2026 EDITION

UNLOCKING OPPORTUNITY

EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

protiviti®
Global Business Consulting

NC STATE Poole College of Management
Enterprise Risk Management Initiative

Table of contents

Introduction

Successful companies view even challenging times as catalysts for innovation and growth, actively seeking opportunities where others see obstacles.

Over the last 13 years, we have issued annual research reports on the top risks faced by leaders all over the world. This year, we have added an emphasis on opportunities to set the tone for identifying and responding proactively to emerging trends, market shifts and evolving customer expectations. Organisations balancing risk management with a strong focus on seeking growth are better equipped to innovate products and services, enhance their resilience, adapt to change, and achieve top-line growth and strategic differentiation. It is all about unlocking opportunity. Accordingly, our discussions of risks are framed contextually with a high-level focus on opportunity with the intention to enhance the discussion of risk by linking it to value-creating initiatives.

This report — our **14th annual edition** — contains insights from 1,540 board members and C-suite executives around the world regarding their perspectives on:

- Three specific areas for growth considering the current environment;
- Opportunities and challenges associated with the transformative impact of artificial intelligence (AI) on their organisations;
- The top risks on the horizon for the near-term (two to three years ahead) related to 28 specific risks across three dimensions (macroeconomic, strategic and operational) and for the long-term (a decade from now) related to 12 risk themes that consider the strategic and operational near-term risks; and
- A discussion of their organisations' near-term strategic investment priorities, given the opportunities and the risks they face.

Our survey participants shared their views through an online survey conducted from early September through mid-October 2025. As in the past, the report provides analyses across organisations of different sizes, industries, geographic regions, as well as the executive positions held by the respondents (board members, CEOs, CFOs, etc.).

The key findings in this report provide useful insights for board members and senior executives to benchmark their organisation's opportunities and risks against those on the minds of other executive leaders around the world. Our hope is that this report will foster meaningful dialogue and discussion among an organisation's leaders as they seek to create strategic value in these challenging times.

Executive summary

Notwithstanding several years of uncertainty and shifting geopolitical and economic dynamics, our results indicate that business leaders are ready to act and are embracing innovation, strategic partnerships and long-term planning to drive transformation and realise growth opportunities. The biggest risk organisations face today is doing nothing.

In brief: what you need to know

There is strong optimism for revenue growth over the next two to three years. Nearly seven in 10 board members and executives (69%) agree somewhat to completely that, considering current conditions, there are significant opportunities to increase revenues over the next two to three years.

Ecosystem expansion is a strategic priority. More than six in 10 leaders (62%) indicate their organisations plan to expand their strategic alliances and partnerships over the next two to three years.

AI is both a transformative growth driver and a complex challenge. AI is a long-term strategic priority, with 31% of leaders focused on integrating it into current technologies and business processes. AI ranks sixth among near-term global risks, while concerns about IT infrastructure performance have risen to the fourth-rated risk this year versus 13th last year. Thus, while AI is seen as a transformative growth enabler, IT infrastructure and talent readiness present major barriers to its effective deployment and realising its full benefits. Cybersecurity risks linked to AI also remain top of mind.

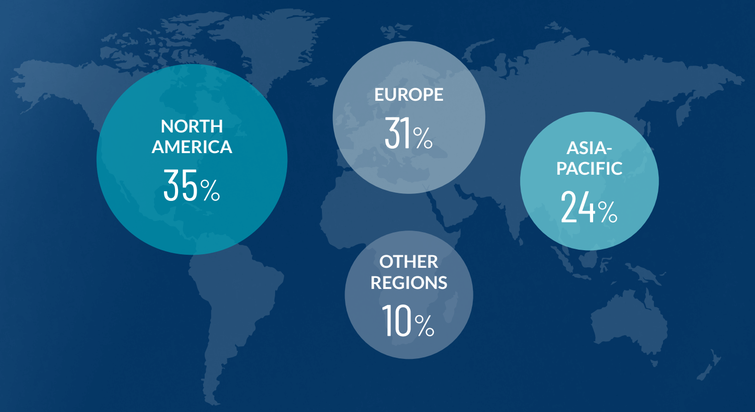
Cybersecurity is the top global risk and investment priority. Not only are cyber threats ranked as the top global near-term risk, but third-party risks (which are linked to cyber concerns) rank second. Cybersecurity also stands out as the top investment priority for organisations to address near-term risk issues. Interestingly, there are geographical distinctions in rating these risks.

