From Guidance to Action:

Exploring Practical Enterprise Risk Management

Authors
Ryan Luttenton, Stefany Samp, and Alexa Stone

Acknowledgements
Thank you to the COSO Board and COSO Board Chair and Executive Director Lucia Wind for providing input, assistance, and valuable feedback in developing this paper. We also thank the interviewees and survey participants, risk leaders from across industries and geographies, for sharing their time and insights from experience implementing ERM in practice.

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence. COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

The Committee of Sponsoring Organizations of the Treadway Commission

coso.org

Content and design contributions provided by Crowe LLP.

Table of Contents

Introduction

Dana the Director has thirty minutes before the Risk Committee call begins. She opens the packet and sees the familiar trio: a heat map, a list of 25 top risks, and a paragraph of risk appetite language that sounds important but doesn't tell her what to do. Dana isn't impatient – she's busy – and doesn't have time to decode what matters. When the meeting starts, she asks three direct questions: **What has changed since last quarter? What matters most right now? What do you want from us?** The room gets quieter. What's missing is clear: signals, triggers, owners, and a board-ready view of risk that supports decisions – not another report.

That moment reflects the reality of enterprise risk management (ERM) in many organizations. Time is limited, information is imperfect, and leaders want clarity, not more documentation. While ERM programs often mature over time and produce a growing set of outputs, their impact varies wildly. In many programs, output arrives too late, or in a form that doesn't help leaders choose between options, trigger meaningful action, or impact decisions. And the challenge isn't only technical – it's cultural. ERM depends on people being willing and able to voice concerns early, question assumptions, and surface uncertainty. When those behaviors don't feel safe, even a well-designed ERM process can fall flat. Without psychological safety, leaders hesitate to challenge assumptions, name uncertainty, or escalate concerns early. Risk becomes performative ("we scored it") or a paperwork exercise ("we documented it"). The result is the same: the hard conversations happen after the window to act has already closed.

That challenge is the catalyst for this paper – to move ERM from documenting risks to influencing choices. The goal is embedded risk decisioning – a repeatable way of working, built into planning, investment, delivery, and escalation – so leaders get decision-ready risk signals even when the risk team isn't driving.

This paper provides practical, experience-based guidance on how organizations are applying the COSO ERM Framework in practice – what works, what doesn't, and how to make ERM more decision-useful under real constraints. Rather than treating COSO as a stand-alone framework, we use it as a toolkit: a common language and set of anchors for activating its principles though practical management behaviors.

In practice, four ideas make the difference between ERM activity and ERM impact:

ERM creates value through both protection and creation.

ERM earns relevance when it contributes to decisions, not just documents. Its value shows up in outcomes leaders and boards care about: clearer choices, earlier pivots, fewer surprises, and stronger board confidence.

Strategy and risk are inseparable.

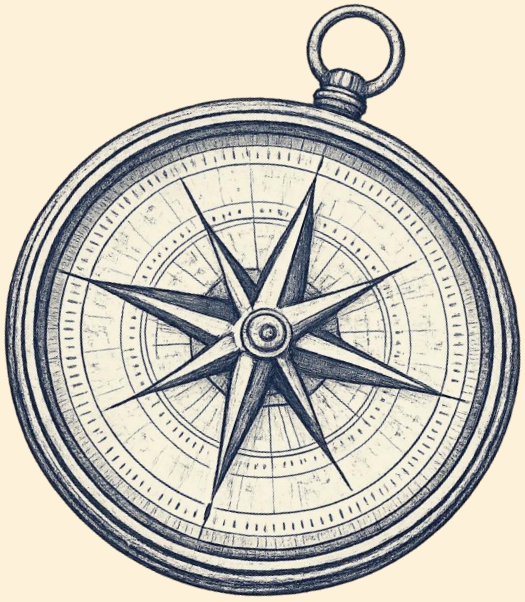
Every strategic choice carries an explicit – or implicit – risk posture. Effective ERM ties risk to strategy choices and outcomes, clarifies ownership, and defines escalation paths so risk information arrives in time to affect the decision.

The implementation gap is real.

Many programs produce outputs; far fewer improve decisions. Heavy artifact production – risk registers, heat maps, and extensive risk and control self-assessments (RCSA) or control inventories – often consume significant effort without affecting choices or triggering action. The practical test is simple: does this work product improve a decision, accelerate execution, or clarify what changes when conditions change?

Effective ERM is decision-led, lightweight, and embedded.

The most effective programs show up where decisions are made – inside planning, investment, and operating rhythms – not alongside them. Under real constraints, ERM earns its seat by focusing every update on what changed, which choice it affects, and the trigger points that would force a different plan.



What you'll get

This paper provides practical components you can use immediately:

- **A value model** for linking strategy and risk at key decision points, such as strategy setting, investment decisions, transformations, and escalation decisions.
- **Real-world case patterns** showing what works and what doesn't, and why certain ERM program designs succeed while others stall.
- **ERM in action under constraints**, including an approach designed for limited capacity and limited board time.
- **Ten ERM operating disciplines** you can apply at any maturity level to increase decision usefulness, reduce noise, and strengthen ownership and follow-through.

Who this is for

This paper is for leaders who need ERM to change something observable. It's for Chief Risk Officers and ERM leaders, risk team members, executives and leadership teams, boards and audit/risk committees, internal audit leaders, and others who rely on ERM insights. Whether you build ERM, consume ERM outputs, or provide assurance over ERM, the goal is the same: make risk information usable, timely, and connected to strategic decisions.

How to use this resource

This paper is designed to be used in layers – you do not need to read it cover to cover to get value.

Skim (30 minutes). Start with this Introduction and the ERM Operating Disciplines. Identify two or three disciplines that would most improve decision usefulness, speed, or board confidence.

Apply (1 day). Choose one discipline you marked during the skim and apply it to a deliverable you already need to produce. Aim for one visible improvement: a clearer decision frame, a usable trigger, or a more focused board update.

Deepen (over a quarter). Read the guide in full and embed the practices into planning, capital allocation, transformation governance, and board reporting. Keep what works and cut what does not. Progress shows up in clearer choices, earlier pivots, fewer surprises, and increased confidence among leaders and the board.

Our approach

This paper was shaped by listening first. We conducted a global survey of risk leaders and practitioners and held a series of conversations with senior leaders across industries and regions to understand how ERM is experienced in practice today. We explored where ERM is delivering value, where it becomes overly abstract or compliance-driven – and what distinguishes programs that meaningfully support strategy and decision-making. These insights form the foundation for the perspectives, examples, and practical guidance presented.

Meet the people and the practices
You'll see them throughout the paper

Personas

To keep guidance grounded in real-world moments, not just concepts, we use a small set of recurring personas. They represent common roles in (and around) ERM, and they reappear in short vignettes and examples to show how practical choices play out in meetings, decisions, and board discussions.

Dana the Director Board member
Dana has fifteen minutes and a high bar for clarity. She focuses on what changed, what matters now, and what management wants the board to decide, endorse, or challenge. If the update doesn't connect risk to strategy, performance, and ownership, she tunes out and cannot contribute in a way that supports the company.

Sasha the Strategy Shaper Strategy and transformation leader
Sasha is making big bets and moving fast. She values risk management when it sharpens choices: clear trade-offs, scenarios, and triggers that enable confident speed. Long lists and abstract language slow her down.

Ravi the Risk Builder ERM leader
Ravi runs ERM with limited time and a small or non-existent team. He wins by simplifying: a small set of priorities, a repeatable cadence, and triggers that drive action. He measures success by whether ERM changes decisions and prevents late surprises.

Tahlia the Toolmaker ERM team member
Tahlia turns principles into usable tools. She is focused on cutting noise, streamlining templates, and building a lightweight operating system leaders will actually use. Her test is simple: what decision will this change?

Casey the Capital Keeper Finance / capital allocation leader
Casey owns the "yes/no" on funding and expects clarity, not confidence theater. Casey leans in when ERM translates uncertainty into ranges, scenarios, and the triggers that would change a plan. If risk cannot be expressed as decision-relevant trade-offs, Casey treats it as noise.

Operating Disciplines

These practices help organizations turn ERM principles into decision-ready behavior. Each Operating Discipline shifts something tangible in how leaders frame choices, handle uncertainty, and drive follow-through.

You'll see these practices identified throughout the paper and explored later with practical guidance – and quick ways to begin.

1. **Link strategy and risk**
2. **Treat value creation as a required outcome**
3. **Make risk appetite meaningful and usable**
4. **Manage risk as a portfolio**
5. **Prioritize decisions over documentation**
6. **Measure value, not activity**
7. **Run governance as a behavior system**
8. **Embed ERM into operating rhythms**
9. **Build candor as a capability**
10. **Learn continuously**

Strategy + Risk in Practice: Why They Must Be Linked

ERM creates the most value when risk is inseparable from strategy. Too often, strategy is treated as "where to play and how to win," while risk runs in parallel as registers and heat maps – reported after the fact. That split is artificial. **Strategy choices are risk choices.** The only question is whether they are made explicitly (with time to shape outcomes), or implicitly (by default).

