IRIS · ESSAY ONE · 2026

Enterprise Risk Was Built Within a Constraint That's Lifting

BY JAY DUNNE SERIES PART 1 OF 3 DOMAIN ENTERPRISE RISK INTELLIGENCE

Most large enterprises today operate with mature risk frameworks, significant ERM investment, and sophisticated capability across security, cyber, financial, and operational domains. And yet, the strategic integration the field has formally pursued for nearly a decade — risk synthesis that reaches executive decisions in time to shape them — remains rare in practice.

The numbers are not subtle. According to a January 2026 study by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), only 7% of enterprise risk management programs are fully integrated into strategy decisions. Fifty-four percent are still perceived as compliance or assurance functions. Ninety-eight percent of risk practitioners surveyed believe ERM should play a more strategic role than it currently does.[1] The framework's own stewards now openly describe a persistent gap between what the field aspires to and what it actually delivers.

The conventional explanations for this gap are familiar and partly true: organizational inertia, budget constraints, the difficulty of changing culture. However, these explanations also fall short. The argument of this piece is that the more important explanation is structural: the field's current posture was shaped by a binding economic constraint that has held for a generation, and that constraint is now beginning to lift due to the increasing frequency of risks that cross organizational and geographic boundaries and reshape what enterprises must contend with. The implications for how enterprises organize their risk and resilience functions over the next several years will be significant, and they are not primarily about tooling.

For most of its modern history, enterprise risk intelligence has been a tactical and operational function and siloed by nature. To understand why, it helps to look at how the field arrived at its current posture. Security teams responded to incidents. Cyber teams managed exposure within their lane. Geopolitical analysts

produced reports that traveled poorly across organizational boundaries. Supply chain, ESG, financial, and regulatory functions monitored their domains with discipline, but rarely connected their signals into a unified picture before disruptions arrived. The integration that ISO 31000[2] and COSO[3] have called for since 2017 — risk management embedded in strategy, woven into decisions at every level — remains more aspirational than common practice.

It is tempting to read this as a failure of vision, or of will, but this may be too harsh a conclusion. The field's operational posture was a rational response to a constraint shaping enterprise risk intelligence for a generation: the analyst-hour economics of continuous cross-domain synthesis at enterprise scale.

To do the work the frameworks describe — to monitor geopolitical, cyber, financial, supply chain, ESG, regulatory, and security signals continuously, translate them into business-impact terms, identify where one domain's signal amplifies another's exposure, and deliver that synthesis into executive decisions before disruptions fully materialize — requires a volume of skilled analytic labor that, until recently, only the largest intelligence agencies and a handful of Fortune 50 firms could afford. Everyone else did what was rational under the constraint. They built the function and the teams they could affordably staff. They optimized their operational lanes. They left the synthesis layer aspirational.

This is the insight Arjen Boin developed in his work on transboundary crisis management:[4] the bureaucratic toolkit was built for bounded problems, and the risks organizations now face are not bounded. Coordination and centralization — the two mechanisms institutions traditionally reach for when boundaries blur — both presuppose conditions that cross-domain risk synthesis cannot supply on demand. There is rarely a single actor within the enterprise with the authority to centralize. There is rarely time to negotiate coordination before the next signal arrives. The integration mandate has lived in the gap between what the frameworks describe and what the underlying economics allow.

Credit the leaders in the field who have worked within this constraint while also calling out its existence. The tactical posture is the rational institutional response when the cost of the better model exceeds what the organization can sustain.

The integration mandate did not fail because the field ignored it. ISO 31000:2018 calls explicitly for risk management to be integrated into core business activities at every organizational level. COSO ERM 2017 was revised specifically to strengthen the connection between risk intelligence and strategy-setting. These are not obscure, theoretical documents, but foundational frameworks of the discipline, and the integration requirements have been visible to every serious risk practitioner since they were issued.