Talent challenges are evolving but not disappearing. Talent risks continue to be at the forefront among board members and C-suite leaders globally, with issues surrounding workforce upskilling and the availability of skilled labour remaining significant, particularly given the expected impact of AI on job roles and workforce transformation.

Concerns about the economy and trade-related challenges and their impact on global markets are top 10 near-term risk concerns. Trade-related challenges entered the top 10 list as the 10th-rated risk for this year, while uncertainties linked to interest rates and inflation continue to create reason for pause among respondents.

Customer experience, cyber and AI are top long-term strategic focus areas. Organisations are prioritising customer and competition dynamics, security and privacy, and AI deployments in their long-term strategies, indicating a shift toward integrated decision-making that encompasses both immediate and future opportunities and risks.

Snapshot of key findings



Number of respondents = 1,540

Top global near-term risks

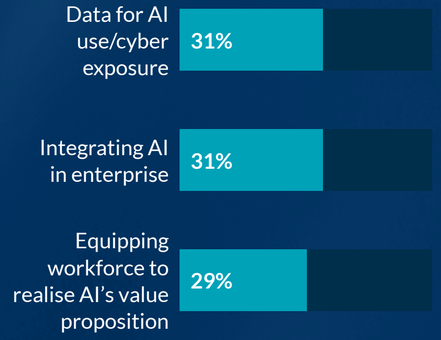
2026 rank	Risk issue	Average*	2025 rank
1	Cyber threats	3.39	2
2	Third-party risks	3.16	7
3	Adopting new/emerging technologies elevates need to upskill/reskill workforce	3.06	9
4	Operations/legacy IT unable to meet expectations	3.05	13
5	Economic conditions	3.05	1

** Average based on a five-point scale where 1 reflects "No impact at all" and 5 reflects "Extensive impact."*

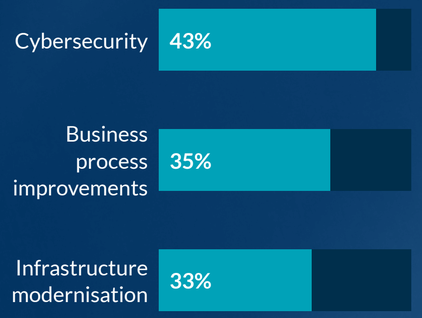
There is optimism for potential growth opportunities

Based on a five-point scale assessing agreement/disagreement.
Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

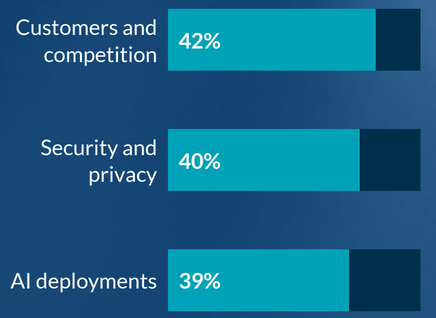
Top 3 priorities — impact of AI



Top 3 investment areas



Top 3 long-term challenges



Differences across respondent groups

In the following pages, we offer analysis and insights based on subsets of the full survey sample, including breakdowns by executive position, industry group, geographic region and organisation size. These subsets are defined below.

Executive position

Position	Number of respondents	Percentage of sample
Board Member (Board)	94	6%
Chief Executive Officer (CEO)	62	4%
Chief Financial Officer (CFO)	314	20%
Chief Operating Officer (COO)	236	15%
Chief Information/Technology Officer (CIO/CTO)	211	14%
Chief Information Security Officer (CISO)	115	7%
Chief Human Resources Officer (CHRO)	24	2%
Chief Risk Officer (CRO)	159	10%
Chief Audit Executive (CAE)	168	11%
Chief Strategy/Innovation Officer (CSO)	18	1%
Chief Data/Digital Officer (CDO)	10	1%
Chief Legal Officer/General Counsel (CLO)	12	1%
Other C-Suite (OCS)	44	3%
All other	73	5%