The COSO ERM Framework is clear that enterprise risk management is not the strategy function: "Enterprise risk management does not create the entity's strategy, but it influences its development. An organization that integrates enterprise risk management practices into setting strategy provides management with the risk information it needs to consider alternative strategies and, ultimately, to adopt a chosen strategy.[1]" In practice, this influence is what many practitioners describe as ERM having a more strategic role, not owning strategy but being embedded early and continuously enough to shape the options leaders consider, the tradeoffs they debate, and the risks they choose to take.

The same logic must continue after the strategy is chosen. In today's environment – where AI, regulation, supply chains and customer behavior move quickly – annual strategy cycles paired with quarterly risk reporting aren't enough. Decision-useful ERM stays close to strategic decisions as they evolve, helping leaders take new risks deliberately, refine strategy in real time, and move faster with confidence.

Link strategy and risk while options remain

Sasha the Strategy Shaper

The team is green lighting a major initiative. Momentum is high. Someone says, "We've taken risks like this before – we'll manage it." Sasha pauses, not to slow the group down, but to keep the decision honest. "Maybe," Sasha says, "but we still need to be explicit about the return we're expecting for this level of risk. Before we commit, tell me three things: (1) what could derail this, (2) what risk we're intentionally taking to achieve the return, and (3) what would signal the trade-off no longer holds?" Momentum becomes clarity. Speed remains, but now it's disciplined. **This becomes the standing integration step: assumptions, trade-offs, triggers, owners, and a short decision record – done in minutes inside the meeting that already decides funding and pace.**

Linking strategy and risk means accepting that every strategic decision carries uncertainty. Strategy determines objectives and resource choices; risk shapes the range of outcomes those choices may produce as assumptions, external conditions, or execution realities change. In practice, linking strategy and risk means the strategy discussion always includes a short statement of the assumptions that must hold, the boundary conditions that will not be crossed, and the signals that will force a revisit.

Risk management is only as effective as the underlying strategy and objective-setting process.

In our discussions with practitioners, one theme came through clearly: risk management is only as effective as the underlying strategy and objective-setting process. When strategy-setting is a meaningful exercise, risk conversations become sharper because they have real choices, real assumptions, and clear measures to attach to. When strategy is vague, or when a strategy document exists but its components are not tracked over time, risk management has nothing solid to anchor to and drifts into abstraction.

When strategy and risk are treated separately, organizations don't avoid risk – they take it implicitly. Linking the two is the practice of making trade-offs explicit while options remain.

When ERM doesn't operate this way, it becomes peripheral busywork – artifacts without intelligence. Our survey[2] echoes this: many programs produce outputs; far fewer are integrated into strategy decisions or are perceived as a competitive advantage. That gap matters and highlights an aspiration to reality gap – organizations want ERM to matter more, but many programs still sit outside the moments where strategy is shaped and major bets are made.

Decision-useful ERM is not about updating heat maps or compiling RCSAs on a calendar schedule. Those artifacts matter only if they change a decision, trigger an action, clarify

1

OPERATING DISCIPLINE
Link strategy and risk

5

OPERATING DISCIPLINE
Prioritize decisions over documentation

[1] Enterprise Risk Management: Integrating with Strategy and Performance (COSO, June 2017, Page 35)
[2] Insights Into Practical ERM Application Survey (COSO and Crowe LLP, January 2026)

ownership, or fulfill a regulatory requirement. If ERM does not influence decisions, it is activity, not effectiveness.

Every strategic objective implies a risk posture, whether it's named or not. How much uncertainty will we tolerate? Which outcomes are unacceptable? Where will we invest to reduce uncertainty versus accept it? When these questions remain implicit, risk posture is set by default, often by urgency, recent events – or the loudest voice in the room. Making risk posture explicit doesn't require complex scoring models. It requires decision language leaders already use:

- **Trade-offs:** what we gain, what we give up, what we're choosing not to do
- **Ranges:** best case, expected case, downside case, upside opportunity, and what widens the range
- **Triggers:** what we'll watch, and what will cause action or escalation
- **Pivots:** what "stop, pause, or change course" looks like in practice

Decision-useful ERM is best understood by contrast. It is not defined by how many risks are catalogued, how often reports are produced, or how polished the visuals appear. It is defined by whether it helps leaders choose well. When ERM is decision-useful, it frames real options, focuses attention on uncertainty that matters, defines triggers that prompt action, and makes ownership and follow-through explicit. When it's not, ERM often shows up as long, unprioritized lists, generic scoring that does not change behavior, or after-the-fact reporting that arrives when leaders have little room to maneuver.

This is where the "opportunity lens" matters. ERM is often experienced as a cost because it shows up as an add-on: more deliverables, more updates, more meetings layered onto already full agendas. Viewed through an opportunity lens, ERM becomes a way to move faster with discipline. It preserves options by forcing early clarity on what must be true, reduces costly late-stage surprises, enables earlier and more affordable pivots – and supports value creation by helping leaders take the right risks rather than defaulting to avoidance or overconfidence. ERM also improves the quality of strategic and operating conversations, which often surface "other" opportunities leaders would not have named otherwise: process fixes that remove friction, investments that strengthen capabilities, or pivots that unlock growth. Bottom line: when ERM is decision-useful, the byproduct is not just better risk taking, but a better-run business.

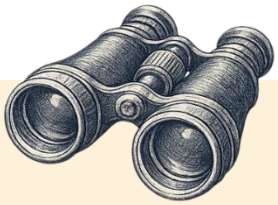
6

OPERATING DISCIPLINE

Measure value, not activity

Sasha the Strategy Shaper

By the end of the meeting, the team hasn't slowed down – they've sharpened. Sasha closes with a two-minute recap: "What are we choosing, what are we accepting, and what would make us change course?" The group agrees on the decision, names the critical assumptions, and agrees on three triggers that will force a revisit if conditions shift. Owners leave with clear follow-up, and the next update is obvious: what changed, what matters, and whether the decision still holds. That's what it looks like when risk isn't a separate exercise, it's part of how strategy gets made.



SURVEY SAYS

The implementation gap in practice

54%

of ERM programs most commonly perceived as a compliance or assurance function

28%

of ERM programs most commonly perceived as a strategic partner

7%

of ERM programs are fully integrated into strategy decisions

98%

of respondents believe ERM should play a more strategic role in their organizations

Prove value through protection and creation

Casey the Capital Keeper

Casey has two funding requests on the table. Both are well written, promise upside, and come with confident timelines and polished slides. But when Casey asks the simplest question, “What could change the outcome?” the answers get fuzzy. The teams can describe what they plan to do; yet they struggle to describe the uncertainty around whether it will work, how wide the range of outcomes might be, and what would cause them to change course. Casey isn’t anti-risk, he’s anti-unknowable risk. “If we can’t explain the risk-adjusted return,” Casey says, “it’s a hobby.” The room laughs, but the point lands.

This is where ERM earns its keep. The value isn’t more artifacts; it’s creating decision leverage – better choices under uncertainty and faster adjustment as conditions change. The value has two lanes that should always travel together:

Value protection is the most familiar side of ERM. It focuses on reducing volatility, preventing surprises, and safeguarding reputation and the license to operate – and there is nothing wrong with that. The problem arises when protection becomes the only story. When ERM is framed solely as prevention, it will always feel like a cost center, especially to leaders under pressure to grow, transform, and compete.

Value creation is the side of ERM that too often gets lost and is the hardest to operationalize. ERM creates value when it helps leaders place better bets, allocating resources with clearer trade-offs, setting boundary conditions for risk-taking, and building options that preserve flexibility.

Survey respondents highlight a critical mental-model shift: risk management is still widely seen as a compliance exercise, and many believe that risk management slows decision-making. The value equation challenges both assumptions: When done well, ERM should increase decision confidence and speed by clarifying trade-offs, triggers, and ownership.

ERM shifts from “cost” to “investment” when it is linked to outcomes leaders care about. That requires answering a simple leadership question: *What did ERM change this quarter?* Not what was produced, but which decisions were influenced, pivots enabled, or risks avoided through earlier action.

A short before-and-after makes the difference tangible.

Before: a leadership team approves a major investment based on a single forecast, a set of optimistic assumptions, and milestones treated as inevitable. ERM is asked to “review” it later; a risk register is created, and the board receives a heat map.

After: the same investment decision is framed differently. Leaders see ranges and scenarios instead of a single number and agree on a small set of triggers that force a revisit: missed adoption thresholds, regulatory slippage, changes in critical vendor dependency changes, or cost overruns. Ownership is explicit, and board updates are focused. And while risk isn’t eliminated, the quality of the bet and the speed of response improve. That is value creation and value protection working together.

Value creation shows up in a handful of repeatable ways.

- **Capital allocation:** scenario ranges and what widens them (not false precision)
- **Transformations:** thresholds and triggers drive early pivots; signals aren’t ignored
- **Portfolio view:** allows leaders to concentrate resources and avoid the accumulation of “medium risks” across initiatives that, in aggregate, create material exposure – a death by a thousand cuts

The practical goal: Don’t try to quantify everything – ERM should speak in the language of decisions. When leaders ask for more people or more effort, offer a value hypothesis: what uncertainty will be reduced, what decision will be improved, and what outcome will change as a result? That is how ERM becomes an investment tied to outcomes, not a calendar of deliverables.

