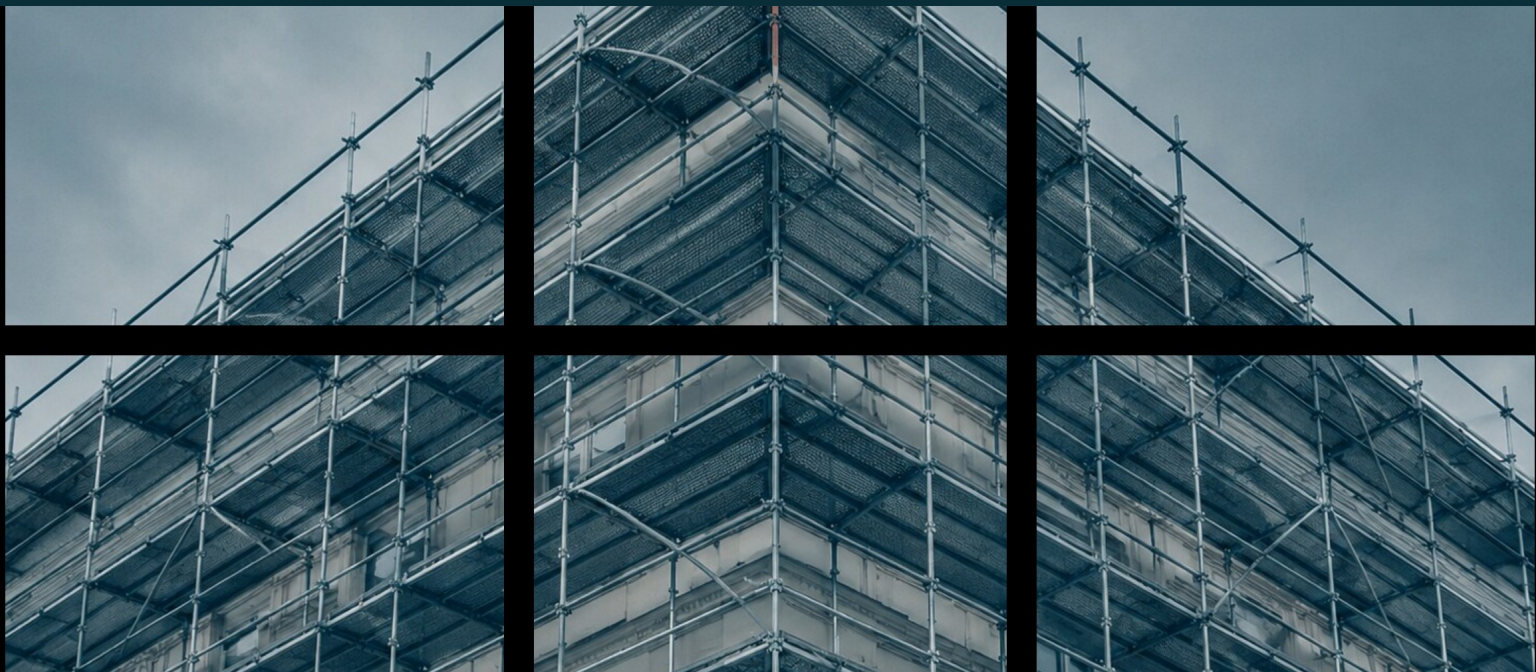


BEYOND THE BOLT-ON

Compliance by Design Versus Compliance by Retrofit — Why Most Organisations Choose Wrong

A Practitioner's Perspective on Regulatory Integration in Regulated Industries



Giovanni Leonardi

January 2007

Compliance by Design Versus Compliance by Retrofit – Why Most Organisations Choose Wrong

Transformation · No. 122

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

“The organisations that treat compliance as a design constraint from the outset do not spend less on compliance – they spend less on failure.”

The Default Position

In my experience, the overwhelming majority of organisations facing a new regulatory obligation begin from the same place: they look at what they already have and ask how it can be made compliant. This is the retrofit instinct – the assumption that the existing architecture of processes, systems, and governance is fundamentally sound and merely needs adjustment. It is an understandable instinct. It is also, in most cases, the wrong one.