Industry group

Industry	Number of respondents	Percentage of sample
Financial Services (FS)	325	21%
Consumer Products and Services (CPS)	241	16%
Manufacturing and Distribution (MD)	216	14%
Technology, Media and Telecommunications (TMT)	167	11%
Aerospace and Defense (AD)	125	8%
Healthcare (HC)	142	9%
Energy and Utilities (EU)	117	8%
Government (GOVT)	127	8%
Not-for-Profit/Higher Education (NFP/HE)	59	4%
Other industries (not separately reported)	21	1%

Geographic region

Region	Number of respondents	Percentage of sample
North America	536	35%
Latin America	87	6%
Europe	479	31%
Middle East and Africa	68	4%
India	87	6%
Asia	207	13%
Australia and New Zealand	76	5%

Organisation size

Organisation size	Number of respondents	Percentage of sample
Largest organisations: Revenues of $10 billion or greater; assets or budget under management $50 billion or more	363	24%
Medium-to-large organisations: Revenues $1 billion to $9.99 billion; assets under management $10 billion to $49.99 billion; budget under management $5 billion to $49.99 billion	586	38%
Small-to-medium organisations: Revenues $100 million to $999.99 million; assets under management $1 billion to $9.99 billion; or budget under management $500 million to $4.99 billion	406	26%
Smallest organisations: Revenues less than $100 million; assets under management less than $1 billion; budget under management less than $500 million	185	12%

03

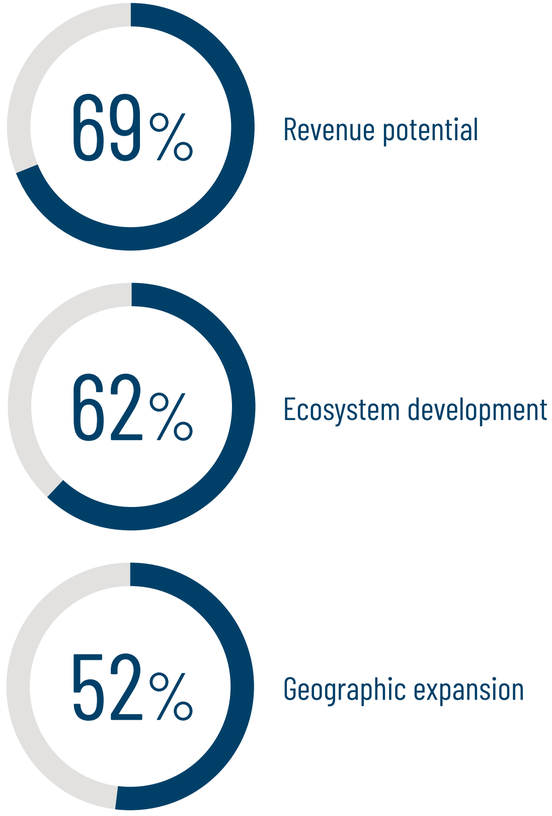
Opportunities for enterprise growth

We asked respondents to rate the level of their agreement with the following three statements about strategic growth opportunities over the next two to three years using a five-point Likert scale ranging from 1=Disagree completely to 5=Agree completely.

- **Revenue potential:** Current macroeconomic conditions notwithstanding, there are significant opportunities to grow our revenues.
- **Ecosystem development:** There are significant opportunities to expand our ecosystem of strategic alliances and partnerships to enhance how we go to market.
- **Geographic expansion:** There are significant opportunities to grow our business in markets other than our headquarters' domestic market.

Figure 1 summarises the overall level of agreement with each of these statements from the full sample of 1,540 respondents:

Figure 1: Views about opportunities for growth



Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

There is **strong confidence in revenue growth potential,** with 69% of respondents expressing agreement ("Agree completely" or "Agree somewhat") with this statement, the highest among the three statements. Respondents express a strong belief that **revenue growth opportunities exist despite the headwinds their organisations face,** whether it be the economy, geopolitical developments or other matters. This suggests that many organisations are maintaining a forward-looking posture, unlocking opportunities to innovate, expand offerings or capture market share even in uncertain environments. These findings highlight the importance of exploring growth avenues while ensuring that risk-adjusted returns are considered when making capital allocation decisions.