2

OPERATING DISCIPLINE
Treat value creation as a required outcome

4

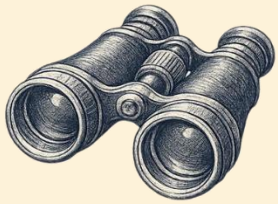
OPERATING DISCIPLINE
Manage risk as a portfolio

Casey the Capital Keeper

By the end of Casey’s funding review, the slides look the same, but the conversation is completely different. Teams leave with a clear request: come back with scenario ranges, assumptions that matter most, and three triggers that will change the plan if conditions shift. Casey hasn’t demanded certainty – just discipline. The decision still carries risk, but it’s taken with eyes open and guardrails in place.

SURVEY SAYS

What leadership behaviors or language have you found most effective in connecting risk and strategy conversations?



Set the tone from the top: CEOs and senior leaders visibly sponsor candid risk discussions in formal meetings and behind closed doors.	Position ERM as a "Department of Know, not No" that helps leaders make better strategic decisions, not slow them down.	Frame risk as an opportunity to secure the right change, resources, and investment.
Start with success: ask "what has to go right?" to surface the dependencies that could derail the strategy.	Keep the conversation balanced by weighing upside opportunities alongside downside risks.	Encourage leaders to "price for risk" so viability, return, and trade-offs are explicit instead of defaulting to avoid/minimize.

Translate the framework into a working operating system

Tahlia the Toolmaker

Tahlia is staring at a shared drive full of ERM templates – multiple versions of the risk register, heat maps in different formats, KRIs with inconsistent definitions, slide decks from past workshops, hundreds of RCSA results, and meeting notes that never turned into action. Leadership keeps asking for "framework-compliant ERM," but when Tahlia asks what value they want ERM to add, the answers vary: assurance, faster escalation, fewer surprises, better decision support. With no shared intent, the program drifts toward producing more things – instead of enabling better decisions.

The heart of translating the COSO ERM Framework into a usable operating system is turning principles into repeatable decision behavior, not more documentation. **A framework isn't a program.** A framework guides design by describing what strong risk management should achieve. A program is how an organization brings that intent to life. Treated as a checklist, teams often produce ERM programs that look complete on paper but do not function as part of how the organization actually runs. Treated as a **design space**, teams build ERM programs as operating systems that shape decisions and behaviors consistently, through rhythms leaders actually use.

In high-speed, less-regulated environments such as large technology firms, the concern isn't usually with the COSO ERM Framework itself – it's the perception that ERM introduces bureaucratic layers. As one risk leader explained, without a regulatory "hammer," ERM must tie directly to strategy and demonstrate ROI. In this model, ERM earns its place by speaking the language of the business and enabling speed. Real-time risk monitoring is technically straightforward – the harder challenge is proving it's worth building instead of delivering more products.

Regardless of industry, a practical operating system is built from a small set of reinforcing components:

- **Forums where risk-informed decisions actually happen.** These include weekly leadership huddles and operating reviews to product release checkpoints, sales pipeline reviews, program check-ins, and exception escalation routines. If ERM isn't present where priorities are set and trade-offs are decided, it remains peripheral.
- **A cadence that matches how the organization truly runs.** Risk conversations need to show up before and during the moments that matter: annual strategy and planning, monthly performance reviews, quarterly reforecasting, investment approvals, and major delivery milestones. The goal is not to create a separate "risk calendar," but to align with existing rhythms so uncertainty surfaces early enough to shape choices.
- **Triggers that convert awareness into action.** Effective operating systems rely on a small set of thresholds that leaders recognize and owners can monitor. Good triggers are tied to objectives and assumptions, paired with a clear response, and revisited at the right frequency. Without triggers, risks remain observations. With triggers, risk becomes a series of defined decision points.

7

OPERATING DISCIPLINE

Run governance as a behavior system

- **High-leverage artifacts that travel with the schedule.** These artifacts are short, consistent, and built for real-time use: a one-page decision brief (choice, options, ranges, triggers, owner), a simple action log that tracks follow-through, and board updates that lead with what changed and what decision is needed. Artifacts exist to support action, not to prove activity.
- **Clear ownership and follow-through**. Business leaders own risks because they own the outcomes. The ERM team provides consistency, visibility, and effective challenge.

This model can be scaled but shouldn't be diluted. If any one component is missing, the system tends to collapse into busy work. Without forums, ERM becomes reporting. Without cadence, it becomes episodic. Without triggers, it becomes descriptive. Without disciplined artifacts, it becomes noisy. Without ownership, it becomes performative.

A practical operating system also depends on who helps shape it. Several interviewees noted that bringing in talent from operational and business roles to work within the risk function – even temporarily – accelerated adoption. When people who have carried targets, managed constraints, and owned delivery help shape the ERM approach, the work becomes more grounded, language becomes more practical, and leaders are more likely to trust the outputs. This can take the form of rotations or secondment for a strategic initiative or a small bench of "risk partners" embedded in business units who help translate risk appetite, triggers, and trade-offs into decision-ready inputs.

Most importantly, **"minimum viable" ERM does not mean "minimal effort**." Minimum viable ERM means focusing on the few elements that actually change decisions. Programs often start with a short list of priority risks tied to strategic objectives, a small set of triggers for each, and a real forum where leaders make decisions and track follow-through. Mature programs build by embedding risk into planning, capital allocation, and major transformations – and proving value through measurable indicators, such as decisions influenced, pivots enabled, and fewer surprises. Over time, the operating system becomes less visible as "ERM" and more about **how the business runs.**

The COSO ERM Framework is most useful when it is treated as design guidance for how ERM should function inside the business, not as a list of outputs to produce. The test is simple: does your approach create clearer choices, earlier pivots, and visible ownership as conditions change? The Framework is a map. The operating system is the vehicle.

Our survey reinforces this: Respondents most often cite a sustainable, efficient approach as the single most effective action to advance ERM maturity, followed by developing risk appetite statements. Maturity improves when ERM is designed as an operating system leaders use and appetite becomes usable in real decisions.

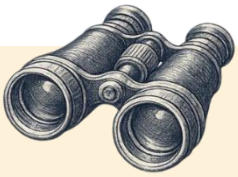
8

OPERATING DISCIPLINE

Embed ERM into operating rhythms

Tahlia the Toolmaker

Tahlia's documentation simplification is not less rigor. It is clearer intent and cleaner execution. When ERM is designed as an operating system, leaders engage more readily, teams execute more consistently, and boards get clarity instead of volume. Most importantly, it becomes easier to stop producing low-value artifacts and invest in the few elements that actually change decisions.



SURVEY SAYS

Name a specific example where ERM insights directly influenced a strategic decision or business outcomes?

Energy
North America

ERM highlighted concentration risk in a specific market segment, influencing a decision to exit a product line.

Technology
North America

ERM surfaced technology risks (for example, software design practices and technology debt) during enterprise risk review, leading to a concrete response strategy and action plan that materially improved the risk profile.

Financial Services
Europe

ERM recommended pens down with a broker facing bribery charges given the risk of potential fines impacting our outstanding premiums owed.

Transportation
North America

ERM engaged midstream in a strategic departmental project and helped shift to a more measured approach, reducing significant people and vendor risks.

Healthcare
Asia-Pacific

ERM used an annual risk workshop with the Board to inform the strategic plan.

Industry Snapshots: ERM in Action

Aligned and Advantageous: ERM as a Competitive Edge

Watching what great ERM looks like – and where it breaks – helps leaders tune their own programs. **Based on our interviews with industry leaders**, these snapshots illustrate how ERM maturity shows up in practice: in the conversations leaders have, the analytics they rely on, and the culture they reinforce.

WHO / INDUSTRY:
CRO / Financial Services

PROFILE:
Mid- to large-size retail brokerage / wealth platform with a relatively straightforward business model (no proprietary trading; limited balance-sheet risk). Built ERM largely from a clean slate. Uses the COSO ERM Framework alongside regulatory guidance to shape an ERM approach anchored in operational, conduct, and compliance exposure. Strong "tone from the top" sponsorship, with board and executive leadership expecting ERM to support fast, high-confidence decisions.

What they did

With little ERM structure in place, the CRO chose to redefine the role of risk from the start – focusing on how risk would be used in decisions rather than building out full ERM processes and documentation first. He recognized that teams often get caught up in ERM mechanics before changing the underlying behaviors that make risk meaningful. Instead of positioning ERM as a gatekeeper, he framed it as a **decision-support function**, focused on helping leaders find "a pathway to yes" through practical controls and resourcing – not preventing action. That reframing immediately shifted how the business perceived risk and opened the door for genuine partnership.

"Our job wasn't to say 'no.' It was to map a credible 'yes' – with the controls, resources, and tradeoffs spelled out."

To build credibility quickly, he hired **business-savvy risk talent** – people who understood products, operations, and profit and loss (P&L) deeply enough to show up with their own point of view. Rather than ask broad, unhelpful questions like, "What keeps you up at night?" or "What are your top risks?" the risk team came prepared to discuss the business in the business's language.