The alternative – designing compliance into the operating model from the outset – is rarely chosen, and when it is, it is usually chosen late, after the retrofit has already failed. The pattern I have observed across multiple regulatory programmes is remarkably consistent: an initial conviction that the change is containable, followed by a gradual and painful discovery that it is not.

Why Retrofit Feels Right

The appeal of retrofit is not irrational. It promises continuity. It suggests that the disruption can be bounded – that the regulatory requirement is an addendum to the existing way of working rather than a challenge to it. For senior leadership, retrofit carries a comforting implication: we are already mostly there.

This is reinforced by the way compliance programmes are typically funded. A retrofit can be scoped as a discrete project with a defined budget and timeline. A design-led approach, by contrast, implies a more fundamental rethink – one that is harder to cost, harder to govern, and harder to explain to a board that wants certainty.

The retrofit instinct is not a failure of intelligence. It is a failure of diagnosis – a systematic underestimation of how deeply a regulatory requirement reaches into the operating model.

There is also a political dimension. Retrofit allows the existing owners of processes and systems to retain control. A compliance-by-design approach often implies that the current way of working is inadequate, which is an uncomfortable message for the people who built it.

What Retrofit Actually Costs

The pattern that recurs across complex regulatory programmes is this: the retrofit begins confidently, encounters resistance from the underlying architecture, and then enters a prolonged phase of workarounds, exceptions, and manual interventions. Each workaround introduces operational risk. Each exception requires its own governance. The result is a compliance layer that sits uneasily on top of the operating model, maintained through effort rather than design.

The organisations that treat compliance as a design constraint from the outset do not spend less on compliance — they spend less on failure. They spend less on the rework that follows a retrofit that could not hold. They spend less on the operational risk that accumulates when compliance depends on human discipline rather than structural enforcement.

I have seen organisations spend eighteen months retrofitting a regulatory reporting capability onto legacy data architectures, only to discover that the data quality problems that made the retrofit necessary in the first place also made the reports unreliable. The retrofit succeeded technically — the reports were produced — but failed substantively. The data could not be trusted, and the organisation found itself in the uncomfortable position of being compliant in form but not in substance.

The Design Alternative

Compliance by design does not mean starting from scratch. It means starting from the regulatory requirement and working backwards into the operating model, rather than starting from the operating model and working forwards to the requirement. The difference is directional, not necessarily revolutionary.

In practice, this means three things:

- Treating the regulation as a design input, not a constraint to be managed. The requirement shapes the target architecture rather than being accommodated within the existing one.
- Accepting that some existing capabilities will need to be replaced, not adapted. This is the hardest organisational conversation, because it challenges the sunk-cost logic that protects legacy investments.
- Building compliance into process design rather than layering it on top. A compliant process should not require a separate compliance check — the check should be inherent in the way the process works.

None of this is conceptually difficult. The difficulty is organisational. It requires leaders who are willing to acknowledge that the current state is not a viable foundation, and it requires programme structures that can hold a broader scope without losing control.

The Real Choice

The choice between design and retrofit is rarely presented as a choice. It is usually made implicitly, in the early days of a programme, when the scope is being defined and the approach is being set. By the time the limitations of retrofit become apparent, the programme is committed — politically, financially, and contractually.

The practitioner's honest observation is this: most organisations choose retrofit not because they have assessed the alternatives and found retrofit superior, but because retrofit is the path of least organisational resistance. It does not require anyone to admit that the current state is inadequate. It does not require a broader conversation about operating model design. It does not challenge existing ownership structures.

But the regulatory environment is not static. Each new obligation adds weight to the compliance layer, and a retrofitted compliance architecture becomes progressively harder to maintain. The organisations that will navigate the next decade of regulatory change most effectively are those that learn to treat each new requirement not as something to be bolted on, but as an opportunity to improve the underlying design.

The question is not whether compliance by design is better — in my experience, it almost always is. The question is whether organisations can overcome the structural incentives that make retrofit the default.