ANALYSIS & OPINION · GOVERNANCE, RISK & HUMAN FACTORS

The Confidence to Lead

Every governance framework, every risk model, every control environment ultimately rests on the same foundation: a person making a judgment call.

E van Doorn · 99 Risks Insight Series · 2025

EXECUTIVE SUMMARY

Understanding why human judgments go wrong — and how organisations can help them go right — may be the most important and least-examined question in risk management. This article examines the compliance illusion, four documented failure modes of human judgment, and the emerging discipline of curiosity as a risk practice. Drawing on case studies from Lehman Brothers and the NHS, it argues that the gap between what governance systems are designed to do and what they actually do is, in almost every case, a human gap.

In the summer of 2019, fires of unprecedented scale tore through the Australian bush. In the months that followed, floodwaters consumed communities that the fires had already scarred. For the people working inside Australia's emergency management systems during those months, the experience delivered a lesson that no framework document had prepared them for: that in genuine crisis, the quality of an organisation's response is almost entirely a function of the quality of the human judgment operating within it.

The plans existed. The frameworks were in place. The procedures had been written, rehearsed, and filed. And yet, at the moments of highest pressure, what determined whether a community received the help it needed on time — none of that was determined by the plan. It was determined by the person holding it.

We have spent decades building increasingly sophisticated frameworks for managing organisational risk. We have invested in controls, in oversight structures, in reporting hierarchies, in assurance mechanisms of considerable complexity. What we have invested in less systematically is our understanding of the human beings through whom all of those frameworks are interpreted and enacted.

> *"The gap between what our governance systems are designed to do and what they actually do is, in almost every case, a human gap."*

▶ THE COMPLIANCE ILLUSION

The Compliance Illusion

There is a comfortable fiction that underlies much of contemporary risk management, and it is worth naming plainly: the fiction that a well-designed control environment will produce well-managed risk, regardless of the quality of the human judgment operating within it.

This is the compliance illusion — the belief that the right policies, the right procedures, the right sign-offs, and the right attestations are, in themselves, sufficient to ensure that an organisation is managing its risks effectively. Controls are visible, documentable, and auditable in ways that judgment is not. The tendency to focus governance investment on what can be measured, at the

expense of what actually matters, is one of the most persistent pathologies in organisational risk management.

> **The predictable consequence**
>
> An organisation that has invested heavily in its compliance infrastructure and lightly in the human understanding that gives that infrastructure meaning will produce an enormous quantity of evidence that its controls exist, alongside a much smaller quantity of evidence that they work. The documentation will be impeccable. The reality will be variable. And the gap between them will be invisible until the moment it is not.

This is not an argument against controls. Controls are necessary. Structure matters. The argument is, rather, that controls are necessary but not sufficient — that every control environment requires human beings who understand what the control is trying to achieve, who are genuinely committed to achieving it, and who have the judgment to apply it intelligently in conditions that the person who designed it did not anticipate.

In the language of Intelligent Risk — a framework that has emerged from decades of applied governance practice across sectors as varied as law enforcement, emergency management, and corporate leadership — control is the first discipline of organisational risk, not the last. The organisations that treat the Three Lines of Defence as the totality of their risk management capability have the structure but not the awareness, the accountability but not the foresight. They are disciplined. They are not yet intelligent.

▶ HOW JUDGMENT FAILS

How Judgment Fails: Four Documented Failure Modes

To understand why human behaviour is so consequential in risk environments, it is useful to understand the specific ways in which human judgment tends to fail — not through incompetence or dishonesty, but through cognitive and social dynamics that are predictable, consistent, and largely immune to the mere existence of a governance framework.

01 Normalisation of Deviance

An anomaly is observed, does not produce a problem, and is therefore noted with less concern over time. What was once an anomaly becomes a new normal — not because anyone decided it should, but because the absence of adverse consequences was interpreted, erroneously, as evidence that the risk was lower than originally supposed.

02 Motivated Reasoning

The tendency to process information in ways that support the conclusion that serves our interests or confirms our prior beliefs. The project manager committed to a timeline processes ambiguous schedule signals systematically toward the optimistic. None of this is dishonesty. It is the predictable result of being human.

03 Authority Bias

The disproportionate weight given to the views of people in positions of seniority, independent of the quality of those views. The junior analyst who has spotted something the senior partner missed will, in a surprising proportion of cases, find a way to doubt their own analysis before challenging the partner's.

04 Incentive Misalignment

The straightforward human tendency to act in ways that serve the interests by which we are rewarded, even when those interests diverge from the organisation's. Incentives are not everything in human behaviour. But they are a great deal, and governance systems that do not take them seriously are working against the grain of the people they depend on.

▶ CURIOSITY AS A RISK DISCIPLINE

Curiosity as a Risk Discipline

If the failure modes of human judgment in risk environments are this well-documented, the question is what organisations can do about them. The answer begins not with more controls but with something that most governance frameworks have historically undervalued: curiosity.

Curiosity, in the context of risk management, is not a personality trait or a cultural aspiration. It is a discipline — a structured, deliberate, institutionally supported practice of questioning assumptions, seeking disconfirming evidence, and treating the absence of visible problems not as proof of safety but as an invitation to look harder.

The Three Lines of Attack

Where the traditional defence model asks “do our controls exist and are they functioning?”, the attack model asks “what are we not seeing, and why?” It transforms every person in the organisation from a follower of procedure into a sensor — someone whose observations, questions, and anomalies are genuinely valued as inputs into the organisation’s understanding of its own risk environment.

