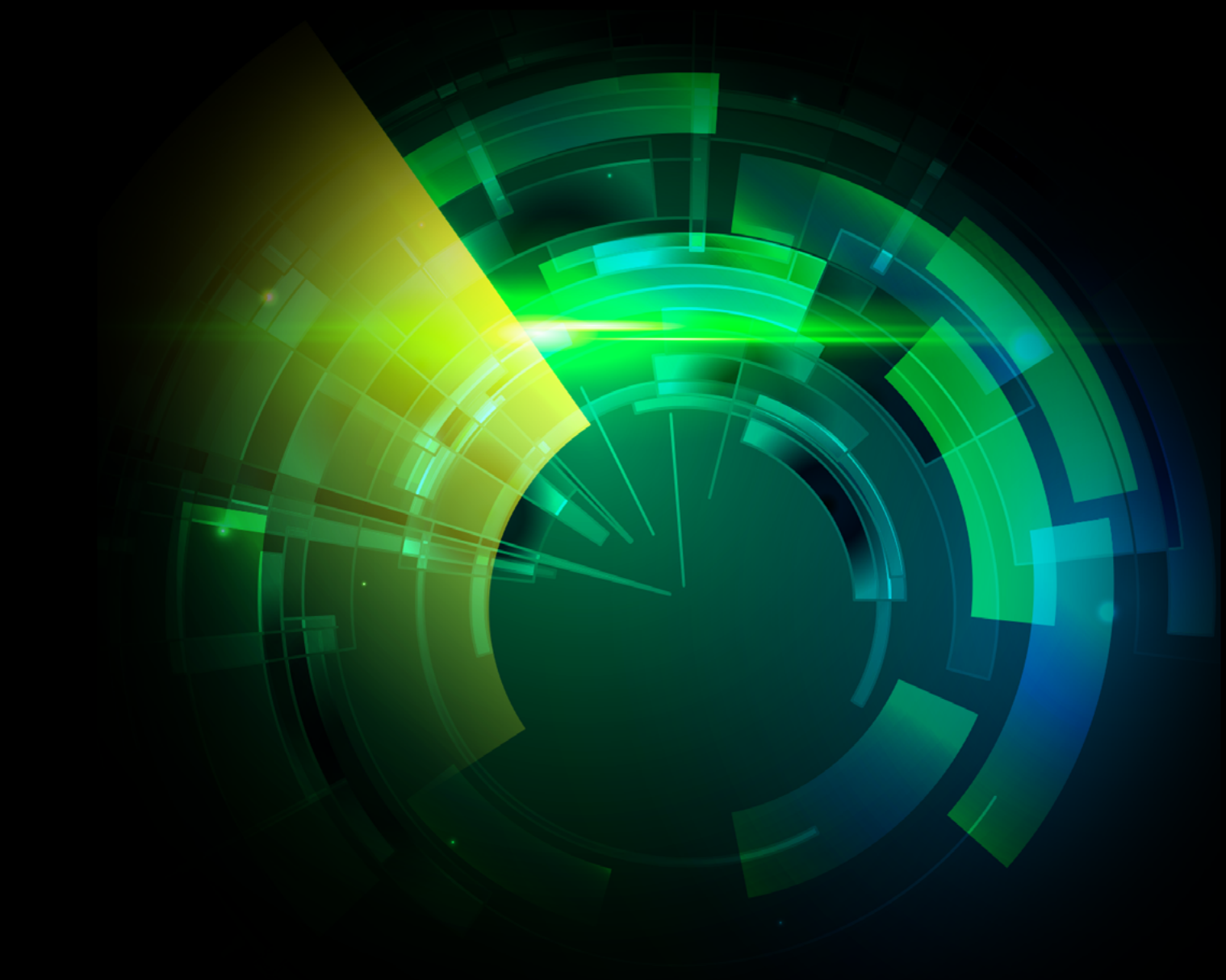
Deloitte.
Private



Enterprise risk management (ERM): The modern approach to managing risks

Introduction

When radar systems were first introduced in the early 20th century, their primary purpose was to keep ships from colliding on the high seas. From this narrow but important starting point in managing risk, the technology evolved over the ensuing decades as new innovations yielded greater range and precision, reducing risk by tracking more objects, from aircraft to speeding cars to atmospheric phenomena.

Much in the same way, organizations' approaches for identifying and addressing the risks they face have grown increasingly sophisticated since the term "enterprise risk management" (ERM) was first used in the late 1990s. While the common definition of ERM still holds—an enterprisewide strategy for identifying and preparing for the most impactful risks an organization faces—the scope of what's possible through ERM has well exceeded its original bounds, backed by technology gains, the proliferation of data, and leading practices in risk governance. Today, ERM is widely used not just for spotting possible threats to strategy, but also for identifying new opportunities and building organizational resilience for when something unexpected happens.