From there, the CRO worked with senior leaders to translate strategy into a **clear, concise Risk Appetite Statement**. It laid out, in plain terms, what risks the firm would and would not take in pursuit of strategy – such as avoiding proprietary positions and balance-sheet leverage. This became the first screen for evaluating new initiatives. Misalignment didn't lead to an automatic "no," but to a structured conversation and, when appropriate, escalation to the board.

"When your CRO tells you to take more risk in a defined area, it gets attention – because it's grounded in understanding the business."

The CRO also **distributed ownership** of major risk categories across the executive team, assigning leaders responsibility for enterprise-level risks beyond their silos. These executives regularly presented to an ERM Committee attended by the CEO, which helped embed risk thinking into day-to-day leadership behavior.

Finally, the CRO grounded ERM's value in **hard operational loss data**. By establishing a disciplined process for capturing events and losses, the company reduced loss levels dramatically, directly supporting quarterly earnings performance and proving ERM's tangible financial impact.

"Every dollar of avoided loss flows to earnings per share. That got the street's attention."

Key takeaways:

- Equip ERM to show up with a POV – and a "pathway to yes."
- Keep the RAS short, specific, and board-owned – but living (update when crypto/AI/other new risks emerge).
- Anchor credibility with hard outcomes (event/loss data, trend lines).

Industry Snapshots: ERM in Action

Designed with the Business: ERM as a Connector and Insight Engine

Who / industry:
Director of ERM / Transportation

Profile:
Large, operationally complex transportation services organization that formalized ERM after board concern about fragmented, non-repeatable risk reporting. ERM built largely from a clean slate and led by a small, central team. Uses a hybrid, COSO-informed approach tailored to operational realities and existing governance structures. Strong operational, safety, and regulatory risk presence; growing executive and board engagement.

What they did:
When the organization committed to standing up a formal ERM function, the director of ERM began by **co-designing the program with executives**, rather than arriving with a prebuilt model. The team spent time understanding how leaders made decisions, tested early drafts of the taxonomy and scoring approach with them, and refined the structure until it felt intuitive and business-owned. This collaborative start gave the program immediate credibility.

"ERM only works if leaders can see themselves in the process – and see how it helps them decide faster and better."

Using COSO as the foundation, the director built a **hybrid, business-fit ERM framework** that incorporated practical impact lenses – operational, regulatory, cyber, and people – to reflect how the organization actually manages risk. This multidimensional view aligned with how the organization actually managed its risks, and made the process more relevant to day-to-day operations.

Risk accountability was clarified early. Major enterprise risks were assigned directly to executive owners, reinforcing that ERM was a **leadership responsibility**, not a risk or compliance reporting exercise. Executives reviewed their risk narratives with the director before anything advanced to the audit committee, ensuring alignment and clarity.

"The gap between how the board sees risk and how management sees it isn't a problem – it's the conversation."

As the process matured, the director invited the audit committee to participate directly in the assessment. Board input – kept separate from management – surfaced natural differences in strategic versus operational perspectives and led to richer discussions before formal board meetings.

To strengthen risk conversations, the director replaced static heat maps with **dynamic dashboards** integrated into the organization's GRC system. These dashboards highlighted trends, mitigation confidence, and emerging issues, helping leaders focus on evolving conditions rather than static visuals.

Finally, the director embedded himself across operational, safety, and continuity committees, becoming a **connector** across the enterprise. These touchpoints helped risk insights travel across silos and upward, informing audit planning, capital discussions, and early detection of cross-functional risks.

Key takeaways:

- Design ERM *with* leaders to create ownership and longevity – not compliance.
- Use dynamic data and analytics to shift conversations from scoring to insight.
- Pace maturity intentionally – credibility first, board participation second.

Practitioner Translation Guide:

Applying the COSO ERM Framework to Power Real-World Decisions

9

OPERATING DISCIPLINE
Build candor as a capability

The previous section made the case for a decision-led approach to ERM: treating risk as part of every strategic choice, recognizing that value includes both protection and creation, and using the COSO ERM Framework as an operating system rather than a checklist. Many organizations agree with these ideas in theory yet still experience an execution gap. Risk assessments drift into scoring exercises, risk appetite remains abstract, governance roles blur, and board updates emphasize information volume instead of clarifying what's changed and what decisions are needed.

The COSO ERM Framework is intentionally principles-based – a strength that allows it to apply across industries, geographies, and maturity levels – and leaves room for management judgment. The challenge is translation: how teams convert that intent into repeatable behaviors at the point of decision, and into outputs that leaders and boards can actually use.

Some of the barrier is technical, but much of it is cultural. In interviews, leaders emphasized that elevating ERM requires the CRO and leadership team to be bold, and normalize candid conversations about uncertainty. Survey results reinforce this: Only 20% of respondents report high psychological safety in leadership discussions. That number matters because it sets a hard ceiling on effectiveness – if leaders don't feel safe to surface concerns or challenge assumptions, even a well-designed ERM program will be diluted in the moments that count. Where leaders cannot speak plainly about uncertainty, triggers, and trade-offs, ERM becomes either performative or disconnected from real decisions**.** Where candor is normalized, ERM becomes usable. One interviewee captured the standard bluntly: if a risk position "can't withstand the scrutiny of light," it won't hold up over time. That standard requires ERM leaders to surface uncomfortable truths early – including when the honest answer is "not yet" or "not on these terms."

Where leaders cannot speak plainly about uncertainty, triggers, and trade-offs, ERM becomes either performative or disconnected from real decisions.

This is why culture shows up throughout the practices that follow. Our survey shows a persistent cultural gap (>80%) between how organizations talk about risk and how they talk about strategy, marked by different language, limited influence on decisions, and misaligned incentives. Closing that gap requires building candor, influence, and shared language.

With that foundation, this section translates the COSO ERM Framework's intent into practice. It shifts three common sticking points into concrete behaviors, usable triggers, and decision-ready outputs.

Risk assessment that informs decisions (not scoring theater)

The COSO ERM Framework is clear that severity is not a single point estimate. "There may be a range of possible impacts associated with a risk."[3] Yet under time pressure, many organizations reduce assessment into a likelihood-by-impact score and a heat map. These outputs look clean and comparable but often steer the discussion toward scoring rather than what leaders actually need: what could happen, how bad it could be, what would change our plan, and when would we act? They also embed a flawed math assumption: likelihood × impact approximates "expected loss," while many leadership and board decisions hinge on "unexpected loss" and volatility: tail outcomes, concentration, and the speed at which conditions can shift. A single score can obscure the range that actually drives whether you proceed, pause, or redesign.

This dynamic shows up in both enterprise-wide (top-down) assessments and in process-level (bottom-up) assessments – what changes is the entry point, not the requirement for decision usefulness.

When psychological safety is low, scoring tools can make things worse. In a typical top-down enterprise risk assessment, no leader wants to be the person owning a high score, so the conversation quietly shifts from *what uncertainty could change the decision* to *defending a lower score*. Teams end up negotiating likelihood and impact to move a bubble out of the upper-right

[3] Enterprise Risk Management: Integrating with Strategy and Performance (COSO, June 2017, Page 116)

corner. The presentation has improved; the underlying risk exposure has not.

The same pattern shows up in bottom-up assessments like RCSAs. The issue isn't the RCSA itself – it's the implicit purpose it takes on: a mandate to demonstrate that risks and controls have been assessed rather than a mechanism that changes how the organization decides or acts. What makes an RCSA valuable is not completeness, but what it enables: surfacing meaningful exposure, forcing conversations and escalation, prompting investment or corrective action, and translating risk into language leaders can use.

Even in regulated environments, "the regulator requires it" shouldn't be a permission slip for low-value work.

Even in regulated environments, "the regulator requires it" shouldn't be a permission slip for low-value work. A decision-useful risk assessment starts with a different question: **What decision are we trying to make, and what uncertainty could change it?**

Sasha the Strategy Shaper

For Sasha, the difference is simple: an assessment that slows the conversation versus one that sharpens the decision.

Tahlia the Toolmaker

For Tahlia, it's the moment ERM stops being a template exercise and becomes decision input, because the output tells leaders what to do next, not just what to rate.

This doesn't remove the need to understand relative risk. Leaders still need clarity on what matters most. What changes is the way that clarity is achieved. Instead of relying on a single score to rank risks, decision-useful assessments compare risks based on the outcome ranges, the speed at which conditions could shift, and the degree to which they could disrupt strategic objectives. This helps leaders focus on the risks most likely to alter their plans.

From there, good assessments make uncertainty usable. It frames a small number of scenarios that reflect meaningful differences in outcomes – including at least one disruption case that would force a pivot. It uses ranges where precision is not available and makes assumptions explicit instead of hiding them inside a number. It also acknowledges that risks interact. Not every assessment needs a complex portfolio model, but teams should surface interdependencies when one risk materially changes another, or when multiple risks converge on the same objective.

