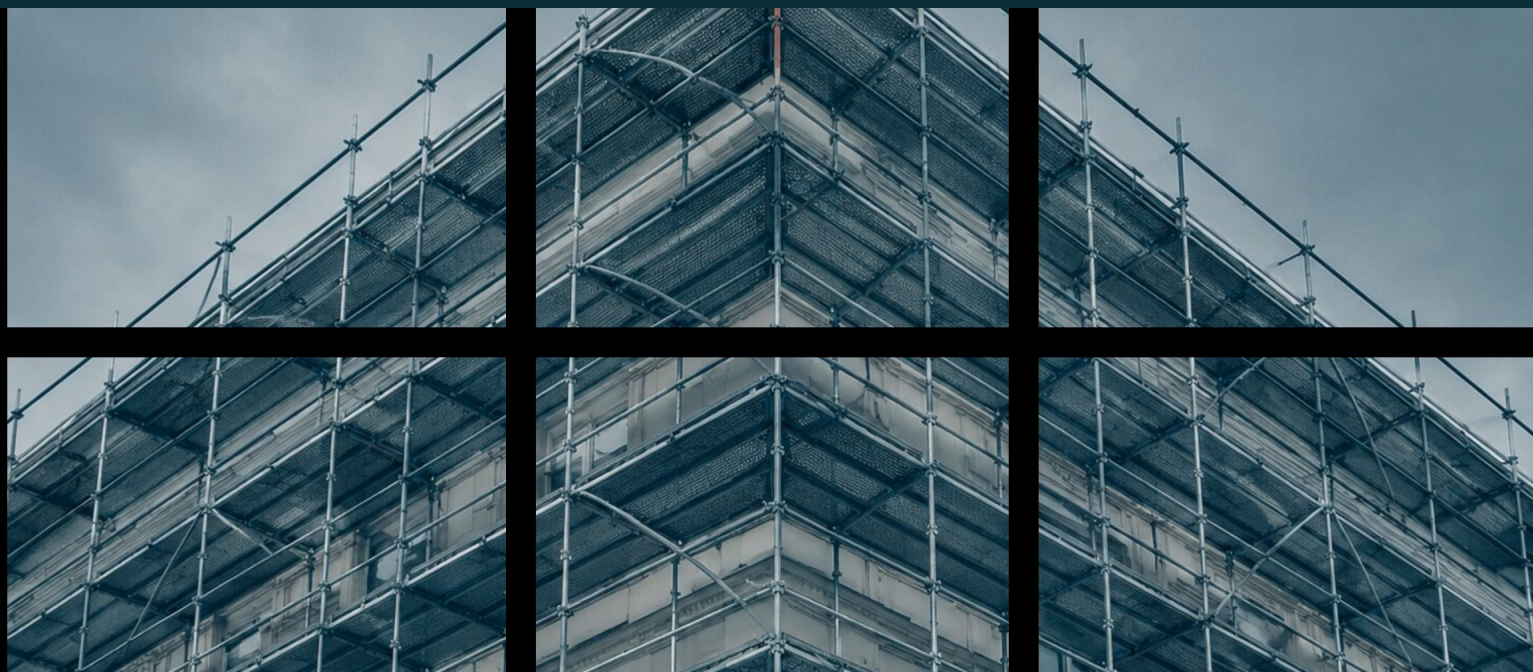


BEYOND THE SECOND LINE

Risk and Compliance Functions as Transformation Partners — The Alliance That Neither Side Knows How to Build

A Practitioner's Perspective on Bridging the Structural Divide Between Second-Line
Defence and Organisational Change



Giovanni Leonardi

September 2007

Risk and Compliance Functions as Transformation Partners – The Alliance That Neither Side Knows How to Build

Transformation · No. 156

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

“The transformation leader who treats the compliance function as an obstacle to be managed rather than a partner to be engaged is building on foundations that will not hold.”