While ERM has long been a staple of many large public companies that needed to adopt a top-down approach to risk-taking given their regulatory obligations and shareholder expectations, in our experience many private companies and family-owned enterprises have tended to manage risks more from a subjective, bottom-up approach. This tactic may work well for spotting and putting out fires, but it may have positioned such organizations as constantly being in reactionary mode, oftentimes at a cost to their brand, reputation, and culture. We observe that many such entities still manage risk at the individual business unit level—with little integration across the enterprise or the type of coordination that is often required by the leaders of these entities to effectively govern and fulfill their oversight responsibilities.

Due to mounting pressures in the operating environment, in addition to rising expectations around issues tied to environmental, social, and corporate governance (ESG), industry convergence, and technological disruption, there's a growing expectation among directors, investors, and strategic partners for companies to modernize their risk management approaches. This dedicated series on ERM is meant to help prepare the leaders of private companies and family-owned enterprises as they seek to build or strengthen their risk management capabilities and supporting resources and infrastructure.

Shifting the mindset

Practicing effective ERM involves private companies and family-owned enterprises to elevate the risk conversation to help them make more informed strategic choices and decisions that consider the potential risks involved. For many organizations, this might be more of a subtle shift than a dramatic one, but myriad benefits can be realized by integrating risk intelligence in strategy setting, business planning, and performance management.

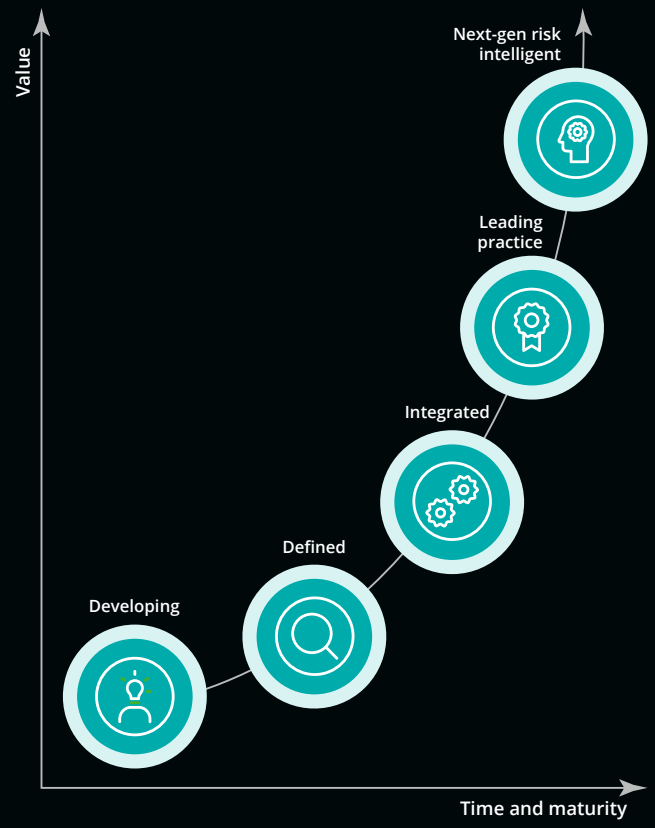
In our extensive ERM work with clients, we've discovered a few lessons that can help pave the way for organizational buy-in and, ultimately, successful ERM projects.

1 Call it what it is

It's important from the start to convey ERM initiatives as what they are: efforts to build an organization's risk intelligence.

The fact is, no matter where they reside on the risk-management maturity curve, organizations can typically be more risk intelligent by creating a structure or process that sparks and facilitates risk conversations across the business (figure 1). Employees should be able to connect with and appreciate the concept of risk intelligence, particularly in an operating environment in which the risks worth paying attention to are rapidly expanding. It can allow them to think of risk management as a more fluid and flexible endeavor.

Figure 1: ERM maturity model



Next-gen risk intelligent
Uses predictive analytics and data-driven technologies to automate processes, generate insight, and enable risk-intelligent decision-making.

Leading practice
Risk is built into decision-making. Selectively seize opportunities because of ability to exploit risks.

Integrated
Activities are implemented consistently across the enterprise and are correlated and aggregated across risk types and business units, and encompass most risk types.

Defined
Most business units function independently. Activities are either not applied consistently across business units or may be in development but are not yet finalized.

Developing
Activities are unstructured, uncoordinated, and undocumented, or they may be absent. No overarching philosophy or objectives are defined.

2 Look for incremental improvements

Some believe that ERM initiatives represent massive commitments that tend to upset cultures that are resistant to change. However, even incremental gains in risk intelligence can matter for helping to achieve these ends. It's important to think of risk intelligence as a journey, one in which you can build capabilities in phases rather than in one fell swoop.