The COSO ERM Framework also emphasizes that assessment should be dynamic, not static. "The organization strives to identify triggers that will prompt a reassessment of severity when required."[4] Triggers shift risk assessment from static scoring to dynamic oversight. Here, triggers are not risk appetite limits. They are the few indicators that tell you conditions have shifted enough that your risk assessment should be revisited – your scenario range, severity view, or response.

This is where data and analytics matter most. Triggers only work when they can be monitored with minimal friction – ideally through data leaders already trust, such as operational KPIs, delivery metrics, financial indicators, incident trends, vendor performance, and customer signals. Even simple automation – standard thresholds, exception flags, trend views, and alerts – can shift ERM from episodic assessment to continuous awareness.

A practical starting point is to apply this approach to one priority decision. Replace the scoring conversation with two scenarios and a range (base case and downside/disruption), plus a short note on what would widen the range. Then define two triggers that would force a revisit, assign an owner to monitor them, and specify what happens when a trigger is met. The value is not sophistication – it's **earlier pivots, clearer trade-offs, and faster decisions with fewer late surprises.**

Two traps appear consistently:

- **False precision and average-case bias.** If the data isn't strong enough to quantify likelihood or impact, don't pretend it is. Likelihood × impact discussions drift toward "average" outcomes, even though the decisions that matter often hinge on volatility, tail scenarios, and how quickly conditions can change.
- **Analysis paralysis**. The purpose of assessment isn't to model every possibility. It's to identify the few uncertainties that could change the decision and define how the organization will respond as those uncertainties move.

[4] Enterprise Risk Management: Integrating with Strategy and Performance (COSO, June 2017, Page 120)

Risk appetite that is usable (thresholds, triggers, actions)

3

OPERATING DISCIPLINE
Make risk appetite meaningful and usable

COSO is explicit that risk appetite is meant to **guide choices**, not decorate a policy document. "Risk appetite provides guidance on the practices an organization is encouraged to pursue or not pursue. It sets the range of appropriate practices and guides risk-based decisions rather than specifying a limit."[5] At its core, risk appetite represents a shared understanding between the Board and management about which risks are worth taking in pursuit of strategy, and which are not. The Board's role is to endorse those boundaries; management's role is to translate them into decisions, thresholds, and actions.

In practice, risk appetite often stalls because it remains high-level and disconnected from day-to-day decisions. The issue is rarely that a risk appetite statement doesn't exist – it's that it's too abstract to use. A useful appetite expression is rarely a single sentence. It is strategy made explicit under uncertainty – a small set of choices that guide where the organization will be conservative and where it will take disciplined risk.

Today's risk environment demands risk appetite to function as **clear decision boundaries**. This isn't just about influencing a single decision in the moment; it's about improving priorities and follow-through, so risk insights consistently shape outcomes.

Dana the Director

For Dana, usability means she can see the boundary and the consequence – what management will do as the organization approaches it.

Ravi the Risk Builder

For Ravi, usability means appetite translates into triggers, escalation paths, and decision rules that operate week-to-week without heroic effort.

In many organizations, appetite statements sound reasonable but don't change behavior. They're endorsed and disseminated, then rarely referenced when decisions get difficult. When leaders revert to intuition or urgency, appetite becomes background noise – one reason ERM is often viewed as a compliance function rather than strategic.

The translation is straightforward: convert appetite into a small set of decision boundaries linked to thresholds, triggers, and actions. Consider a bank deciding whether to expand into higher-yield lending. Absent a usable risk appetite, the discussion tends to remain abstract – growth weighed loosely against risk. With a clear appetite, leadership sets an explicit boundary: acceptable loss levels relative to return. They define a trigger: if early delinquency indicators exceed that range, originations tighten and underwriting adjusts. The decision still carries risk, but it is taken deliberately, with explicit boundaries and a defined path to adjust. In this way, risk appetite becomes a clear basis for decisions, not a statement on paper.

In practice, leaders should be able to answer three questions without reaching for a policy document:

1. **What are we willing to accept** in pursuit of our strategy?
2. **How will we know** we are nearing the boundary?
3. **What will we do** if we cross it?

If the answers don't end in a clear "then we will…," appetite is still abstract.

One CRO we interviewed illustrated this translation with a deliberately simple dashboard: a red/yellow/green "stoplight" view where each status is tied directly to a measurable risk appetite threshold – and how far conditions had drifted from that target. The point wasn't to introduce another scoring ritual; it was to give leaders a quick read on "in bounds vs. out of bounds," supported by trusted metrics and a pre-agreed escalation with the Board when the light changed. Many teams begin with areas where measurement maturity is already strong – often treasury-owned risks like credit, liquidity, or interest rate – and extend the same logic to harder-to-measure exposures as the trigger discipline improves.

The hardest part for many teams isn't mechanics – it's committing to thresholds at all. Many leaders hesitate to "put their neck out" by naming limits for worry of being wrong. But usable appetite is an art, not a one-time calculation. It improves through iteration, learning, and adjustment as conditions change. Treat thresholds as working hypotheses: define them, run them for a cycle, learn, and adjust without blame. Psychological safety matters here. When leaders can speak candidly about uncertainty and revise boundaries as conditions change, appetite becomes a living tool rather than a static statement.

[5] Enterprise Risk Management: Integrating with Strategy and Performance (COSO, June 2017, Page 46)

A practical starting point is to begin with your existing risk appetite statement and pressure-test it for usability on a small set of priorities. Select five risks tied to delivering key strategic objectives and translate the relevant appetite language into a single decision boundary for each. Then define one trigger, assign an owner who monitors it, and specify the escalation action if that trigger is met. Treat these initial thresholds as working hypotheses, not permanent limits: document the assumptions, pilot them for one cycle, and refine based on what you learn. Finally, test usability: can a leader apply the boundary to a real decision in under 60 seconds? If not, it needs to be simplified.

Two watch-outs matter here:

- **Avoid "statement only" appetite**. Without thresholds and actions it will not influence decisions.
- **Avoid over-engineering**. A long list of metrics no one monitors and a dashboard no one owns is less effective than a few well-chosen metrics leaders trust.

As appetite matures, emphasize the outcome it is meant to enable: clearer priorities, earlier action, and fewer surprises – so strategy is executed with intention, not just speed.

Board reporting that is communication (not compilation)

The COSO ERM Framework frames board communication as an enabler of oversight and timely response – not a packaging exercise. It's guidance is practical: "Communicating about risk starts by defining risk responsibilities clearly: who needs to know what and when they need to act.[6]"

Dana the Director

For Dana, board-ready risk reporting is clarity: what changed, why it matters, and what you want the board to decide, endorse, or challenge

Ravi the Risk Builder

For Ravi, it's a repeatable format that builds trust over time and supports escalation when signals move.

The most common breakdown is that board materials become compilations. In an effort to be complete, teams include everything – registers, heat maps, KRIs, narratives, and RCSA results. Signals get buried. Directors receive information but not orientation. The conversation shifts to passive review instead of active oversight, and the board ask becomes unclear or disappears altogether.

Decision-useful board reporting starts with discipline about purpose. The board's role is oversight, so reporting should focus on what oversight requires:

- What has changed since the last update
- What matters most now
- What management is doing
- Where the board needs to decide, endorse, advise, or challenge

COSO's emphasis on linking risk information to strategy, objectives, appetite, and tolerance is critical here. If an update does not show how current conditions compare to stated boundaries – and what management will do as the organization approaches them – directors cannot judge whether risks are being managed appropriately. One of the cleanest ways to make that linkage real is to include loss and event signal in the board discussion – not as a catalog, but as a trend and a learning loop. Material losses, near-misses, and recurring events reveal where the operating system is working (or not), and often reveal where assumptions, controls, or resourcing need to change.

A practical next step is to spend 10–15-minutes with the committee chair (or a trusted director) to confirm their top questions and where they want clearer triggers or decision points at the next meeting. Then replace the risk section of the board packet with a concise, decision-ready summary of the top priorities, with supporting detail behind it. Use the four-question structure above as the organizing frame. For each priority topic, include one trigger, name the owner, and state the action or escalation path if the trigger is met. Add a short trend line or forward-looking indicator where it materially improves oversight. Keep the appendix detail available, but don't let it bury the headline.

Two watch-outs show up frequently:

- **Don't let the heat map become the headline.** If it's the first thing directors see, the discussion often drifts to colors and scoring instead of what changed, what matters, and what management will do.
- **Don't treat completeness as the goal.** Boards don't need everything; they need a complete, decision-ready discussion of the top priorities. Clarity, actionability, and consistency over time are what build confidence.

10

OPERATING DISCIPLINE
Learn continuously

OPERATING DISCIPLINE
Learn continuously

[6] Enterprise Risk Management: Integrating with Strategy and Performance (COSO, June 2017, Page 156)

Final Thought

These translations are substitutions, not add-ons. They replace familiar but low-leverage habits – scoring debates, abstract appetite language, after-the-fact reviews, and board packets that compile rather than clarify – with a small set of repeatable behaviors that make ERM decision-useful. Start small: choose one sticking point and apply the practical starting point steps to an existing decision moment. Once leaders feel the lift – clearer trade-offs, earlier pivots, visible ownership, and cleaner escalation – scale from what works.

