, but the quiet redesign that makes the no unnecessary.