1. Two Functions, One Problem, No Shared Language

There is a structural paradox at the heart of most large organisations that rarely receives the attention it deserves. The risk and compliance functions exist to ensure the organisation operates within its regulatory and risk boundaries. The transformation function exists to change how the organisation operates. Both are concerned with the same underlying question – is the organisation fit for purpose? – yet they approach it from opposing directions, using different vocabularies, different governance frameworks, and different definitions of success.

The result is a relationship that is, at best, transactional and, at worst, adversarial. Transformation leaders view compliance teams as gatekeepers who slow things down, impose unnecessary controls, and lack commercial awareness. Compliance professionals view transformation leaders as risk-blind optimists who underestimate the consequences of getting it wrong, move too fast for proper assurance, and treat regulatory requirements as afterthoughts. Both characterisations contain enough truth to be self-reinforcing, and neither side has sufficient incentive to bridge the gap.

This essay argues that this division is not inevitable. It is a product of organisational design choices that can be changed – but only if both functions are willing to rethink what they are for.

2. The Roots of the Divide

The separation between risk and compliance on one side and transformation on the other is not accidental. It reflects a deliberate organisational design principle: the second line of defence must be independent of the first line in order to provide credible assurance. This principle is sound, and nothing in this argument seeks to undermine it. The problem is not independence itself but the way independence has been interpreted and institutionalised.

In most organisations, independence has been implemented as separation. The compliance function operates in a parallel governance structure, with its own reporting lines, its own committees, its own language, and its own priorities. It interacts with the business – and with transformation programmes – primarily through formal mechanisms: policy reviews, risk assessments, regulatory impact analyses, and assurance checkpoints. These mechanisms are necessary, but they are also inherently backward-looking and

binary. They ask "Does this comply?" rather than "How can this be designed to comply better?"

The transformation function, meanwhile, has developed its own governance apparatus — programme boards, design authorities, change advisory boards — that is oriented toward delivery and decision-making speed. Compliance input is sought at prescribed stages (typically at inception and before go-live) but is rarely integrated into the ongoing design and delivery process. The compliance function reviews; it does not co-create.

This pattern has persisted because it serves both sides' institutional interests. The compliance function preserves its independence and its authority to say no. The transformation function preserves its agility and its freedom to design solutions without being constrained by what it perceives as excessive caution. Neither side recognises that their mutual isolation is making both of their jobs harder.

3. What the Isolation Costs

The costs of this separation are substantial, though they are often invisible because they are distributed across multiple programmes and multiple risk categories.

Late compliance discoveries. The most obvious cost is the regulatory issue that surfaces late in the programme lifecycle — after the architecture has been set, the design has been approved, and significant investment has been committed. Late compliance discoveries are expensive to remediate, disruptive to programme timelines, and damaging to the relationship between the two functions. They reinforce the transformation leader's view that compliance is an obstacle and the compliance professional's view that transformation teams do not take regulatory requirements seriously enough.

Defensive over-engineering. When compliance input arrives late or is perceived as unpredictable, programme teams respond by building in excessive margins of safety — additional controls, redundant processes, conservative design choices that satisfy the worst-case interpretation of regulatory requirements. This defensive over-engineering adds cost and complexity without adding proportionate risk reduction, because it is driven by uncertainty about what the compliance function will require rather than by a shared understanding of the actual risk.

Missed opportunities for risk reduction. Transformation programmes routinely redesign processes, replace systems, and restructure operating models. Each of these changes is an opportunity to address known risk and compliance weaknesses — manual controls that could be automated, data quality issues that could be resolved, reporting gaps that could be closed. When the compliance function is not engaged in the design process, these opportunities pass unrealised. The organisation invests in transformation and emerges with the same risk profile it started with, having failed to capture the risk-reduction benefits that were available at marginal cost.