The next section turns these same practices into a concrete, five-hour-a-week operating rhythm, enabling an effective ERM program even when time is scarce. If you have a larger team, treat this as a minimum viable baseline or jump ahead to the ERM Operating Disciplines to select the practices you want to institutionalize at scale.

Quick-Start:
ERM Under Constraints

Most ERM teams are expected to deliver value long before they can build a perfect program. Time, capacity, and leadership attention are limited. Delivering value has less to do with producing more artifacts and more to do with delivering decision-ready signal and clear ownership, even when resources are tight.

This section introduces a lean operating model designed for constraints. You can use it as a minimum viable baseline – whether you're a CRO-of-one or part of a large team**.** It is intentionally lean and built to help Ravi sustain an ERM program with limited hours, and to help Dana get what she needs in the minutes available. The goal isn't completeness, it's to get a grip on what matters now, clarify what would make leaders change course, and build the ability to pivot early.

Ravi the
Risk Builder

Ravi looks at his week and sees roughly five hours available for ERM – scattered between competing demands, urgent requests, and the reality that risk does not pause when calendars fill up.

Meanwhile, Dana has a board committee meeting coming up, and risk is one item on a busy agenda. Dana has about fifteen minutes of attention before the discussion moves on. Ravi has learned that if the update doesn't get to the point quickly, Dana will tune out – not because she doesn't care, but because she has a fiduciary duty to focus on what matters and isn't positioned to help if the signal is unclear.

Dana the
Director

Under pressure, Ravi's instinct could be to update the register, refresh the heat map, and assemble another deck. But Ravi understands the uncomfortable truth survey respondents reflected: **When ERM is seen as a compliance function, it's often because it produces outputs disconnected from decisions.** Leaders see activity but don't feel value. Instead, Ravi decides to run ERM like an operating system. He has five hours to create signal, clarify trade-offs, and drive follow-through – and fifteen minutes to earn board confidence with clarity.

Signals (1 hour)

Ravi starts with one question: *What changed?* The goal isn't to search for every risk but to identify shifts that could affect outcomes – leading indicators, emerging issues, and early warning signs from operations, finance, regulatory developments, cyber, third parties, or key markets. He doesn't try to build a new dashboard. He pulls from the operational and financial data streams the business already uses and looks for exceptions, trend breaks, and threshold breaches tied to predefined triggers. Where possible, he automates this scan – using basic analytics, alerts, or AI-assisted summarization of unstructured inputs like incident notes and customer complaints – so the signal list can be refreshed quickly and discussed consistently. The output is a short list of signals that could change a decision, trigger an escalation, or shift priorities or actions already in motion.

Decision framing (2 hours)

Ravi then prepares decision-ready insight for one or two priority topics. This is where ERM becomes strategic. Ravi focuses on the decisions that matter most right now – tied to strategy execution, transformation delivery, or a shifting material exposure. For each, he frames: the decision at hand, the uncertainty that matters, the options, and the triggers that would prompt a pivot. He states the assumptions explicitly and defines what pause, stop, or change course means in practice. This replaces generic risk scoring.

Business touchpoints (1 hour)

Ravi connects with leaders who will use the risk insight or own the response. Quick conversations with key general managers surface operational reality and confirm whether triggers are realistic, while a check-in with Sasha the Strategy Shaper ensures the framing fits the decision context and supports momentum. These are not stakeholder management meetings – they are how ERM becomes shared ownership and how insight gets converted into action.

Follow-through (1 hour)
This is where many programs quietly fail. Risks are discussed and then drift. Actions are assigned but untracked. Escalations happen only when something breaks. Ravi uses this hour to confirm owners, deadline, and escalation paths, and to capture what changed – and why. Over time, this discipline of learning and follow-through – not a quarterly slide cycle – is what builds credibility.

This weekly five-hour schedule produces exactly what Dana needs in fifteen minutes at the board meeting: an update that includes the top two or three changes and why they matter – and concludes with the board ask. The update is short because it is designed for governance, not completeness.

This approach also supports resource conversations. Every ERM program eventually asks for more capacity. Ravi uses a value test. If we request more people or time, what direct measurable improvement will it produce – in decisions, speed of pivots, or reduction of surprises? Survey results highlight a perception gap here: ERM becomes a competitive advantage *only* when leaders experience it as decision support – and see a clear link between risk insight and performance outcomes.

Equally important is what Ravi stops doing. Under constraints, cutting noise often produces the biggest gains. Ravi stops updating unused artifacts, narrows the register to risks tied to objectives, standardizes to one decision memo format, and avoids new templates unless they replace old ones. This isn't laziness – it's designing for sustainability. Survey respondents cite efficient, sustainable design as the most effective action to advance ERM maturity. A program that collapses under real-world constraints cannot mature. It will exhaust itself.

Ravi the Risk Builder

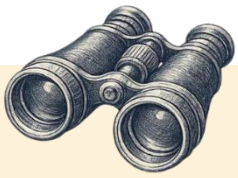
By week's end, Ravi is not claiming every risk is covered. He is claiming something more valuable: The organization has a clear view of what changed, what matters, and what will trigger action. Priority decisions are framed with trade-offs and options. Owners understand what they are accountable for.

Dana can do her job effectively because the update respects her time and is designed for oversight, not for compilation.

Dana the Director

This is ERM as a strategic capability under constraints. Not bigger – sharper. It earns attention by respecting attention and builds credibility by making uncertainty usable.

You've now seen a minimum viable rhythm for running ERM when attention is scarce. Next is the ERM Operating Disciplines section you can use to translate these ideas into a small number of moves that fit your context. Don't try to do all of them. Mark the two or three that would change what happens in a real meeting this month, and start there.



SURVEY SAYS

What leadership behaviors or language have you found most effective in connecting risk and strategy conversations?

Start small with maybe the top 5 or so risks and really try to develop those well before expanding out significantly.

Find senior leadership sponsors who will help get ERM in the room – and build engagement with the board so risk insights inform strategic discussions.

Build a network of influencers, meet regularly, and look for practical ways to help, including the unglamorous work that removes friction for the business.

Engage, learn, and communicate. Partner closely with the business so you can translate ERM into value people recognize, and be patient because it is a marathon.

You get invited to the party when you bring great gifts! Bring meaningful insights and data that improve the conversation and earn your seat at the table.

Bring talent in from front lines and support functions to broaden your ERM mindset.

ERM Operating Disciplines

The operating disciplines that follow represent the practical and impactful ways organizations put risk principles into action –shaping decisions where uncertainty and performance pressures are highest. Each discipline is intended to change something observable: how a decision is framed, how uncertainty is surfaced, how escalation works, or how follow-through happens.

Drawn from patterns observed in practice, these disciplines align with the intent of the COSO ERM Framework while translating it into real-time behaviors leaders can apply. They are deliberately flexible so they can fit organizations with different structures, risk profiles, and levels of maturity. For navigation, the ten disciplines are grouped into five themes: Strategy and Value, Enterprise View, Decisions and Proof, Governance in Motion, and Culture and Adaptation – reflecting the primary capability each discipline strengthens.

These disciplines are not meant to be adopted as a checklist. They are meant to be applied with judgment, starting with the few that address your biggest pain points. Begin small, apply the quick-start behaviors, and expand only after they are improving decision clarity and outcomes.

1. Link strategy and risk

The uncomfortable truth

Every strategy carries risk. The only question is whether leaders discuss it early – when choices can still be shaped – or later, when options are limited and reversals are expensive. Ignoring risk doesn't make strategy bolder. It makes leaders blind to the tradeoffs they are already making.

What this means

Risk is not a separate discussion. It is embedded in the assumptions, tradeoffs, and resource choices that make strategy work. When those assumptions aren't named, risk remains invisible until results force the conversation.

What ineffective strategy discussions look like

- Strategy is framed as certainty rather than a set of assumptions
- Key uncertainties are left implicit
- Downside is deferred until after approval
- Risk is addressed later as oversight or damage control

When uncertainty isn't discussed upfront, risks don't disappear – they simply show up later as an unexpected outcome. By then, options are limited and course correction is costly.

How to run strategy discussions that work

- Explicitly state the few assumptions that must hold
- Define which outcomes are unacceptable
- Agree on what would trigger a revisit or pivot
- Revisit assumptions at natural checkpoints: planning, performance reviews, and major investment decisions

Risk doesn't slow strategy. It sharpens decisions – by illuminating both what could go wrong and where upside could be lost.

QUICK START BEHAVIOR

For one strategy or major initiative already on the agenda, address the following questions:

1. What are we trying to achieve?
2. What must be true for this to work?
3. What could realistically go wrong and how severe could it be, i.e., what are the unexpected risks?
4. What outcomes would make this no longer acceptable – or leave meaningful upside uncaptured?
5. What would trigger us to revisit or stop the decision?

Connecting strategy to risk is an act of discipline. When these answers aren't clear, exposure remains implicit rather than understood.