Ecosystem development is seen as a means of unlocking opportunity, with it receiving the second-highest response, 62%. Ecosystems are powerful enablers to helping organisations outperform traditional, isolated business models by fostering interconnected networks that drive innovation and value. Collaboration among ecosystem participants facilitates the sharing of ideas, technologies, capabilities and access that support rapid co-innovation, expanded market reach, and operational efficiency and agility, allowing participants to achieve revenue growth

and other outcomes that would be difficult or impossible for any single organisation to accomplish alone. Our survey findings reflect optimism about **expanding strategic alliances and partnerships**, indicating that many organisations view the development of these relationships as a key enabler of success. Leaders should assess whether they are fully leveraging external relationships for co-innovation, data sharing and platform integration, among other opportunities.

Geographic expansion is viewed with more caution given there was a lower level of agreement — 52% — among respondents. This finding suggests **more tempered enthusiasm for international or cross-border growth.** This may reflect concerns about trade policies, geopolitical instability, regulatory complexity or uneven recovery across global markets. Directors and executives should probe whether strategies for growth in foreign markets are being pursued with consideration of the opportunities and risks, especially in light of shifting trade policies and regional dynamics, and are supported by robust digital platforms.

Overall implications

These findings suggest that while executives are generally optimistic about growth, they are prioritising **strategic partnerships and core market expansion** over aggressive geographic moves as they look over the near-term horizon to enhance operational readiness, strategic clarity and competitive advantage. Furthermore, a digital world minimises the importance of a physical footprint due to the efficiencies, capabilities and flexibility offered by virtual tools, cloud infrastructure and digital platforms. That said, half of the survey respondents overall expressed a priority to grow business in foreign markets.

The following tables summarise respondent views about opportunities for growth across different executive positions and across organisations of different sizes, industries and geographies.[1]

Table 1: Views about opportunities for growth — by executive position*

	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
Revenue potential	81%	68%	71%	68%	73%	71%	46%	62%	66%
Ecosystem development	65%	55%	65%	61%	67%	68%	67%	60%	59%
Geographic expansion	63%	61%	50%	49%	55%	56%	46%	51%	51%

Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group.

[1] In Tables 1-4, we have highlighted in darker blue those statements for which 66% or more of respondents are in agreement that they represent strategic growth opportunities for their organisations; statements for which 50%-65% of respondents are in agreement are highlighted in medium blue, while those for which less than half of respondents are in agreement are highlighted in turquoise.

Board members have the highest level of optimism regarding revenue potential. This may be due to the board's role to challenge management to pursue ambitious goals and think expansively. Boards receive summarised, high-level reports that emphasise strategic wins and growth initiatives. Accordingly, board members may not have the same level of transparency into the operational realities that executives manage day-to-day. In addition, directors serving on multiple boards may be positioned to bring a broader perspective to strategic conversations in the boardroom.

The focus on opportunities to expand the ecosystem of strategic alliances and partnerships to enhance go-to-market strategies is relatively consistent in the boardroom and across the C-suite. The higher interest of directors and CEOs than anyone else in the C-suite in pursuing significant opportunities to grow in foreign markets suggests a sharper focus on their respective roles as stewards of the company's vision, growth and long-term value.

In viewing the results across organisation size, the two largest groups of organisations show the most optimism, though all see positive signs and opportunities, particularly in terms of revenue potential and ecosystem development.

Table 2: Views about opportunities for growth – by organisation size

	Largest organisations	Medium-to-large organisations	Small-to-medium organisations	Smallest organisations
Revenue potential	74%	72%	62%	65%
Ecosystem development	66%	63%	60%	60%
Geographic expansion	60%	54%	44%	48%

Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

Regarding the different views on growth opportunities across geographies (see Table 3), organisations in Australia and New Zealand are less bullish than other regions, likely because this year's respondents from the region have a markedly different mix, including government and mining. That said, the top 10 near-term risks overall are largely the same and the long-term risks overall are identical, with and without inclusion of the respondents from this region.

The focus on revenue potential is typically higher in North America, Latin America and India than in Europe and Asia due to a combination of factors — market growth opportunities, economic conditions, favourable consumer demographics, evolving regulatory environments and competitive opportunities. These factors generally contrast with the greater maturity and saturation in many parts of Europe and some developed parts of Asia, particularly Japan. To illustrate:

- India is projected to be the fastest-growing major economy, outpacing China, the U.S. and the EU.
- Latin America has a predominantly young and skilled labour force with a rapidly expanding middle class, driving increased consumption. In contrast, many European and some Asian nations face challenges with ageing populations.
- In North American companies, the higher level of revenue growth optimism than, say, Europe and Asia likely stems, at least in part, from a more risk-embracing corporate culture, a more dynamic market-based financial system

that encourages investment, and investor expectations that prioritise growth and innovation. The U.S. market is a magnet for global investment, including substantial capital from European and other foreign investors, which drives high valuations and provides ample funding for growth.

