

The Operating Model Is the Risk Control

Risk is rarely created by a single action. Much of it is created by what the structure allows.

Mohamad M. Burjak

For much of my career, I believed what most institutions believe: that if a risk exists, the answer is a control. Another approval. Another review. Another committee. Another signature. Another line in the procedure.

The logic seemed sound. Regulators asked for controls; auditors tested them; risk committees reviewed them. Every incident appeared to justify adding one more. And so the register grew.

What took me far longer to understand is that many of the most serious losses I witnessed in more than three decades of banking did not come from the absence of a control. They came from the design of the work itself — not only from what people did, but from what the structure allowed them to do. Operational risk has several sources — people, processes, systems, and external events — and the design of the operating model shapes how each of them can turn into a loss.

Every institution I worked in kept extensive inventories of controls: reviewed, tested, documented, reported. Most were accurate about what existed. Far fewer were honest about where the exposure actually lived — because risk is often created long before any control is exercised.

In trade finance, the outcome is often shaped before the first approval is granted. It is shaped by where authority sits. By who owns a decision, and who is permitted to challenge it. By whether the specialist examining an instrument reports independently, or to the business line that profits from its issuance. By whether a technically unsound clause can pass because those reviewing it understand legal drafting but not the professional requirements of the instrument itself. By whether responsibility is concentrated in one clear place, or quietly dispersed across departments until no one fully owns the result.

None of this appears in a control register. Much of it decides whether a loss becomes possible.

I remember transactions in which every required approval existed. Every policy had been followed. Every signature obtained. Every control had, technically, worked — and the institution remained exposed. The failure belonged to no individual. It belonged to the operating model. Authority had been fragmented, responsibilities had overlapped, and

ownership had dissolved somewhere between departments. Each participant completed his own task correctly. The weakness lived in the design that connected those tasks. No additional approval would have prevented it, because the problem was never a missing checkpoint. The problem was the path itself.

This is why institutions so often respond to incidents in ways that reassure without protecting. A loss occurs. A new approval is added. A new committee is formed. A new mandatory field appears in the system. The register lengthens; the operating model stays much as it was. The organisation grows slower, more expensive, more elaborate — but not necessarily safer. Complexity is mistaken for control. Delay is mistaken for prudence. Neither is reliably true.

The most effective controls rarely appear on a dashboard. A well-designed operating model works quietly and continuously. Segregation of duties built into the workflow does not depend on anyone remembering to apply it. A system that removes the opportunity for the wrong action is stronger than one that merely warns against it. A structure that keeps conflicting responsibilities from ever converging offers protection no single signature can replicate. Such controls are easy to overlook precisely because they leave little behind: many of the incidents they prevent never occur, and so never appear in any report.

Looking back, I no longer believe the safest institutions are those with the longest lists of controls. They are the ones whose operating models make the wrong decision difficult, the dangerous decision visible, and the unacceptable decision as nearly impossible as design can make it.

Controls may prevent, detect, or help correct problems; the operating model determines where those controls sit and how effectively they work. Good design can remove or reduce the opportunity for error before any control is exercised — not the only way to prevent a loss, but the one that does not depend on anyone remembering to act.

And that changes the question worth asking. Not "What controls do we have?" but "What does our structure make possible?"

Risk control was never only something added to an operation after the fact. Much of it was always embedded in the design of the operation itself.

The strongest control in any institution is the one no one has to remember to apply.