2. Treat value creation as a required outcome

The uncomfortable truth

ERM is often judged only by what it prevents. When risk is framed solely as avoidance, it becomes a cost to be managed rather than a capability leaders depend on. Organizations don't invest in ERM to say "no" more often, they invest in it to place better bets, capture opportunity, and pivot sooner when conditions shift. When upside isn't considered, the risk isn't just loss, it's the value left on the table. It shifts the role of ERM from maintaining and remediating to actively shaping better outcomes.

What this means

Protecting value and creating value are not separate activities. Both rely on the same discipline: making decisions with uncertainty visible and trade-offs explicit. ERM creates value when it improves how leaders choose, not just how they control.

What ineffective ERM looks like

- Risk discussions focus on controls, limits, and compliance
- Downside is documented, but choices remain unchanged
- ERM is brought in late, after direction is already set

Risk is acknowledged. Value is unchanged.

What effective ERM does differently

ERM doesn't reduce risk-taking – nor should it; it makes risk-taking more deliberate. It helps leaders:

- Compare options using ranges and scenarios, not single-point forecasts
- Clearly state the trade-offs being accepted
- Agree in advance on what would trigger a pause, pivot, or reallocation
- Surface second-order opportunities: process improvements, capability gaps, or strategic adjustments

The result: leaders move faster with more confidence, and pivot sooner when assumptions stop holding.

QUICK START BEHAVIOR

For one major decision this quarter, require risk input that meaningfully improves the choice:

- A small set of scenarios with ranges, not point estimates
- The key assumptions behind the preferred option
- Signals that those assumptions are weakening
- The action taken if that happens

If risk doesn't improve the decision, it isn't creating value.

3. Make risk appetite meaningful and usable

The uncomfortable truth

Risk appetite often exists only on paper. It fails in practice when it cannot guide real decisions in real time. When disconnected from strategy, it becomes a statement of intent rather than a tool for choosing and adjusting strategic bets.

What this means

Risk appetite is not a belief statement; it is the mechanism that translates strategy into boundaries for action. It should help leaders quickly understand what is acceptable, what is not, and when conditions require a change of course or escalation. If appetite cannot be applied under pressure, it isn't doing its job.

What ineffective risk appetite looks like

- Broad language that sounds right but guides nothing
- Statements that require interpretation instead of enabling action
- Leaders reluctant to set thresholds for fear of being "wrong"
- Appetite discussed annually but ignored as strategy and conditions shift

The intent is clear. The connection to strategy and decision-making is not.

What meaningful risk appetite looks like

Leaders can explain, in plain terms:

- What is out of bounds given the strategy
- What is tolerable but needs monitoring
- What conditions would force a strategic decision, escalation, or stop

This guidance is tied to measures the business already uses, with:

- Defined thresholds
- Named owners who monitor them
- Agreed actions when thresholds are crossed

When risk appetite is built this way, it becomes the practical mechanism through which strategy is governed – not something recited in principle.

QUICK START BEHAVIOR

Apply an existing risk appetite statement to a current strategic or operational decision and assess whether it provides clear, actionable guidance. If leaders cannot quickly determine acceptability, escalation, or required action, the statement needs simplification. Start by defining one measurable threshold or trigger tied to the strategy and refine it over time rather than waiting for perfection.

4. Manage risk as a portfolio

The uncomfortable truth

Organizations rarely fail because of a single risk. They falter when multiple risks collide, amplify one another, or tap into the same constrained resources. What seems manageable in isolation becomes damaging in combination.

Most leaders sense this intuitively, but few have a clear way to see it.

What this means

Risk does not live neatly within individual initiatives, functions, or registers. It builds across the enterprise. While risks are assessed in the context of specific decisions, they must be managed as a portfolio – balancing multiple exposures, trade-offs, and resource competition.

ERM creates value when it helps leaders understand where risk is concentrated, how risks interact, and where trade-offs are being made implicitly instead of deliberately. A portfolio view transforms scattered concerns into something leadership can actually see, manage, and prioritize.

For example, an aviation company may face fuel price volatility, labor constraints, fleet availability issues, and operational disruptions at the same time – all competing for the same limited resources. These risks are interconnected. Adjusting flight schedules to address crew shortages can reduce revenue, while deferring maintenance to preserve capacity can increase operational risk. Like managing a portfolio, leadership must prioritize based on where risk is most concentrated, how exposures are shifting, and the trade-offs involved. In this view, risk is less about managing isolated challenges and more about prioritization and resource allocation.

What ineffective ERM looks like

- Risks assessed individually and in isolation
- “Medium” risks accepted repeatedly across multiple initiatives
- Shared dependencies – people, platforms, vendors, timing – discussed informally, if at all
- Local optimization that increases enterprise-level exposure

Individually, nothing appears critical. Together, the exposure is significant.

How effective portfolio risk management works

Leaders focus on a small number of meaningful interactions, such as:

- Overlapping transformations competing for the same talent
- Reliance on common vendors, platforms, or data
- Concentration in particular geographies or markets
- Tight sequencing where a delay in one initiative triggers another

These interactions are discussed explicitly, with:

- A coordinating owner across initiatives
- Shared triggers that indicate rising exposure
- Agreed actions that cut across functions and silos

This makes enterprise-level risk trade-offs visible rather than optimized locally.

QUICK START BEHAVIOR

Identify three risk interactions leadership already worries about. Make each explicit by defining:

- Where the interaction occurs
- Who coordinates across initiatives
- What signals indicate the exposure is worsening
- What action will be taken if those signals are met

If the portfolio view doesn’t result in coordination or a decision, it isn’t doing its job.

5. Prioritize decisions over documentation

The uncomfortable truth

ERM activity is often easy to see, while its impact on decision-making can be much harder to spot. Reports get produced, registers get filled, and frameworks get followed – yet decisions continue to be made in the same way.

Documentation grows. Decisions don't change.

What this means

ERM doesn't exist to create artifacts. Its purpose is to help leaders make informed choices in the face of uncertainty.

Documentation matters – for formality, auditability, regulatory requirements and coordination – but it is never the outcome. The outcome is a better decision, made with clearer tradeoffs and ownership.

What ineffective ERM looks like

- Long, dull reports that describe risk but don't influence choices
- "Risk noted" with no shift in direction, funding, or timing
- Heat maps that add color but not insight

The work is visible. The impact is not.

What effective ERM does instead

- Embedded into existing decision forums, not separate ERM meetings
- Concentrates on moments where leaders choose, fund, pause, or pivot
- Frames issues in decision-ready terms:
  - What decision is needed?
  - What are the options?
  - What could change the outcome?
  - Who owns what happens next?

Artifacts are concise, consistent, and designed to enable action – not compliance.

QUICK START BEHAVIOR

Select one standing ERM report or reporting package and critically challenge its contents and purpose. For each section, ask: *What decision is this meant to inform, and how does it help leaders ask better questions?* Refine the content so the decision, options, key uncertainties, and implications are clear at-a-glance.

Where appropriate, condense the material into a short, decision-focused memo that clearly states: the decision required, the options available, the key uncertainty and range of outcomes, two triggers that would force a revisit, the owner responsible for monitoring them, and the next action or escalation path. Aim for clarity and brevity – if leaders can't quickly grasp the insight and ask sharper questions, the content is doing work without adding value.

6. Measure value, not activity

The uncomfortable truth

Counting work is easy. Demonstrating value is much harder – and it's what actually matters.

What this means

ERM earns credibility when leaders can point to moments where risk insight changed a decision, altered a priority, or prevented a loss, not when it simply produced more outputs.

What ineffective measurement looks like

- Success measured by volume: risks logged, workshops held, reports produced
- Dashboards packed with activity but disconnected from outcomes
- Leaders asking, *"So what did this actually change?"*

The program looks busy. Its value is unclear.

What effective measurement does instead

ERM focuses on a small number of outcome signals, such as:

- Decisions that changed because risk was made visible
- Early pivots or course corrections that avoided bigger losses
- Material surprises that were anticipated, mitigated, or softened
- Clear ownership and timely escalation when conditions began to drift

Leading indicators may still be tracked, but only to help explain why outcomes moved, not to replace them.

QUICK START BEHAVIOR

Define three outcome measures and review them quarterly alongside two short "impact stories" that show: what decision or action changed, why, and what outcome improved (or what surprise was avoided).

7. Run governance as a behavior system

The uncomfortable truth

Most organizations believe they have governance because they have committees, charters, and recurring meetings. But governance only exists when it consistently produces timely decisions, clear escalation, and reliable follow through – especially when the news is uncomfortable. If meetings occur but decisions don't, ownership is unclear, or actions quietly fade, governance exists in name only.

What this means

Governance is not structure. It is a repeatable decision behavior embedded in how the business already runs. Effective governance answers four questions every time something changes:

1. Where does this get surfaced?
2. Who decides – and who does not?
3. What triggers escalation?
4. How do we ensure follow-through happens?

Most organizations don't lack governance, they lack consistency in how decisions are surfaced, escalated, and closed.

What ineffective governance looks like

- Meetings centered on updates rather than decisions
- Escalation driven by personalities or politics
- Risks are "noted" but not owned
- Actions are captured but not revisited
- Boards receiving information, not decision-ready clarity

The organization stays busy, but uncertainty accumulates.