- While markets in Europe are often considered mature and highly competitive, regions like Latin America and India offer a wide range of untapped opportunities in sectors such as digital services, infrastructure and financial services.

The heightened interest in ecosystem development in North America and Latin America is driven by dynamic market growth, innovation-friendly environments, generally supportive policies and the need for collaborative solutions to address complex challenges. While some of these factors exist in other regions, their combination creates an ideal landscape for ecosystem models to flourish, enabling organisations to unlock new opportunities, drive innovation and achieve sustainable growth.

Table 3: Views about opportunities for growth – by geographic region

	North America	Latin America	Europe	Middle East & Africa	India	Asia	Australia & New Zealand
Revenue potential	75%	79%	65%	71%	83%	67%	34%
Ecosystem development	67%	75%	60%	63%	58%	63%	34%
Geographic expansion	58%	52%	51%	56%	56%	49%	16%

Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

As for growing business in foreign markets, we continue to point out that in a digital world, the need for physical expansion is reduced. The emphasis on pursuing opportunities in foreign markets is generally consistent across geographies, with a slight uptick in North America, where the focus on foreign markets has always been strong. Developed markets in North America and Europe have been the traditional centres of innovation and revenue. However, these markets are now often described as more mature, with higher saturation and complexity, pushing companies to look to new epicentres of growth in emerging regions for significant expansion. As emerging markets liberalise investment laws and actively create favourable environments to stimulate international trade and investments, they become more attractive for foreign companies.

The heightened interest in ecosystem development in North America and Latin America is driven by dynamic market growth, innovation-friendly environments, generally supportive policies and the need for collaborative solutions to address complex challenges.

The emphasis on revenue growth remains largely uniform across industry groups, with the exception of Energy and Utilities and Government. While a reduced focus in the Government sector may be anticipated, the pattern observed within Energy and Utilities is notable, considering the growth prospects associated with increased energy demand driven by data centres. Differences in attention to ecosystem development across industry groups can be attributed to various factors, particularly the view that sustainable growth, ongoing innovation and competitive advantage are increasingly reliant on collaboration and interdependence. Sectors that adopt an ecosystem-oriented approach are generally more equipped to respond to disruption, enhance customer value and secure long-term success. This context may explain the comparatively lower focus observed within Government and Energy and Utilities, as these organisations face less exposure on these fronts.

The focus on growing foreign business is relatively consistent across industry groups, with two exceptions. Understandably, these exceptions are Government and Energy and Utilities.

Table 4: Views about opportunities for growth – by industry group

	AD	CPS	EU	FS	GOVT	HC	MD	NFPHE	TMT
Revenue potential	79%	71%	61%	72%	50%	76%	68%	41%	76%
Ecosystem development	72%	63%	58%	66%	53%	60%	62%	62%	63%
Geographic expansion	59%	56%	40%	55%	31%	58%	55%	34%	57%

Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

Differences in attention to ecosystem development across industry groups can be attributed to various factors, particularly the view that sustainable growth, ongoing innovation and competitive advantage are increasingly reliant on collaboration and interdependence.

