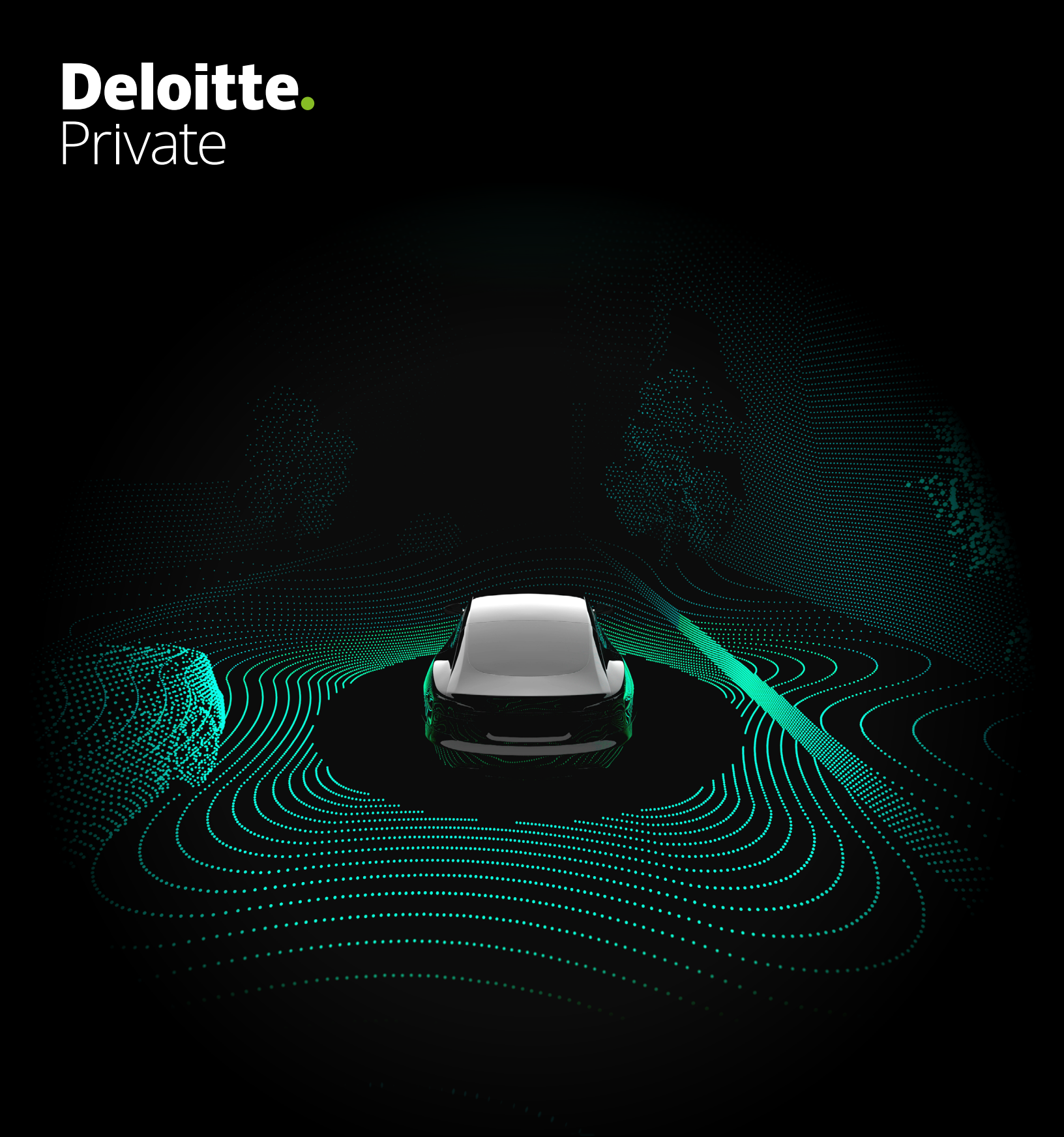
Deloitte.
Private



Smart monitoring for operational risks

Introduction

Businesses can face operational risks at every turn—whether these dangers are immediately apparent or not. They may come from within as with ever-present risks like employee misconduct, data mishandling, or lapses in internal controls. They may also originate beyond the company walls, stemming from third-party actions and the inherent cultural and ethical concerns that can come with doing business in a global context. Layered on top of these hazards is the prospect of reacting too slowly to disruptive technologies. From whatever direction they're coming, many of these risks can begin as incremental missteps that may expand into systemwide failures.

The list of specific vulnerabilities is long and can touch every part of an organization. A wide range of industries face workforce shortages. An enterprise risk management program that was suited in the past may not be able to keep up with the pace of today's technology and digital challenges (Figure 1). These issues and others are front and center for many as company leaders seek to stay resilient amid ongoing geopolitical and economic uncertainty.

To confront these evolving threats, businesses can rely on "always-on" monitoring, similar to autonomous cars that feature this type of protection. They're manufactured with one or more radar sensors to detect risks like nearby vehicles and objects, stay in their lane, or perform emergency stops. The thinking is that individual components of a system need continuous monitoring to avoid adverse consequences.

