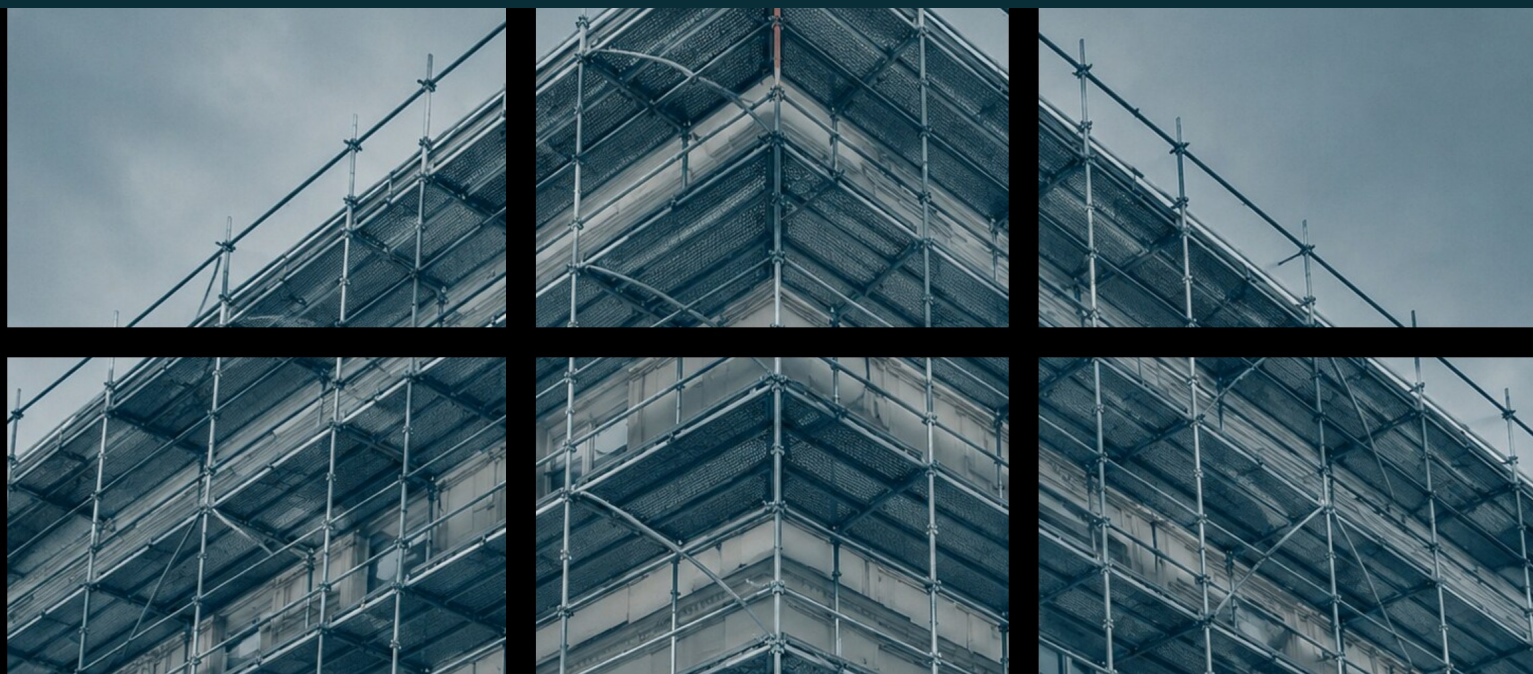


BEYOND THE RISK REGISTER

Risk Registers Without Risk Thinking — Why Transformation Programmes Treat Risk Management as a Compliance Exercise

A Practitioner's Perspective on the Gap Between Risk Process and Risk Intelligence in Programme Delivery



Giovanni Leonardi

June 2002

Risk Registers Without Risk Thinking — Why Transformation Programmes Treat Risk Management as a Compliance Exercise

Transformation · No. 42

Originally written June 2002 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“The risk register has become the place where uncomfortable truths go to be documented and then systematically ignored.”

1. The Ritual of the Risk Register

Every transformation programme of any scale maintains a risk register. It is one of the few artefacts that programme governance universally demands. Auditors expect it. Steering committees review it. Programme managers update it. The Turnbull Report elevated it to a board-level concern. Risk management, by any measure, has never been more prominent in the governance of change.

And yet the pattern I have observed across dozens of programmes, in multiple sectors, over the past several years is one of profound dysfunction. The risk register exists. It is maintained. It is presented at every governance forum. But it does not, in most organisations, drive decision-making. It does not change behaviour. It does not prevent the failures it catalogues. It has become, in the most precise sense, a tick-box exercise — a process that satisfies the requirement for risk management without delivering risk intelligence.

This is not a failing of individual programme managers. It is a structural problem, and understanding why it persists is essential if we are to close the gap between risk process and risk thinking.

2. What a Risk Register Actually Does

The standard risk register is a simple artefact. It lists identified risks, assigns them a probability and impact score, calculates a composite rating, names an owner, and records a mitigation action. At each governance review, the register is updated: risks are re-scored, mitigations are reported as on track or delayed, and new risks are added. The register provides a snapshot of the programme's risk landscape at a point in time.

This sounds reasonable. The problem is that almost every element of this process is compromised by incentives that work against honest risk identification and assessment.

Identification is filtered. The risks that appear on the register are not a complete inventory of what could go wrong. They are the risks that the programme team is willing to surface — which means they are filtered through political sensitivity, career self-interest, and the programme manager's assessment of what the steering committee can tolerate. The risks that would genuinely change the programme's direction — the ones that challenge the business case, question the sponsor's assumptions, or suggest the programme should not have been approved — rarely appear.