04

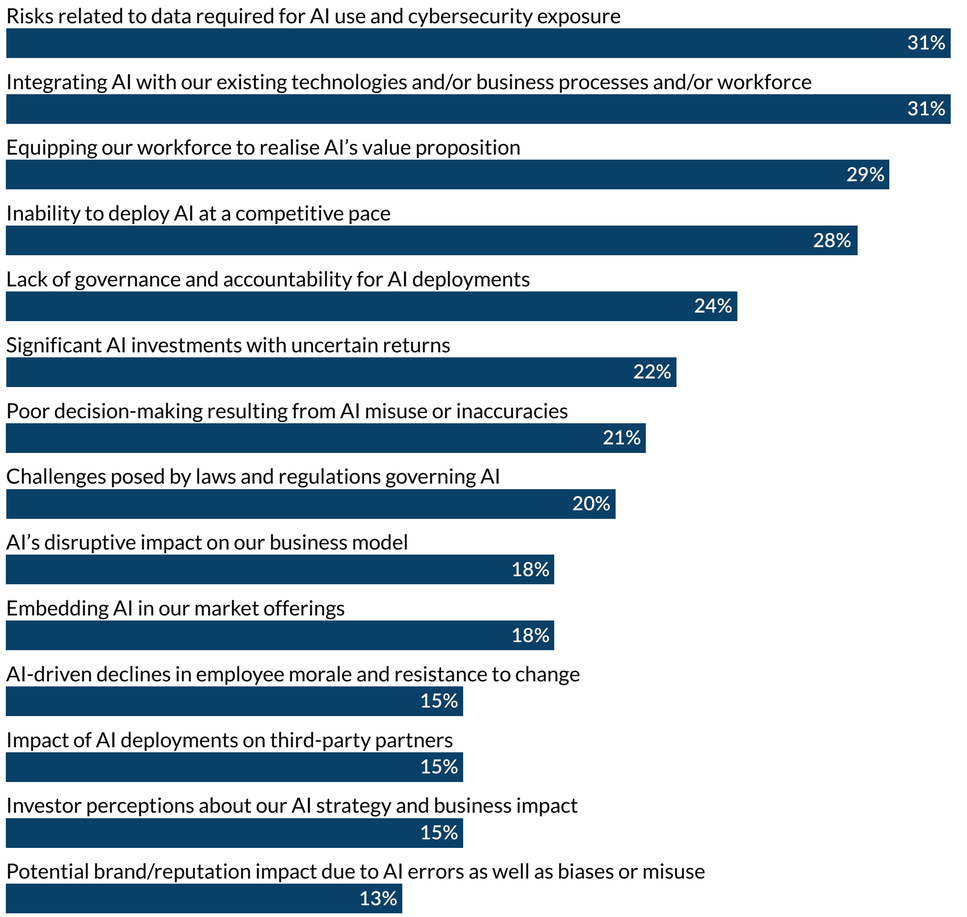
Transformative impact of AI

AI is a critical component to unlocking efficiency, personalisation, new innovations and the ability to scale — all drivers of new revenue streams and expansion. As organisations increasingly integrate AI into their core strategies, they are discovering new ways to optimise operations, enhance customer engagement and stay ahead of competitors in a rapidly evolving marketplace. But AI also introduces governance challenges.

The impact of AI is interwoven throughout a number of the top risks on the minds of executives for both near-term and long-term risk horizons. Given the importance of AI capabilities to enabling growth strategies and their rapid deployment, we asked respondents to provide their perspectives about the impact of AI on their organisations over the next two to three years. Specifically, we asked them to select their three most important priorities from a list of 14 potential AI risk issues.

Figure 2 summarises the percentage of times each AI risk was included as one of the respondents' top three AI risk concerns. As shown, "Risks related to data required for AI use and cybersecurity exposure" and "Integrating AI with our existing technologies and/or business processes and/or workforce" were included most often among the top three AI risk issues for respondents (31%).

Figure 2: Which of the following issues reflect your organisation's most significant priorities regarding the impact of AI on your business over the next 2-3 years?



Percentages reflect frequency with which each area was selected among the top three.

These results reveal a unified, yet complex, perception of AI deployment risk over the next two to three years. The primary focus is not on existential threats but on **foundational organisational and operational risk.** The collective consensus points to an overwhelming prioritisation of three core challenges:

- Security and data integrity
- Seamless operational integration
- Talent and skills readiness

These concerns underscore a critical tension in the current enterprise AI adoption cycle: The risk of failing to integrate AI effectively and responsibly into existing processes, technologies and workflows is seen as equally pressing as the risk of fundamental security failure. Executives are concerned that poor integration, combined with an ill-equipped workforce, will neutralise any value proposition and competitive advantage that can be gained from AI investments, all while exposing the organisation to heightened data and cyber threats.

While risks associated with making "significant AI investments with uncertain returns" and "poor decision-making resulting from AI misuse or inaccuracies" are also high-ranking, our analysis of key findings across executive positions, industry groups and regions reveals that the current risk agenda is dominated by product/service delivery and enterprise defence, signalling a transition from experimental AI investment to operational necessity. A tailored, integrated strategy addressing technology, talent and cyber governance simultaneously will be the defining characteristic of high-performing organisations in the AI era.

