

B L A C K F O X S T R A T E G Y

CONNECTING STRATEGY & ERM

A CRO Guide

Erin Sedor

Executive Advisor & Strategic Performance Expert

ErinSedor.com

New Science. Ancient Wisdom. Better Business.



The Promise That Was Never Kept

Enterprise risk management was supposed to change the game. That was the whole point of it. The evolution from traditional risk management — which dealt primarily with safety, insurance, contracts, and claims — to *enterprise* risk management was built on a singular, powerful premise: risk should be connected to strategy.

COSO said it. ISO affirmed it. RIMS has championed it. Every major framework and standard published in the last two decades has pointed to the same conclusion — that ERM is a strategic business discipline designed to allow an organization to manage risks and seize opportunities related to the achievement of its strategic objectives.

And yet. Here we are.

Only 11% of senior finance leaders view their organization's risk management as a strategic tool delivering competitive advantage. Six in ten ERM programs claim connection to strategic planning, but many fail to connect ERM insights with actual strategic decision-making. And only 18% of ERM leaders express high confidence in identifying and managing emerging risks. These aren't fringe data points from obscure studies. These are findings from AICPA, the IIA Foundation, Baker Tilly, and Gartner — in 2025.

Organizations claiming complete ERM processes grew from 9% in 2010 to 34% in 2023 — and then plateaued. The industry has stalled. And if you're a Chief Risk Officer, you already know this. You've felt it. The board conversations are getting more frequent. Risk awareness is higher than it's ever been. But maturity hasn't caught up, and the connection between what your ERM program produces and what your CEO needs to execute strategy remains frustratingly thin.

The promise of ERM — that it would bridge risk and strategy — was never fully kept. Not because the concept was wrong. But because the design was incomplete.

This guide is about what's missing and what it takes to close the gap.

Three Reasons ERM Stalled at the Strategy Doorstep

Let me be direct. ERM doesn't fail because risk practitioners aren't good at their jobs. It fails to connect to strategy because the process itself has structural gaps that no amount of effort or technology can overcome without a fundamental reframe. There are three specific reasons this connection has never been fully made, and understanding them is the first step to solving the problem.



1. ERM and Strategic Planning Lack a Common Language

Risk professionals speak in terms of likelihood, impact, risk tolerance, risk appetite, heat maps, and mitigation controls. Strategic planners speak in terms of vision, growth targets, competitive positioning, market expansion, and performance metrics. These two disciplines have been operating in parallel for decades, and while they occasionally intersect in a board presentation or an annual planning cycle, they have never developed a shared language for measuring risk from a strategic standpoint.

This isn't a communication problem. It's a structural one. ERM frameworks were designed to capture, categorize, and prioritize risk. Strategic planning frameworks were designed to set direction and allocate resources. Neither was built to speak the language of the other. And so even when both disciplines are functioning well independently, the translation between them requires manual interpretation by whoever happens to sit at the junction — usually the CRO, the CFO, or the CEO themselves.

That's not a system. That's a workaround. And workarounds break down when the people holding them together change roles, retire, or simply run out of bandwidth.

What's needed is a framework that creates a common context — a shared lens through which both risk and strategy can be viewed, measured, and discussed in terms that matter to both disciplines. Without that common language, ERM outputs remain data that leaders acknowledge but rarely use to shape strategic decisions.

2. ERM Captures Enterprise Risk without Separating Strategic Risk

Here's where it gets interesting. One of ERM's greatest strengths is also its greatest limitation. ERM was designed to capture risk from across the entire organization — operational, financial, compliance, reputational, technological, and more. That holistic view is enormously valuable. It gives leaders a panoramic lens on what could go wrong and where the exposures are concentrated.

But here's the problem: it captures everything in the same bucket. Operational risks that could disrupt daily performance sit alongside strategic risks that could derail a multi-year growth initiative. A supply chain disruption and an existential competitive threat are categorized, scored, and reported using the same methodology, the same scales, and often the same risk register.