Figure 1: Technology and digital risk hot topics 2024, according to the Deloitte Center for Board Effectiveness

Rank	Across all sectors	Financial Services	Non-Financial Services
1	Cyber security	Cyber security	Cyber security
2	Digital transformation and IT change	Cloud environments	Data management and data quality
3	Data management and data quality	Digital transformation and IT change	Artificial intelligence
4	Artificial intelligence	Technology resilience	Digital transformation and IT change
5	Cloud environments	Outsourcing and critical third parties	Legacy IT and IT simplification
6	Technology resilience	Data management and data quality	Cloud environments
7	Outsourcing and critical third parties	Artificial intelligence	Technology resilience
8	Legacy IT and simplification	Identity and access management	Outsourcing and critical third parties
9	Identity and access management	Legacy IT and IT simplification	Identity and access management
10	Emerging technology trends: digital assets and blockchain, UK controls regime, responsible marketing and digital channels	Emerging technology trends: digital assets and blockchain, responsible marketing and digital channels	Emerging technology trends: UK controls regime, responsible marketing and digital channels

Keeping pace and maintaining control over intellectual property (IP)

One way enterprise risks have evolved in recent months is through the increasing adoption of emerging technologies like generative artificial intelligence (Gen AI). But there's a flip side to core facets of the technology like AI-generated code and natural language models. A recent survey reveals that 56% of IT and information security leaders surveyed are actively exploring solutions to boost their organizations' security posture to confront risks associated with AI. In the survey, 34% of organizations report they're already using or in the process of implementing AI security tools to head off these emerging risks.

As companies map out plans to monitor AI risks, one key concern may be keeping their intellectual property safe and secure. Some companies that use Gen AI have faced criticism for using copyrighted material without permission to train AI prompts. In addition, some enterprises have banned the use of Gen AI because employees have used proprietary data within Gen AI prompts that was ultimately leaked beyond the organization.

Incremental uncertainties can accumulate over time, potentially leading to bigger problems. If a knowledge company fails to address and protect its IP effectively, it could risk losing control over its proprietary assets and may encounter legal, financial, and competitive consequences as a result.

Some questions they might ask include:

- Is our intelligence truly protected?
- Is it considered IP?
- How do we react if we lose control over proprietary assets?

Tapping into leaders and partners

Even as risk-monitoring capabilities evolve, they shouldn't always be left to navigate on autopilot—even with the help of some of the internal controls we highlighted in a previous chapter of this series. Business leaders should help keep their organizations on track, but that could mean drawing on a new level of expertise to navigate operational challenges.

Within the C-suite, one development in managing operational risk is the emergence of positions like the chief trust officer. This C-suite role is gaining prominence as the executive responsible for tracking customers' needs, pushing for trustworthy decisions, and building companywide trust initiatives. According to a Deloitte survey, 62% of people who report highly trusting a brand buy almost exclusively from that brand compared with competitors in the same category.

Risk awareness and intelligence are key drivers for how boards and management govern the organization. For instance, directors can provide a valuable layer of inquiry and different viewpoints. Some boards designate committees with risk oversight responsibilities, such as a compliance or risk committee tasked with questioning management based on the organization's risk posture.

Also, some organizations may opt to engage with external stakeholders, such as trade organizations and nonprofits that specialize in technical assistance to enhance business operations. These inputs may be valuable to help enhance and influence risk management practices and create a risk-intelligent culture.

Depending on the company's risk culture, appetite, or posture, there's typically a board member responsible for monitoring management decisions that influence the company's risk profile. This individual confirms that the decisions made by management are in line with the company's overall risk strategy and asks pertinent questions to help maintain a balanced and appropriate risk posture.

Of course, every company has its risk tolerance. Some companies may embrace a more aggressive approach to risk-taking which might be aligned to growth targets. Others may adopt a more cautious stance. Whatever the company's risk posture may be, it's important to understand when management decisions expose the organization to additional risk. This responsibility often falls to the board—to scrutinize decisions and ensure they align with the company's values, objectives, and acceptable risk levels.

Creating a culture of readiness

Maintaining a culture that understands underlying business risks is an important starting point. But it's the next step—having safeguards in place and learning how to apply them—that can create a greater sense of security. Leaders should be vigilant and consistent with messaging and practices around processes like data sharing and system access. For companies that manufacture physical products, there should be ongoing evaluation around ways to properly secure these goods. Leaders should set the tone from the top to reinforce appropriate behaviors. Financial audits can catch discrepancies and raise red flags. However, companies may need robust, ongoing operational processes and controls to protect the enterprise.

Here are some ways to begin to help ensure operational risks don't slip past the radar:

Decide on a risk posture. Start with a risk assessment that includes structure, regulatory landscape, and exposure to threats—to secure complex environments, prepare for potential incidents, and minimize downtime from disruptive scenarios. Regarding cyber risk, for instance, a board may want to know if there's an emphasis around security risk outside of IT.

Pay attention to the user experience. Instead of large, unwieldy manuals on processes and procedures, think of ways to use the user experience to an advantage. Put policies in an easy-to-digest format—and encourage ongoing consistent communication and reinforcement of the information. Even for the most critical details, what's critical is getting buy-in—so think of ways to ensure people can retain the info and have an incentive to participate. This can be particularly true in organizations with high turnover and a rapid onboarding period.

Don't forget the details. Though many private entities can be as large and sophisticated as the biggest public companies, they often receive less external scrutiny. Even so, it is likely just as important to have rigorous operational controls. After all, it may be a lack of operational discipline in areas like capital needs, technology, or leadership transitions that can push even the most innovative and groundbreaking businesses into the ditch.

NEXT UP IN OUR SERIES

Business resilience for private companies
Crises and disruptions are so deeply linked with the very nature of how businesses are conducted that it's increasingly important to view risks as more intrinsic and ubiquitous than exceptional. The next article in this series will focus on the importance of agility and ever-greater resilience to help reduce the impact of these events and speed up response.

Visit deloitte.com to catch up on other articles in this series.

GET IN TOUCH

Kevan Flanigan
US Deloitte Private Leader,
Risk & Financial Advisory
US Deloitte Private Leader, Private Equity
Deloitte Transactions and Business Analytics LLP
keflanigan@deloitte.com

James Cascone
Partner and Sustainability,
Climate & Equity (SC&E) Leader
Deloitte & Touche LLP
cjcascone@deloitte.com

Deloitte.