ANALYSIS & OPINION · GOVERNANCE, RISK & HUMAN FACTORS

The Blind Spot at the Top

A practical reckoning with governance, oversight, decision rights, and accountability.

E van Doorn · 99 Risks Insight Series · 2025

EXECUTIVE SUMMARY

Intelligent, experienced people surrounded by information consistently fail to act on risk before it destroys value, reputation, or lives. The cause is rarely hidden risk. It is structural: governance arrangements designed in ways that make clear sight almost impossible. This article examines the four practical pillars of effective governance — oversight, decision rights, accountability, and assurance — through two landmark failures and offers principles for organisations that wish to rebuild the capacity to see.

OVERSIGHT	DECISION RIGHTS	ACCOUNTABILITY	ASSURANCE
Who is actually watching?	*The invisible authority map*	*Ownership, not responsibility*	*Governance checking itself*

There is a particular kind of catastrophe that haunts boardrooms and policy chambers alike — not the catastrophe that arrives without warning, but the one that was visible all along, lurking in plain sight, obscured not by complexity but by the way organisations chose to look at it. Or chose not to.

The question that serious governance thinkers have been asking for the better part of two decades is deceptively simple: why do intelligent, experienced people, surrounded by information, consistently fail to act on risk before it destroys value, reputation, or lives? The answer, increasingly, is not that the risks were hidden. It is that the structures meant to surface and manage them — the governance arrangements, the reporting lines, the decision rights, the accountability frameworks — were themselves designed in ways that made clear sight almost impossible.

> *"Risk is not the problem. The inability to see risk clearly is."*

▶ THE ARCHITECTURE OF OVERSIGHT

The Architecture of Oversight

Governance is one of those words that accumulates meaning until it becomes almost meaningless. In its original sense — the systems by which organisations are directed and controlled — it is admirably practical. In practice, however, governance has a tendency to become ceremonial. Committees are formed. Policies are written. Attestations are signed. Risk registers are populated with colour-coded heat maps that convey a reassuring orderliness. And then something goes catastrophically wrong, and the post-mortem invariably reveals that the formal apparatus of governance was operating at some distance from the actual terrain of risk.

The distinction matters enormously. Formal governance and effective governance are not the same thing and confusing them is perhaps the most dangerous mistake an organisation can make.

Effective governance rests on four practical pillars: oversight, decision rights, accountability, and assurance. Each is necessary; none is sufficient on its own. Together, they constitute the architecture by which an organisation can actually see what is happening and respond to it. When any one of the four is weak or poorly designed, the whole structure begins to lean — and usually in the direction of the risks that matter most.

▶ OVERSIGHT

Oversight: Who Is Actually Watching?

Oversight is not the same as monitoring. Monitoring is the generation of information. Oversight is the active, purposeful scrutiny of that information by people with the authority and capability to act on it.

The distinction is lost in many organisations. Risk dashboards proliferate. Reporting cycles multiply. Boards receive thick packs of material every quarter, structured to demonstrate control rather than to reveal vulnerability. The incentive — almost always — is for information to travel upward in a form that reassures rather than alarms.

This is not dishonesty, at least not in most cases. It is the natural result of how organisations process risk when they have failed to separate the function of generating information from the function of scrutinising it. When the same team that manages a risk is also responsible for reporting on that risk, the information that reaches the board is structurally filtered. Not out of malice, but out of optimism, out of professional loyalty, out of the entirely human tendency to present one's own work in the most favourable light.

> **What effective oversight actually requires**
>
> Structural independence — people with both the mandate and the standing to ask uncomfortable questions and receive honest answers. A genuine "second line" that is neither captured by the first nor merely duplicating it. And, most elusive of all: an organisational culture in which bad news travels fast and honest risk assessment is valued over comfortable reassurance.

Culture cannot be mandated by policy, but it can be shaped by behaviour — particularly the behaviour of those at the top of the organisation.

▶ DECISION RIGHTS

Decision Rights: The Invisible Map

If oversight is about what an organisation can see, decision rights are about what it can do with what it sees. Decision rights — the formal and informal allocation of authority to make consequential choices — are perhaps the least examined dimension of governance, and among the most important.