Overall implications

The full sample results provide a definitive baseline, grouping the most pressing AI risks into three strategic focus areas that occupy the executive agenda: operationalisation of AI, playing defence, and the pace of adoption and utilisation. With a near-unanimous focus, C-suite leaders acknowledge that the primary hurdle for AI is not technological capability but organisational change.

- **AI integration** being tied for the top spot highlights a shift away from pilot projects toward embedding AI into the fabric of the enterprise. This risk is intrinsically a complex challenge, involving the fusion of new algorithmic logic with legacy systems and deeply entrenched human workflows. Failure to address the integration challenge means AI investments become "shelf-ware," creating fragmented, difficult-to-scale solutions that defeat the purpose of deploying AI.

- **Talent readiness** closely follows, recognising that AI's return on investment (ROI) is contingent on human capability. This risk is a stark acknowledgment that simply purchasing AI tools is insufficient; organisations must invest in upskilling, new roles and a cultural shift where AI is a collaborative co-worker, not merely a tool. The bottom line: Properly implemented, AI becomes an extension of the workforce.

Playing defence represents security, ethical and compliance non-negotiables that must underpin any AI initiative.

- **Security and data** (31%) is the most-cited risk, signalling executives' understanding that AI models are fundamentally new attack surfaces. This risk extends beyond traditional cybersecurity to encompass model poisoning, data leakage during training and inference,

and the ethical use of massive, sensitive datasets. No AI deployment can succeed without addressing the data lifecycle from acquisition to decommissioning.

- **Governance and accountability** (24%) indicates that a quarter of all respondents foresee the risk of a direct failure of organisational control. This risk speaks to the difficulty of establishing clear ownership for AI outputs, ensuring traceability and transparency, and providing appropriate human oversight, especially as systems' decision-making and actions become more autonomous.

- The **evolving regulatory landscape** (20%) reveals that the challenges posed, as new laws and regulations governing AI emerge, are of significant concern to executives as they continue down the path to AI implementation and reliance on outputs from AI deployment.

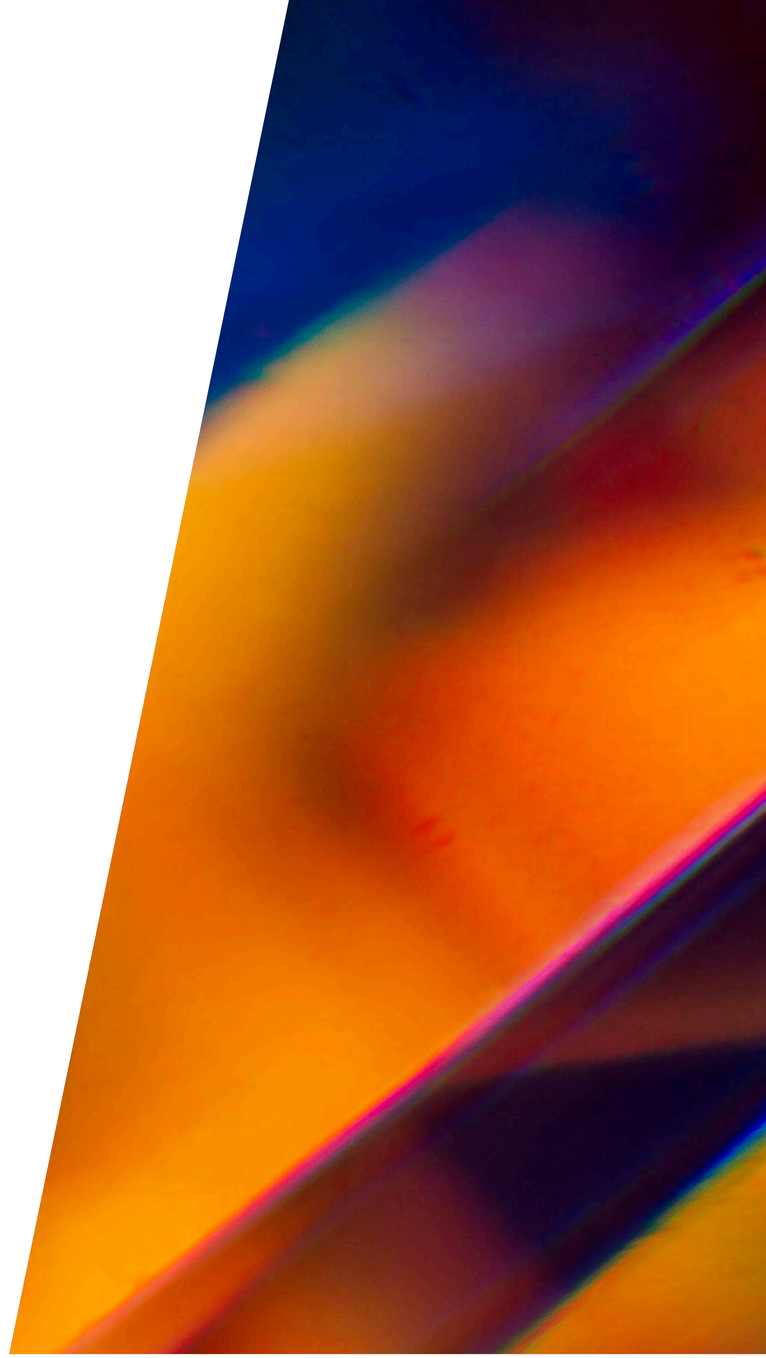
The risks related to competitive speed and financial efficacy reflect market pressures.