What effective governance forces to happen

- A small number of standing decision points built into planning, operating reviews, and investment gates
- Explicit decision rights: who decides, who recommends, who challenges, who must be informed
- A consistent decision frame:
  - What changed?
  - Why does it matter?
  - What decision is required?
  - What happens next – and who owns it?
- Automatic escalation when predefined triggers or thresholds are crossed
- Actions that are tracked, revisited, and closed – not forgotten

Governance becomes predictable and reliable, not performative.

QUICK START BEHAVIOR

Choose one existing meeting where important issues are discussed. Require that every material risk raised ends with a clear disposition: a decision, a clear escalation, or a named owner with a next step. If none of these occur, the issue does not move forward.

8. Embed ERM into operating rhythms

The uncomfortable truth

When ERM runs on its own calendar, it becomes peripheral. Risk updates arrive after priorities are set, funding is allocated, and commitments locked in. At that point, ERM can document decisions – but it can't shape them.

Risk matters most where the business is actually run.

What this means

ERM should follow the organization's decision flow, not a reporting cycle. Risk becomes actionable only when it is discussed in the same places where leaders set direction, allocate resources, and make delivery trade-offs.

If risk is discussed somewhere else, it will always be secondary.

What ineffective integration looks like

- A separate ERM schedule of quarterly updates and annual refreshes
- Risk reports summarizing exposure only after decisions are effectively made
- Escalations that feel late or disconnected from delivery realities

ERM stays informed. The business moves on.

What effective embedding does differently

ERM is built into the operating rhythm the organization already uses:

- Annual planning and budgeting
- Quarterly business and performance reviews
- Capital allocation and investment gates
- Major program, transformation, and delivery checkpoints

Risk discussions align to milestones, funding decisions, and performance measures. Triggers and escalation paths match how work actually progresses, so issues surface when leaders can still act.

QUICK START BEHAVIOR

Identify one recurring business meeting where real trade-offs are regularly surfaced (for example, speed versus scope, cost versus resilience, or delivery versus risk). Add a short, consistent risk segment that answers:

- What has changed,
- Why it matters to delivery or outcomes
- What decision or adjustment may be needed

Then align your risk update cadence to that meeting – not the other way around.

9. Build candor as a capability

The uncomfortable truth

The most damaging risks are rarely unknown. They are known but left unsaid.

When people soften bad news, avoid difficult questions, or wait for certainty that never arrives, leaders lose the chance to act while options still exist.

What this means

ERM works only when leaders can speak openly about uncertainty, trade-offs, and the possibility that things may not go as planned. Candor is not a personality trait or a cultural slogan; it is a capability that must be deliberately practiced, reinforced – and protected.

Without it, risk discussions drift into polite agreement or technical analysis, disconnected from real concerns and lived experiences.

What ineffective candor looks like

- Updates that are optimistic and heavily filtered
- Risks framed in abstract or technical language instead of concrete exposure
- Escalation delayed until problems are undeniable

The meeting feels calm. The exposure quietly grows.

What effective candor looks like

Leaders make it both safe and expected to:

- Talk openly about uncertainty and doubt
- Surface uncomfortable assumptions early
- Explore downside scenarios without blame
- Treat escalation as good discipline, not disloyalty

Over time, this changes how people show up. Risk becomes part of how leaders think together, not something to manage around.

QUICK START BEHAVIOR

In one recurring leadership meeting, change how updates are delivered. Ask presenters to answer three questions:

- What are we least certain about right now?
- What's the downside we don't want to face, but should be prepared for?
- What would make us come back and say this plan needs to change?

Then do the most important part: respond constructively when people answer honestly. Candor becomes real when leaders reward it with attention and support, not consequences.

10. Learn continuously

The uncomfortable truth

Risk does not stand still – and neither can ERM. When learning happens only after major failures, or not at all, organizations repeat the same surprises, often with higher stakes.

Annual refreshes are not learning. They are documentation.

What this means

Effective ERM improves over time by paying attention to signals, outcomes, and near misses. It adapts how risks are monitored, escalated, and discussed based on what actually happened, not what was expected to happen.

Learning is what turns experience into advantage.

What ineffective learning looks like

- Risk lists that stay largely unchanged year after year
- Surprises treated as one-offs instead of patterns
- No structured reflection on what assumptions failed or which signals were missed

The organization moves on. The system has not improved.

What effective learning does differently

Teams regularly pause after key decisions, initiatives, or events to ask:

- What surprised us?
- Which assumptions didn't hold?
- What signal would have shown up earlier?
- What should change next time?

Those lessons are translated into updated triggers, clearer ownership, and better-aligned operating rhythms. Over time, the organization recognizes familiar patterns sooner and responds faster.

QUICK START BEHAVIOR

Once each quarter, choose one recent decision, initiative, or incident and conduct a short, focused post-mortem. Capture what was learned, identify one signal that should be watched more closely next time, and update a trigger, owner, or escalation step accordingly. Then make sure that change shows up in the next relevant operating meeting.

Learning only counts when it changes what happens next.

Final word

Each operating discipline represents a practical choice about how ERM shows up in decision-making. Individually, these disciplines improve specific behaviors. Collectively, they build a decision-led ERM program embedded in how the business runs. Organizations should begin where the need is greatest and allow the program to evolve through use.

Conclusion

After a year of improved reporting and dialogue, Dana can feel the shift. Confidence doesn't come from prettier charts. It comes from management arriving with clearer choices and explicit trade-offs. When a risk shifts, Dana sees it in the triggers and tolerances – not months later in hindsight. Owners are named, escalation paths are clear, and uncertainty is discussed openly even when the response is still being shaped. From the board's perspective, this is what confidence looks like: fewer surprises, faster decisions, and a steady sense that management has a grip on what matters.

Effective ERM isn't a bigger risk register or a more polished heat map – it's a way of working that helps leaders and boards make better choices. The COSO ERM Framework offers a strong reference point for this work, providing structure and depth that organizations can use as they shape an approach that fits their business. When applied well, ERM shows up directly in decisions: clearer trade-offs, realistic ranges and scenarios, and triggers that move teams to action.

The goal is not completeness – it's confidence: fewer surprises, faster pivots, visible ownership, and a program that operates sustainably within real constraints.

The next step isn't a redesign; it's replacing low-leverage activity with a small set of decision-led practices that genuinely improve decisions.

You can tell ERM is working when the signs are observable, not theoretical:

- Strategy and investment discussions consistently ask the same disciplined questions: What must be true? What are we trading off? What would make us pivot?
- Risk appetite appears in real decisions as boundaries, not as a static statement.
- Risk assessments use ranges and scenarios tied to objectives – and meaningfully influence the decision or the timing of a decision.
- Triggers are defined early, monitored by named owners, and used to escalate early rather than explain late.
- Leaders spend less time debating scoring and more time evaluating options, controls that matter, and actions that reduce uncertainty.
- Board reporting becomes shorter, clearer, and decision-oriented – focused on what changed, what matters, and what the board is being asked to do.
- The organization learns in a visible loop: decisions are recorded, assumptions are revisited, and practices improve over time.

The point of ERM isn't to predict the future – it's to be ready for it. Make uncertainty explicit, define what would change your mind, and assign ownership before you need it. Build practices that are sustainable. When the next disruption hits, you won't need a better heat map – you'll need better operating disciplines.

Meet the Authors

Ryan C. Luttenton is a Partner and Enterprise Risk Management and Operational Risk Practice Leader in Crowe LLP's Consulting business. He has more than 25 years of experience advising organizations on enterprise risk management, internal audit, and risk governance across a broad range of industries. Ryan supports private and public companies of varying size and complexity on risk, governance, and transformation initiatives. At Crowe, he leads the firm's ERM and Operational Risk strategy, shapes the firm's ERM approach, and works with executive leadership and boards to integrate risk into strategy and decision making, improving how risk is identified, assessed, and managed while strengthening governance and enterprise-level risk insight.

Stefany Samp is a senior manager in the Enterprise Risk Management practice at Crowe LLP. She has 18+ years of experience advising organizations on enterprise risk management, internal audit, and compliance, with a focus on less regulated industries. She supports private and public companies globally across technology, media & entertainment, telecommunications, manufacturing, life sciences, and consumer markets on risk, governance, and transformation initiatives. At Crowe, she develops ERM and RCSA methodologies, leads enterprise risk assessments, and conducts ERM internal audits to strengthen governance and risk reporting and to help leaders use risk insights in strategy and decision-making.

Alexa Stone is a senior manager in the Enterprise Risk Management practice at Crowe LLP. She has extensive experience advising organizations across industries, including highly regulated environments, on enterprise risk management, operational risk, and risk governance. At Crowe, Alexa leads risk engagements spanning risk, governance, and transformation initiatives such as ERM maturity assessments, risk assessment methodology design, risk appetite and risk metrics development, and executive and board-level reporting. She is focused on delivering insights that connect risk practices to an organization's strategy and helping embed practical risk management into business planning and execution.

About COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence. COSO's supporting organizations are the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).

From Guidance to Action:
Exploring Practical Enterprise Risk Management