In most organisations, the formal decision rights framework is incomplete. It describes who can approve a capital expenditure or sign a contract, but it says little about who can escalate a risk, who can override a local manager who is downplaying a problem, who can call a halt to a project that has quietly acquired a risk profile never contemplated when it was approved.

> *"Everyone knows what they are responsible for managing. Far fewer people know what they are empowered to stop."*

This vacuum is particularly dangerous in complex, decentralised organisations, where risk accumulates not through single catastrophic decisions but through the aggregation of many smaller choices made at different levels by different people who lack a systemic view. No individual decision triggers an alarm. The alarm only sounds when the accumulated effect becomes visible — by which point the organisation is typically deep inside a problem it should have seen coming.

The practical remedy is surprisingly unglamorous: a decision rights mapping exercise that explicitly addresses risk escalation, not just resource allocation.

▶ ACCOUNTABILITY

Accountability: The Difference Between Responsibility and Ownership

There is a failure mode so common in large organisations that it has acquired its own sardonic nickname among governance consultants: “diffused accountability” — the condition in which everyone is formally responsible for a risk and no one is actually accountable for it.

Accountability is not the same as responsibility. Responsibility can be shared, distributed, matrixed across functions. Accountability, properly understood, cannot. Accountability means that when a risk materialises in a way that was preventable, there is a specific person who must answer for the gap between what should have happened and what did.

The distinction is not punitive in purpose. It is structural. When accountability is genuinely singular — when there is a named individual who owns a risk outcome, not merely a team or a committee — the behavioural consequences are significant.

The committee problem

Committees do not resign. Committees are not held responsible. The committee as a risk governance mechanism has its uses — deliberation, diverse perspectives, checks on individual judgment — but it is a poor vessel for accountability. In the absence of someone who is personally accountable, the risk management process tends, over time, to drift toward the formal and the performative.

▶ ASSURANCE

Assurance: Closing the Loop

The fourth pillar — assurance — is where the other three are tested. Assurance is the process by which an organisation verifies that its oversight mechanisms are actually working, that decision rights are being exercised appropriately, and that accountability is being discharged. It is, in essence, governance checking itself.

The classic model of assurance is the "three lines of defence" — business operations managing risk on the front line, a risk and compliance function providing oversight and challenge, and internal audit providing independent assurance. The model has considerable merit, but it is frequently implemented in ways that hollow it out.

Internal audit, in particular, tends to suffer from a structural problem: it is chronically under-resourced relative to the complexity of the organisations it is asked to scrutinise, and its independence from management is often more nominal than real. An internal audit function that is effectively controlled by the very management whose decisions it is supposed to review provides something that looks like assurance from the outside but functions as little more than validation.

> **The question boards rarely ask plainly**
>
> "What is it that we are not seeing, and why?" Meaningful assurance requires genuine independence, adequate resources, and a direct line of communication to the audit committee of the board that cannot be filtered by executive management.

▶ CASE STUDIES

Case Studies in Governance Failure

CASE STUDY I · MARCH 2023

The Risk That Was Always There: Silicon Valley Bank

SVB's collapse in approximately 48 hours triggered the most significant American banking crisis since 2008. The failure was not the result of hidden risk. The bank's balance sheet was, in the most literal sense, public information. The Federal Reserve had been raising interest rates at the fastest pace in decades. A bank loaded with long-duration securities was exposed to significant mark-to-market losses in precisely such an environment. This was not obscure. It was elementary.

What failed was the governance architecture around it. The bank had no permanent Chief Risk Officer for the better part of a year leading up to the collapse. The risk committee of the board had received reports on the interest rate exposure. Those reports did not trigger decisive action. Decision rights around liability management were unclear enough that the decision to crystallise losses was made without adequate understanding of the market signalling it would generate.

The Federal Reserve's own post-mortem was unusually candid: examiners had identified the risks, concerns had been escalated, but the escalation pathway was slow, accountability for acting on findings was diffused, and the bank's management had sufficiently captured the confidence of its supervisors that scepticism was difficult to sustain. The mechanisms of oversight were present. They were not effective.