Often, simply getting risk ownership right and creating processes for staying on top of risk-taking on an ongoing basis can move organizations up the maturity curve. Private companies and family enterprises could have a lot to gain from simply driving more organization and integration to risk management, since many rely on bottom-up approaches that meet their most pressing needs.

You don't need a small army of people to achieve this—most companies can benefit from having a chief risk officer or someone else in the organization who understands the concept and principles of ERM and has the passion and relationships with senior leaders to help inform strategy. Existing business leaders should also see a stake in this for themselves—risk management duties should be couched not as layering additional tasks onto their jobs but emphasizing this as something they should be doing already.

Begin today

Companies manage risks every day—one of the challenges is how to integrate risk intelligence across the enterprise so that it aligns with overall strategy and becomes part of the culture. No matter where your company is on the maturity spectrum in managing risks, there are some basic steps in implementing an ERM program that can help you become more risk intelligent in the moment and continue to stay that way as you adjust for changing internal and external conditions:

- **Take a risk inventory.** Companies should be able to map the risks they face based on their likelihood and potential impact. This is the focus of risk assessments, which identify key risks and create a foundation for strategic planning and decision-making. Risk assessments are tailored to each company—correctly sized to the enterprise's size, complexity, and geographic reach. It may have been years since the last time you performed an assessment, over which time things have likely changed. This will be a snapshot in time—it's important to remember that risks aren't static, and the process should be repeated anytime your strategy shifts, market conditions evolve, or your risk profile changes.
- **Prioritize risks and establish thresholds.** Opportunistic and growing companies should have some basic guardrails for risk-taking at an enterprise level, as they can prevent unilateral decisions that put the company at risk. How these thresholds are applied depends on the company's culture—some have hard curbs embedded into their organization, while others could reject rigid frameworks.
- **Embed risk discussions in your culture.** Risk assessments only capture a point in time, but the risk landscape is constantly changing. There should be a regular cadence of conversations around risk, driven by those at the top of the organization. Consider making risk part of regular strategy sessions. Establish risk owners throughout the organization to spearhead these discussions by risk area and talk about changes in the operating environment or economy that might change the organization's risk appetite. Conduct table-top risk management exercises involving crisis scenarios and other potential setbacks. Also, consider setting up an advisory committee that includes members from outside the company or board to get perspectives from those with related experience in dealing with the same types of risks. This may help avoid a common misstep that often plagues a lot of companies: They do all the work to understand their risks and establish thresholds but never go back and adjust them.
- **Activate a risk monitoring program.** Organizations competing today should be thinking about leveraging strategic intelligence provided by risk-sensing tools such as AI, data analytics, and risk dashboards. Leading companies are already tapping these tools to pull in data and let them know when they're exceeding their established risk thresholds. If some activity falls outside the accepted risk parameter, then a flag goes up, giving leaders a chance to discuss whether the potential returns are worth the extra risk.

Conclusion

As your enterprise seeks to become more risk intelligent and build organizational resilience for when disruptions occur or the risks you face evolve, it's likely going to need new capabilities and skills that extend beyond its current capacities. Making the right investments in talent, technology, and other resources will be critical for maintaining internal support for constant improvement. New solutions can quickly turn into new problems without the experience to implement them and determine if they work within your existing culture.

In this series, we will help connect the dots between needs and answers, with a particular focus on identifying the organizational capabilities and other considerations that will be important to keep in mind as your business seeks to become more risk intelligent. In the next article, we'll explore internal controls and how they should function within an ERM program. Other installments in the series will dive into ERM implications for managing the growing threat of cyber risk, sources of operational risk, and what it takes to help build organizational resilience when even the most pernicious risks are realized.

As your organization starts or progresses on its ERM journey, consider how your organization would respond to the following questions about its risk-management approach and capabilities:

- Do we have an integrated way to assess risks across our enterprise?
- Do we have thresholds for risk-taking, and are they well defined, understood, and embraced across the organization?
- What are the problems we as an organization are trying to solve by seeking a greater understanding of the risks and opportunities we face?
- Do we have the internal capabilities and resources to effectively monitor our highest-priority risks on an ongoing basis? What are we doing collectively to improve our risk awareness?
- How does risk management fit into roles and responsibilities among business leaders throughout our organization?
- Do we have a process for refreshing the conversation around risk on a regular basis?

NEXT UP IN OUR SERIES

Enhancing internal controls to improve risk management
Explore ways to enhance internal controls at private companies and family enterprises to allow for more strategic decision-making, increased operational efficiency, the identification of opportunities for automation, mitigation of fraud risk, and more.

GET IN TOUCH

Kevan Flanigan
US Deloitte Private Leader,
Risk & Financial Advisory
US Deloitte Private Leader, Private Equity
keflanigan@deloitte.com

Adam Regelbrugge
Risk & Financial Advisory Real Estate Leader
aregelbrugge@deloitte.com

Deloitte.