The process never includes a mechanism for separating out strategic risk from the larger portfolio. And without that separation, risk profiles become unwieldy at the leadership level. When a CEO or board looks at a risk heat map, everything is blended together. They can see concentration, but they can't clearly distinguish which risks have the potential to materially impact the organization's most critical strategic priorities from those that are operationally significant but strategically peripheral.

For risk profiles to be meaningful at the leadership level, strategic risk must be delineated from non-strategic risk within the data. That requires a deliberate design



choice in the ERM framework — one that most programs have never made because the frameworks they're built on didn't require it.

3. ERM Fails the Crosswalk

This is the one that matters most, and it's the gap I've seen play out in every organization I've worked with over three decades.

Traditional ERM builds risk profiles from the bottom up. It starts with events, incidents, exposures — things that have happened or could happen — and works upward through analysis, categorization, and prioritization to produce a risk portfolio. For operational risk, this approach is exactly right. You need to know what can go wrong, how likely it is, and what the impact would be. Start with the event, trace the consequences, and build your controls.

But strategic risk doesn't work that way. Strategy doesn't start with events. Strategy starts with imperatives — the things that *must* happen for the organization to succeed. And the question that needs to be asked — but almost never is — is this: *What risks have the potential to impact the critical path to achieving those imperatives?*

I call this crosswalking. It's the practice of starting from the strategy — from the strategic imperatives themselves — and working downward to identify which risks, from across the entire enterprise portfolio, have the potential to disrupt what I call the *keystone* path. It's not about replacing the bottom-up process. It's about adding the top-down lens that completes the picture.

Without the crosswalk, ERM remains operationally valuable but strategically incomplete. Risk practitioners are talking about the right stuff from an operations standpoint, but they're not connecting it to the stuff that keeps the CEO up at night — the strategic bets, the growth initiatives, the transformation programs that define the organization's future.

When I speak to risk managers, the number one complaint I hear is that they have no seat at the table. When I speak to leaders about risk management, the comments I hear are that risk managers can't see the big picture and have tunnel vision. Both are right, and both are symptoms of the same missing mechanism. The crosswalk is the bridge. Without it, risk intelligence stays operational and strategy stays unprotected.

The Missing Element: Keystone

At the heart of this gap is a concept that ERM has never formally incorporated — one I call **keystone**.

In architecture, the keystone is the single element at the top of an arch that holds the entire structure together. Remove it, and everything collapses. In strategy, the principle is the same. A keystone is any activity, asset, resource, service, or system that materially impacts — positively or negatively — the organization's ability to successfully achieve its strategic goals and objectives. It is the filter that separates what's important from what's



indispensable. **It is the mechanism that allows risk intelligence to be prioritized not just by likelihood and impact, but by strategic relevance.**

Most ERM programs have no equivalent to this. They have risk tolerance. They have likelihood-impact matrices. They have risk categories and risk owners and escalation protocols. Risk priority is based on a compilation of risk scores offset by mitigation scores. But they don't have a systematic way to determine which of those risks are keystone risks – ones that directly threaten strategic success and which, while significant, are manageable without strategic consequence.

This is the keystone gap, and it's the reason ERM and strategy have never fully connected.

Defining a keystone risk requires both a top-down and bottom-up perspective. From the top down, leadership must clearly articulate its vision, strategic priorities, and the imperatives tied to them. From the bottom up, the operational performance requirements that are critical to the functioning of the organization must be identified and measured. When these two perspectives converge, you have a clear picture of what's keystone — and now the crosswalk has a starting point.

An example helps here — three of them, actually.

The accidental death of an employee on the job is a catastrophic event by any measure. It triggers immediate crisis response, regulatory reporting, legal exposure, and a profound human impact that reverberates across the organization. It demands leadership attention, compassion, and decisive action. But for most organizations, as devastating as it is, it does not impair the execution of strategic priorities or interrupt the critical functions that sustain the business. It is severe, it demands response, and it must be managed with the gravity it deserves — but it is not a keystone risk in the strategic sense. It does not sit on the critical path between where the organization is and where its strategy says it must go.