While the frameworks describe a destination, or outcome, they do not, and were never meant to, specify the organizational economics required to reach it. COSO's January 2026 paper makes this explicit. It diagnoses an implementation gap that has persisted across industries and geographies: programs that produce outputs without changing decisions, risk discussions that happen alongside strategy rather than inside it, board reporting that compiles information without orienting executives toward what matters. The cultural distance

between how organizations talk about risk and how they talk about strategy, the paper observes, exceeds eighty percent in most settings.[1]

This is the gap the field's economics could not close. As Boin's work on transboundary crisis management makes clear, bounded institutions struggle when the problems they face are not bounded. The bureaucratic toolkit — coordination and centralization — was built for a different class of risk. Continuous cross-domain synthesis demands a different design entirely. The frameworks named the destination correctly, but did not present an operational roadmap on how to get there.

There is a useful observation in Thomas Kuhn's work on how fields restructure their understanding of the problems they face.[5] Kuhn's insight was that disciplines do not change because individual practitioners suddenly see things more clearly. They change when the anomalies the existing framework cannot accommodate finally outweigh the cost of building a new one. Enterprise risk intelligence has been accumulating those anomalies for a generation. What has been missing is not recognition of the problem but the structural conditions that would make a different model feasible. Those conditions are now beginning to assemble.

The signs of shift are now visible to anyone paying close attention to the field's institutional discourse. The same January 2026 COSO paper that names the implementation gap also describes what a working alternative would look like. It calls for ERM to function as an embedded operating system rather than a parallel reporting function — decision-led, lightweight, woven into the rhythms in which strategy is actually made. It treats the integration mandate not as an aspiration to be repeated but as a design problem to be solved. The framework's own stewards are publishing about decision architecture rather than risk taxonomy. That is a meaningful shift in where the field's serious thinking is being directed.

The pattern extends beyond ERM. Practitioners in adjacent disciplines are reaching similar conclusions from inside their own fields. The Institute of Strategic Risk Management recently published work observing that traditional security architectures were designed for a narrower class of threat than organizations now face, and that the structural mismatch is becoming difficult to ignore.[6] The diagnosis is converging from multiple directions.

What is changing, in other words, is not the recognition that fragmentation is a problem. That recognition has existed for years. What is changing is the institutional willingness to treat the problem as structural — and the early availability of capabilities that make a structurally different model economically feasible for organizations that are not Fortune 50 firms or intelligence agencies. The constraint that held for a generation is lifting. The implications for how enterprises organize their risk and resilience functions are going to be larger than most executives are currently positioned to recognize.

For executives whose organizations are mature enough to have built credible ERM, security, and resilience functions, this moment is going to matter more than the current conversation suggests. The reflexive response to capability emerging in any field is to ask what tools to buy and what processes to upgrade. That response will be insufficient here. The shift now underway is not a tooling shift. It is a structural one.

The organizations that will benefit most from the constraint lifting are not the ones that move fastest to adopt new platforms. They are the ones that recognize, early, that the synthesis function the frameworks have been describing for a decade is now operationally feasible — and that operationalizing it is fundamentally a question of organizational design. Where the function sits. Who staffs it. How its outputs reach decisions. What authority it carries when it enters the room. These are not procurement questions. They are governance and design questions, and the executives best positioned to answer them are not necessarily the ones currently leading the security and risk modernization conversations inside their organizations.

The next several years are going to reshape what enterprise risk intelligence looks like inside serious organizations. The first wave of change will be visible in tooling, because tooling changes are easy to measure and easy to announce. The more consequential wave will be in structure, and it will be quieter, slower, and harder to point to. But it is the structural wave that will separate the organizations that translate the lifting constraint into durable advantage from those that simply spend more on capability without changing how they decide.

A follow-up piece will look more directly at what is actually shifting and what the redesigned function should become.

WORKS CITED

[1] Luttenton, R., Samp, S., & Stone, A. (2026). *From Guidance to Action: Exploring Practical Enterprise Risk Management.* Committee of Sponsoring Organizations of the Treadway Commission (COSO).

[2] International Organization for Standardization. (2018). *ISO 31000:2018 — Risk Management — Guidelines.*

[3] Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management — Integrating with Strategy and Performance.*

[4] Boin, A. (2019). The Transboundary Crisis: Why We Are Unprepared and the Road Ahead. *Journal of Contingencies and Crisis Management,* 27(1), 94–99.

[5] Kuhn, T. S. (1962). *The Structure of Scientific Revolutions.* University of Chicago Press.

[6] Griffin, B. (2024). *From Snakes to Dragons: Understanding Risk in Modern Security Environments.* Institute of Strategic Risk Management.