The practical expression of this shift is both cultural and structural. Culturally, it requires an organisation in which the person who raises an uncomfortable question is thanked rather than managed. Structurally, it requires channels through which the observations of people close to the work can reach people with the authority to act on them.

> *“Culture is what people do when no one is watching. And what people do when no one is watching is a direct function of what they have learned, through experience, is valued.”*

The organisations that have successfully cultivated curiosity as a risk discipline are, almost without exception, the organisations whose leadership has demonstrated, through consistent behaviour over time, that honest information is more valuable to them than comfortable information.

▶ CASE STUDIES

Case Studies in Human Risk Dynamics

CASE STUDY I · 2008

The Room That Could Not Hear: Lehman Brothers

The collapse of Lehman Brothers has been examined from almost every conceivable angle. What receives less attention, but is in many respects more instructive, is the human and cultural

dimension of the failure: how an organisation populated with intelligent, experienced people produced decisions of such catastrophic quality.

The firm's risk function had identified many of the exposures that would ultimately prove fatal. Risk officers had raised concerns about the concentration in commercial real estate, about the leverage ratios, about the assumptions embedded in structured product valuations. Those concerns had, in a number of documented instances, been shared with senior leadership. They had not been acted on.

Not primarily because the concerns were dismissed on analytical grounds, but because the human dynamics of the organisation systematically prevented uncomfortable information from receiving the weight it deserved. The authority bias that made it difficult for risk officers to sustain a position against senior dealmakers. The incentive structure that rewarded returns far more generously than it rewarded the identification of risk to those returns. The controls existed. The discipline to act on what they revealed did not.

CASE STUDY II · NHS PATIENT SAFETY REFORM

The Organisation That Learned to Ask

A series of high-profile inquiries in the late 1990s and early 2000s — Bristol Royal Infirmary, Shipman, Mid Staffordshire — revealed healthcare organisations in which serious, visible problems had persisted for years without being addressed, in which people who knew about those problems had not felt able to raise them, and in which the culture of professional hierarchy had been more powerful than the obligation to patients.

The response, over two decades, has been imperfect and uneven. But in the areas where investment has been most sustained, the results have been significant. Structured safety briefing tools — borrowed from aviation — explicitly empowered junior members to raise concerns regardless of seniority, addressing the authority bias that allowed serious problems to be visible to junior staff while remaining invisible to decision-makers.

The NHS experience is instructive not because it describes a comfortable success story — variation in safety culture across the health system remains wide. It is instructive because it demonstrates, in one of the most human-intensive environments imaginable, that the human dimensions of risk management are not fixed. They can be shaped, deliberately and systematically, by the choices organisations make about what they value, what they measure, and how they lead.

▶ INTEGRATION

The Integration of Discipline and Curiosity

There is a tension embedded in what has been argued so far, and it is worth naming rather than eliding. The argument for discipline — for structure, for controls, for accountability frameworks — and the argument for curiosity — for questioning, for honest information, for the willingness to challenge — can appear to pull in opposite directions. The disciplined organisation imposes order. The curious organisation disturbs it.

This tension is real. But it is, in the hands of thoughtful leadership, productive rather than paralysing. The organisations that manage risk most intelligently are not the ones that have resolved the tension by choosing one at the expense of the other. They are the ones that have learned to hold both.

Integration in practice

In an integrated organisation, the things that the curiosity function discovers feed directly into the discipline function — updating the controls, revising the risk assessments, prompting the governance conversations that would not otherwise have happened. This is governance not as a static hierarchy of defence lines, but as a living ecosystem in which structure enables curiosity, and curiosity refines structure.

The maturity this represents is not achieved quickly. It requires, above all, the willingness to be honest — at every level of the organisation — about the gap between the risk management system that is documented and the one that is actually operating.

▶ LEADERSHIP IMPERATIVES

What Intelligent Risk Asks of Leaders

The framework of Intelligent Risk — with its three disciplines of Control, Curiosity, and Integration — asks something specific and demanding of the leaders who seek to apply it. It asks them to hold, simultaneously, the discipline to maintain the structures that make governance coherent and the curiosity to question whether those structures are actually working.

This is not a technical challenge. It is a human one. It requires the kind of leadership that creates, through consistent behaviour over time, the conditions in which honest information flows freely, uncomfortable questions are welcomed, and the distance between the organisation's picture of its own risk environment and the reality of that environment is continuously and deliberately narrowed.

The organisations that achieve this do not arrive there through a single transformation programme or a new framework implemented in a quarter. They arrive through the accumulation of countless small moments in which the right choice — the choice to surface rather than suppress, to question rather than confirm, to learn rather than defend — was made by someone who had been given, by their organisation's culture and leadership, the confidence and the safety to make it.

> *"Control without awareness becomes blindness. Awareness without control becomes noise. The integration of both is what intelligent risk management actually looks like."*

The goal is not the elimination of judgment errors. Those cannot be eliminated. It is the creation of an environment in which errors surface quickly, travel fast, and produce learning rather than paralysis. In which the human at the centre of the governance system is not merely a follower of procedure but a genuinely engaged, continuously curious participant in the organisation's collective effort to understand its own reality.

It was true in the chaos of the Australian bushfires. It is true in the boardroom. And it is the same truth, in the end, wherever the ground shifts and a person must decide what to do next.

SOURCES

This article draws on the framework of Intelligent Risk: Evolving Governance from Defence to Foresight to Resilience; Diane Vaughan's development of normalisation of deviance (1996); the Financial Crisis Inquiry Commission's report on Lehman Brothers (2011); and the Francis Report on Mid Staffordshire NHS Foundation Trust (2013).

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.