Now consider a different scenario. A key department leader resigns unexpectedly. It's disruptive, it creates short-term operational strain, and it requires immediate response — but it's recoverable. Contrast that with the organization's inability to attract and retain the specialized engineering talent required to execute a three-year digital transformation initiative that the entire growth strategy depends on. The first is a personnel event. The second is a keystone risk — because without that talent pipeline, the strategic imperative stalls and the competitive window closes.

Or take cybersecurity. A phishing attack compromises a handful of employee email accounts. It's a security incident, it triggers response protocols, and it needs to be managed — but it's contained. Contrast that with the organization's core data platform being architecturally unable to support the AI integration that leadership has committed to as the centerpiece of its market evolution strategy. The phishing incident is operational risk, well-handled through existing controls.



The platform limitation is a keystone risk — because it sits directly on the critical path to strategic execution.

The distinction matters enormously. And right now, most ERM programs can't make it.

A Better Framework: Connecting ERM to Essential Strategy

Solving this isn't about abandoning ERM. It's about completing it. The operational risk intelligence that a well-functioning ERM program produces is invaluable — the problem is that it stops short of strategic integration. What's needed is a strategic framework that creates the context for ERM to connect to, and a mechanism that links the two.

This is where Essential Strategy and the ESRA Framework come in.

Essential Strategy: The Strategic Foundation

Essential Strategy is built on a foundational premise: every organization, regardless of industry, size, or complexity, succeeds or fails based on the clarity and execution of three interdependent dimensions — Purpose, Growth, and Evolution — held in dynamic Equilibrium.

Purpose is at the very heart of strategy design. It defines where the organization came from, where it wants to go, and why others should care. Purpose must be internally compelling and externally valuable in its contribution.

Growth is not just about revenue. It includes deepening core competencies, expanding capabilities, and building the internal muscle required to sustain both speed and scale. Growth is intentional, matched by adaptive learning.

Evolution is about perpetuating the organization — continually navigating to see how well strategy is working, spotting changes in the external environment, and adapting while staying in alignment with purpose. Evolution is not a future consideration. It is a real-time strategic requirement.

Equilibrium threads through the other three in a fluid way, acting as the catalyst for strategic decision-making. Purpose, Growth, and Evolution are interconnected and must exist in a state of dynamic balance.

Why does this matter for ERM? Because this framework creates what traditional strategic planning never has — a structured context that defines *strategic imperatives* tied directly to the organization's most fundamental needs. These imperatives are the anchors. And once they're defined, the crosswalk has a destination.

The ESRA Framework: The Bridge

The Essential Strategy Risk Appetite (ESRA) Framework was designed specifically to solve the problem this guide describes. It is an approach to designing risk appetite by



focusing on key questions that create strategic intent while utilizing enterprise risk intelligence to inform the context and measurement of the answers.

ESRA asks four questions, each one grounded in the Essential Strategy dimensions:

- 1. How much do we invest before the cost is too great?** This question connects to Purpose. It considers the impact on resources and reputation, and creates target measures based on capital and operating outlays.
- 2. How fast can we get there without sacrificing value?** This connects to Growth. It focuses on core competencies, capabilities, and market, with target measures based on performance.
- 3. To what extent are we willing to change?** This connects to Evolution. It addresses impact on culture and industry, with target measures based on the organization's position in both.
- 4. What threats have the potential to disrupt the keystone path?** This is where the crosswalk lives. With Purpose, Growth, and Evolution imperatives now defined, this question steps back to identify the risks — from across the entire enterprise portfolio — that have the real potential to derail the critical path to strategic execution.

Each of these questions is framed by key risk categories and key metric categories, making the discussion holistic, meaningful, and measurable. When risk appetite is clearly defined through this lens, it creates a mechanism for more refined risk prioritization than what risk tolerance alone can accomplish.