Scoring is performative. The probability-times-impact matrix that produces the red-amber-green heat map is treated as though it were a rigorous quantitative assessment. It is nothing of the kind. It is a subjective judgement, made by people who have strong incentives to keep risks in the amber zone — high enough to demonstrate awareness, low enough to avoid triggering intervention. The result is a register where everything clusters in the middle, and the colour coding communicates nothing meaningful about relative severity.

Mitigation is aspirational. The mitigation actions recorded against each risk are frequently statements of intent rather than operational plans. "Engage stakeholders early" is not a mitigation. "Implement robust testing" is not a mitigation. These are descriptions of things the programme should be doing anyway, relabelled as risk responses. The register creates the appearance of active risk management while the actual risks remain unaddressed.

3. The Structural Forces

The tick-box pattern persists not because programme managers are negligent, but because the organisational system rewards it. Three structural forces are particularly powerful.

3.1 The governance incentive

Steering committees and programme boards are, in theory, the mechanism by which risks are escalated and addressed. In practice, they are performance forums where programme managers present a narrative of controlled progress. A risk register full of red-rated items does not signal effective risk management — it signals a programme in trouble. Programme managers learn very quickly that the way to survive governance scrutiny is to present a register that shows risks being identified and managed, not one that shows risks that are genuinely threatening the programme's viability.

The perverse result is that the governance mechanism designed to surface risk becomes the mechanism that suppresses it. The steering committee sees what the programme manager wants it to see, and both sides maintain the fiction that this constitutes oversight.

3.2 The accountability gap

Risk ownership, as practised in most programme environments, is an administrative assignment rather than a genuine delegation of authority. A risk owner is named on the register, but they typically lack the budget, the authority, or the organisational leverage to implement the mitigation they are notionally responsible for. They update the register because they are required to. They do not manage the risk because they cannot.

This is compounded by the fact that risk ownership is almost always assigned within the programme team. The risks that matter most — those that originate in the wider organisation, in strategic decisions made above the programme, in dependencies on other programmes or business units — cannot be owned by anyone inside the programme. They sit on the register as acknowledged but unmanaged, a category that the standard risk process has no honest way to represent.

3.3 The cultural default

There is a deeper cultural force at work, particularly visible in large organisations with strong compliance traditions. Risk management has been absorbed into the compliance apparatus. It is treated as a requirement to be satisfied rather than a capability to be developed. The question that drives risk management practice is not "what could go wrong and how do we prevent it?" but "can we demonstrate that we have a risk management process?"

The Turnbull Report, published three years ago, attempted to shift this by framing internal control as a means of managing risk rather than merely reporting on it. But the implementation of Turnbull in most organisations has followed the familiar compliance trajectory: the requirement has been met, the process has been established, and the underlying culture has not changed.

The risk register has become the place where uncomfortable truths go to be documented and then systematically ignored.

4. What Risk Thinking Would Actually Look Like

The contrast between risk management as currently practised and genuine risk thinking is stark.

Risk thinking starts not with a register but with a question: what are the assumptions on which this programme's success depends, and which of them are most likely to be wrong? This is a fundamentally different starting point from "what are the risks we can identify?" because it directs attention to the foundations of the programme rather than to the events that might disrupt it.

In my experience, the assumptions that destroy transformation programmes are rarely the ones that appear on the risk register. They are embedded in the business case — assumptions about benefits realisation, about organisational readiness, about the stability of the strategic context, about the willingness of senior leaders to sustain commitment over a multi-year horizon. These assumptions are not risks in the conventional sense. They are the premises on which the entire programme rests, and when they prove false, no amount of mitigation planning can save the outcome.

Risk thinking also requires a different relationship with uncertainty. The standard risk process treats uncertainty as something to be eliminated through identification and mitigation. Risk thinking treats uncertainty as a permanent condition to be navigated. The difference is between a programme that tries to predict and prevent every failure, and one that builds the adaptive capacity to respond when the unpredicted failure arrives.

“The programmes that survive are not the ones with the most comprehensive risk registers. They are the ones that have built the organisational muscle to respond when the risk register turns out to be wrong.”

5. The Enron Lesson That Applies Here

The corporate governance crisis triggered by Enron's collapse last year has focused attention on financial controls and audit independence, and rightly so. But there is a lesson from Enron that applies directly to programme risk management, and it is this: the presence of a risk management process is not evidence that risks are being managed.

Enron had risk management. It had policies, frameworks, committees, and reports. What it did not have was a culture in which risk information flowed honestly to the people who needed it, in which uncomfortable conclusions were acted upon rather than reclassified, in which the process served decision-making rather than the appearance of decision-making.

The parallel with programme risk management is uncomfortable but exact. Most transformation programmes have risk processes. Very few have risk cultures. The register exists. The thinking does not.

6. What Would Need to Change

Closing the gap between risk process and risk thinking requires changes that go well beyond improving the risk register template.

It requires steering committees that treat a clean risk register with suspicion rather than satisfaction — that ask not "are the risks managed?" but "what risks are we not seeing?" It requires programme managers who are rewarded for honest risk escalation rather than punished for it. It requires risk ownership that comes with genuine authority, not just a line on a spreadsheet. And it requires a shift in the fundamental purpose of risk management from demonstrating compliance to informing decisions.

None of these changes is technically difficult. All of them are organisationally demanding, because they challenge the incentive structures that currently make tick-box risk management the rational choice for everyone involved.

The question is whether the current governance climate — with its new emphasis on accountability, transparency, and the consequences of inadequate oversight — will be enough to force the shift. The early signs are not encouraging. The instinct across most organisations is to respond to the governance crisis by adding more process, more reporting, more compliance machinery. This will produce better-documented risk registers. It will not produce better risk thinking.

And it is risk thinking, not risk process, that determines whether a transformation programme succeeds or fails.