CASE STUDY II · 2018–2019

The Slow Catastrophe: Boeing's 737 MAX

The crashes of Lion Air Flight 610 and Ethiopian Airlines Flight 302 killed 346 people and exposed one of the most comprehensive governance failures in modern corporate history. The MCAS — the software at the centre of both crashes — became significantly more powerful as

the programme developed. That evolution was not adequately surfaced to regulators, airline customers, or the pilots who would fly it.

The governance framework around the MAX programme created conditions in which commercial pressure systematically overrode safety escalation. Decision rights around safety certification delegated substantial authority to Boeing itself. The oversight relationship between regulator and manufacturer had evolved to a point at which the regulator was, in effect, auditing Boeing's own assessment of its aircraft's safety — without the independence or resources to conduct a genuinely arm's-length review.

What is most striking, in retrospect, is how many people saw elements of the problem. The failure was not one of intelligence or technical capability. It was a failure of governance architecture — of the structures that should have ensured that the right information reached the right people with the right authority at the right time.

▶ PRINCIPLES

Rebuilding Sight: Five Principles

The practical question is what organisations and their overseers should actually do differently. Several principles emerge from both the failures above and from the broader literature on what distinguishes governance that works from governance that merely appears to.

- Separate information generation from information scrutiny. The people responsible for managing a risk should not be the only people responsible for assessing it. The independence of the second and third lines is not a bureaucratic nicety; it is the functional heart of effective oversight.
- Make decision rights explicit around risk escalation, not just resource allocation. What triggers a mandatory board notification? Who can stop a programme that has acquired a risk profile beyond its original mandate? These questions should have written answers, tested periodically against real scenarios.

- Resist the diffusion of accountability. There should be, at the end of any risk governance structure, a named individual who owns the outcome — and whose ownership is visible enough to be real.
- Invest in assurance that is genuinely independent. Internal audit must have the resources, the mandate, the capabilities, and the protected reporting lines to ask: not "are the controls in place?" but "are the controls working?"
- Cultivate the organisational culture in which bad news is welcomed rather than filtered. The boards and chief executives who receive the most honest information are, almost invariably, those who have made it clear that honest information is what they want — even when, *especially when*, it is uncomfortable.

▶ CONCLUSION

The View from the Top

There is a tendency, in most governance literature, to speak of "tone at the top" as if it were a separate category from structural design — something desirable but essentially ornamental. The evidence of the past two decades suggests otherwise. The cases where governance architecture has failed most catastrophically are almost always cases where the culture had been allowed to treat risk management as a compliance function rather than a strategic one — where the instinct to reassure had been rewarded and the instinct to alarm had been penalised.

Governance is, at its best, the organised capacity of an institution to see itself clearly. It is the set of structures and behaviours that ensure consequential decisions are made by the right people, with the right information, at the right time, and that the organisation can learn from the gap between what it expected and what happened.

That capacity is not expensive to create, relative to the cost of its absence. It does not require exotic techniques or new technology. It requires honesty about where the blind spots are, discipline about who is accountable for what, and leadership willing to look at what is actually there — rather than at the more comfortable version of events that a poorly designed governance architecture will always be inclined to provide.

> *"Risk is not the problem. The inability to see risk clearly is. And the inability to see risk clearly is, almost always, a governance problem."*

SOURCES

This article draws on publicly available regulatory reports, congressional testimony, and published post-mortems. The Federal Reserve's review of Silicon Valley Bank's supervision was published April 2023. The House Transportation and Infrastructure Committee's report on the Boeing 737 MAX was published September 2020.

ABOUT 99 RISKS · RAILGUARD · ASSESSUM.COM

99 Risks Pty Ltd is a specialist risk and governance advisory firm. Our work spans governance design, risk framework development, and human factors analysis across highly regulated industries.

RailGuard — our supplier risk management platform — is available at assessum.com. It helps organisations onboard, assess, and continuously monitor service providers against governance and compliance standards.