The fourth question is the linchpin. It is where ERM intelligence meets strategic intent. The measures set here are leading Key Risk Indicators as opposed to lagging Key Performance Indicators that organizations typically rely on in reporting. This final step is informed by historical performance and enterprise risk intelligence, drawing from the very data that your ERM program already produces.

This is the bridge. ESRA takes the rich enterprise risk intelligence your program already generates and channels it through a strategic framework that gives it context, priority, and meaning at the leadership level.

You Don't Have to Start Over

If you're a Chief Risk Officer reading this, you may be thinking: *This sounds right, but we already have a strategic plan. We're not going back to the drawing board.*

Good. You don't have to.

Essential Strategy is not a replacement for your existing plan. It is a lens — a diagnostic layer that can be applied on top of whatever strategic framework your organization already has in place. The value isn't in tearing anything down. It's in revealing what's already there, what's missing, and where ERM can finally plug in.

Here's how it works in practice.



Step One: Map Your Current Strategic Imperatives to PGEE

Take your existing strategic plan and pull out the top-level imperatives — the goals, priorities, or initiatives that your organization has identified as essential. Now map each one to the Essential Strategy foundation. Ask of every imperative: is this fundamentally about Purpose, Growth, or Evolution?

A Purpose imperative is one that speaks to why the organization exists, what it contributes, and how it creates internal alignment around a shared cause. Initiatives tied to mission clarity, stakeholder value, cultural identity, or community impact typically land here.

A Growth imperative is about expanding capacity — revenue, market share, capabilities, talent, infrastructure. But it also includes the internal muscle-building required to sustain that expansion: adaptive learning, operational scalability, and the deepening of core competencies.

An Evolution imperative addresses the organization's ability to adapt and stay relevant. Digital transformation, industry repositioning, business model innovation, and long-term sustainability initiatives live in this space.

Some imperatives will map cleanly. Others will bridge two dimensions — and that's expected, because Purpose, Growth, and Evolution are interconnected. A workforce development initiative, for example, might serve both Growth (building internal capacity) and Evolution (preparing the organization for a changing talent landscape). The mapping doesn't need to be perfect. It needs to be revealing.

And that's exactly what happens.

Step Two: See What the Map Reveals

This is where the real value shows up — and where the CRO brings something to the table that no one else in the organization is positioned to see.

When you map existing strategic imperatives to Purpose, Growth, and Evolution, patterns emerge. In my experience, most organizations discover their plan is heavily weighted toward Growth — revenue targets, market expansion, new product lines, capital investment. That's not surprising. Growth is where the pressure lives. It's what boards ask about, what investors measure, and what leadership compensation is tied to.

But the gaps are where the strategic risk hides.

An organization with no Evolution imperatives is one that has no deliberate mechanism for adapting to a changing world. It may be growing, but it's growing into a future it hasn't prepared for. An organization with no internal Purpose imperative — nothing that speaks to what it means to thrive from within — is running a strategy that depends entirely on external outcomes. Growth without purpose is a house built on sand. Growth without evolution is a house with no windows.



This imbalance is not something your CEO will see on a traditional strategic plan. It's not something the board will catch in a quarterly review. But it is exactly the kind of structural risk that the CRO is uniquely positioned to identify. And when you walk into the strategy conversation with a PGEE map of the existing plan showing that the strategy has no evolution dimension, or that the purpose dimension is purely external with no internal grounding, you are no longer reporting on risk. You are shaping strategic direction.

That is a different conversation entirely. And it's the one that earns the seat.

Step Three: Apply the ESRA Framework

With your strategic imperatives now mapped to the PGEE foundation, the ESRA Framework's four questions become immediately applicable. Each imperative has a strategic home. Each one can now be stress-tested through the lens of investment capacity, speed-to-value, willingness to change, and keystone risk exposure.