Assurance theatre. In the absence of genuine partnership, both functions default to formal assurance mechanisms that create the appearance of rigour without its substance. The programme team produces compliance documentation that satisfies the checklist; the compliance function reviews it and signs off. Neither side is confident that the documentation reflects reality, but both are satisfied that the process has been followed. This is assurance theatre — the ritualised performance of governance without the genuine engagement that governance is supposed to provide.

4. What Partnership Would Actually Look Like

If the current model is separation dressed as independence, what would genuine partnership look like without compromising the compliance function's assurance role?

The answer begins with a distinction that is rarely made explicit: the difference between the compliance function's assurance role and its advisory role. The assurance role is the one that requires independence — the right to assess, to challenge, and to escalate. This role is non-negotiable and should not be diluted. The advisory role, however, is different. It involves bringing regulatory expertise to bear on design decisions, helping programme teams understand the intent behind regulatory requirements (not just their letter), and identifying where compliance objectives and transformation objectives can be served by the same design choices.

Most compliance functions conflate these two roles, treating every interaction with the business as an exercise of assurance authority. This is understandable — the assurance role is the one that carries institutional weight and professional prestige — but it is counterproductive. A compliance professional who is advising a programme team on how to design a process that meets regulatory requirements is not compromising their independence. They are exercising their expertise in a way that makes the eventual assurance assessment more likely to succeed.

In practice, partnership means several things.

Compliance professionals embedded in programme teams. Not as auditors, but as design partners who bring regulatory expertise to the table during the design process rather than after it. This requires compliance professionals who understand programme delivery — its rhythms, its constraints, its decision-making processes — and programme leaders who value regulatory expertise as a design input rather than resenting it as a design constraint.

Shared risk and compliance objectives in the programme business case. If the programme is going to change the systems and processes that the compliance function cares about, the business case should capture the compliance benefits alongside the operational benefits. This is not about inflating the business case; it is about ensuring that the programme is designed to deliver compliance improvements that would otherwise require separate investment.

Joint governance at the design stage, not just the assurance stage. The compliance function should have a seat at the design authority, not just the programme board. This allows regulatory considerations to be factored into design decisions as they are made, rather than being surfaced retrospectively through formal reviews.

A shared language for risk. One of the most persistent barriers to partnership is that the two functions use different risk vocabularies. The compliance function talks about regulatory risk, conduct risk, and compliance breaches. The transformation function talks about delivery risk, benefit realisation risk, and operational readiness. These are not different risks — they are different perspectives on the same risks. A shared risk taxonomy, developed jointly, can bridge this gap and enable more productive conversations about trade-offs.

5. Why This Matters Now

The regulatory environment is intensifying. Across financial services, energy, telecommunications, and healthcare, the volume, complexity, and pace of regulatory

change are increasing. Organisations are running more regulatory programmes, in parallel, with shorter timelines and higher stakes. The old model — in which compliance and transformation operate in separate lanes and interact through formal checkpoints — is increasingly unsustainable. It produces late discoveries, defensive design, and assurance theatre at a scale that the organisation can no longer afford.

At the same time, transformation programmes are becoming more complex and more consequential. They are touching core systems, core processes, and core data assets. The risk of getting the compliance dimension wrong is growing, and the cost of late remediation is escalating. Organisations that continue to treat risk and compliance as a separate conversation from transformation are accumulating risk in precisely the areas where they can least afford it.

The organisations that will navigate this environment most effectively are the ones that recognise what the current model obscures: that the compliance function and the transformation function are trying to solve the same problem from different angles, and that the gap between them is not a necessary consequence of independence but a failure of organisational imagination.

The transformation leader who treats the compliance function as an obstacle to be managed rather than a partner to be engaged is building on foundations that will not hold. The compliance professional who treats transformation as someone else's problem until it arrives for review is abdicating a responsibility that the regulator will ultimately hold them to. The way forward is not for either function to subsume the other, but for both to recognise that their effectiveness depends on the quality of the relationship between them — and to invest in that relationship with the same seriousness they invest in their own capabilities.