This is where your ERM intelligence comes alive strategically. The risk data your program already captures — the enterprise-wide portfolio of operational, financial, compliance, and reputational risks — can now be crosswalked against specific strategic imperatives. You're no longer asking "what are our biggest risks?" in isolation. You're asking "which of our known risks sit on the keystone path to our most critical strategic outcomes?"

The answers to that question change everything about how risk is prioritized, reported, and acted on at the leadership level.

What Changes When This Connection Is Made

Risk gets a common language with strategy. The ESRA Framework's four questions create a shared context that both risk and strategy professionals can navigate. Risk appetite is no longer an abstract concept debated in isolation — it's a set of defined statements tied directly to strategic objectives, with clear measures and thresholds.

Strategic risk is separated from the operational portfolio. By defining keystone risks from both the top-down strategic perspective and the bottom-up operational perspective, the program can clearly delineate which risks are strategy-impacting and which are operationally significant but not on the critical path. Risk profiles become actionable at the leadership level because they speak to what leaders care about most — the success of the strategy.

The crosswalk becomes systematic, not situational. Instead of relying on individuals to manually translate between risk data and strategic priorities, the framework builds the crosswalk into the process itself. Strategic imperatives become the starting point for identifying which enterprise risks demand the most attention, the most resources, and the most rigorous monitoring.

The strategic plan itself gets stronger. This may be the most unexpected outcome — and the one that elevates the CRO's contribution beyond risk management entirely.



When existing imperatives are mapped to Purpose, Growth, and Evolution, gaps and imbalances in the plan become visible for the first time. A strategy with no Evolution dimension is a strategy that assumes the world will hold still. A plan with no internal Purpose imperative is one that asks people to execute a vision they have no personal stake in. These aren't risk findings. They're strategic design flaws — and they're the kind of blind spots that traditional planning processes routinely miss because they were never designed to look for them. By bringing this perspective to leadership, the CRO doesn't just protect the strategy. The CRO helps make it whole.

None of this requires your organization to abandon its current strategic plan. It requires a willingness to look at it through a more complete lens — and to let that lens inform how your ERM program connects to what matters most.

The Bridge Was Always Yours to Build

Here's the truth that rarely gets said out loud: the CRO may be the most strategically underutilized leader in the modern organization.

You sit at the intersection of every function, every risk, and every dependency across the enterprise. No one else has the panoramic view that your role provides. No one else sees how operational exposure in one area cascades into strategic vulnerability in another. No one else is positioned to connect the dots between what's happening on the ground and what the strategy demands from the air.

The problem was never a lack of capability. It was a lack of mechanism. ERM gave you the intelligence. What it didn't give you was the strategic framework to channel it through or the keystone filter to make it land at the leadership level.

The data supports the urgency. Organizations with integrated ERM are 30% more likely to achieve their strategic objectives. Companies with advanced ERM practices are 2.5 times more likely to be top financial performers in their industry. And organizations treating risk management separately from strategy have three times higher failure rates during market disruptions. That's not a risk management statistic. That's a survival statistic.

In an environment defined by unprecedented complexity, rapid change, and compounding uncertainty, the organizations that survive and thrive will be the ones that figured out how to connect what their risk intelligence is telling them to what their strategy demands of them.

That connection starts with identifying keystone. It's built through crosswalking. And it's sustained through a framework that gives ERM and strategy a shared language and a shared purpose.

The promise of ERM was never wrong. It was incomplete. And the person best positioned to complete it — to build the bridge between risk intelligence and strategic performance — has been there all along.

It's you.



Ready to see how building a better risk appetite can help your organization?
Let's talk. **Reach out at erin@erinsedor.com or visit ErinSedor.com.**

Erin Sedor is a CEO Strategy Coach and executive advisor with 30+ years helping organizations build strategy that actually works. She is the creator of Essential Strategy, the ESQI 360, and the Quantum Intelligence framework for conscious, adaptive leadership.

A stylized, handwritten signature in black ink. The signature appears to be 'Erin' followed by a large, sweeping flourish that loops back under the name.