- **Competitive pace** (28%) shows a strong fear of falling behind competitors, treating AI deployment as a strategic race. This gives rise to FOMO (fear of missing out) because proprietary AI deployments are not easily replicated capabilities when they involve unique, protected technologies and processes owned by an organisation, giving them exclusive rights and competitive advantage.

- **Uncertain returns** (22%) serve as the counterpoint: A significant portion of leaders fear that this rapid race will result in expensive failures, leading to stranded assets and a loss of confidence from the board and investors. This concern suggests a need to proceed with clear objectives, quality data sources, the right technology, pilots and testing, and continuous evaluation and monitoring to keep implementations on track.

The overall full sample picture is one of practical, immediate concern: Executives are focused on **execution risks** first and **existential risks** second, as governance and controls struggle to keep pace with the dual demands of implementation speed and seamless integration.

> No AI deployment can succeed without addressing the data lifecycle from acquisition to decommissioning.



Perspectives on impact of AI across selected respondent groups

Table 5: Top three AI risk issues — by executive position*

Risk	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
Risks related to data required for AI use and cybersecurity exposure	35%	29%	25%	27%	23%	32%	17%	40%	42%
Equipping our workforce to realise AI's value proposition	45%	42%	21%	25%	22%	21%	42%	33%	36%
Integrating AI with our existing technologies and/or business processes and/or workforce	33%	52%	22%	18%	20%	15%	33%	53%	48%
Inability to deploy AI at a competitive pace	25%	27%	29%	23%	30%	19%	33%	40%	31%
Significant AI investments with uncertain returns	18%	19%	28%	24%	23%	23%	4%	18%	16%
Lack of governance and accountability for AI deployments	17%	29%	20%	20%	19%	23%	17%	30%	42%
Challenges posed by laws and regulations governing AI	12%	19%	21%	23%	26%	25%	38%	14%	12%
AI-driven declines in employee morale and resistance to change	15%	6%	17%	20%	23%	24%	38%	7%	5%
Embedding AI in our market offerings	18%	21%	21%	25%	17%	21%	0%	7%	12%
Impact of AI deployments on third-party partners	12%	5%	25%	18%	18%	24%	12%	7%	9%
Investor perceptions about our AI strategy and business impact	16%	5%	18%	22%	24%	20%	29%	4%	3%

Percentages reflect frequency with which each area was selected among the top three. Top three areas for each executive role are highlighted in blue (ties included).

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group.

A deeper dive into the data reveals that executive perception of AI risk is heavily modulated by functional accountability, resulting in distinct risk profiles across the C-suite.

CEOs, board members and COOs — the roles most responsible for overall strategic outcomes and operational delivery — demonstrate a strong consensus around the **operationalisation imperative**.

- **CEOs** prioritise **integration**, followed by **workforce** and then **governance**. This profile reflects the three pillars of executive focus: ensuring the system works to make the business operate better, smarter and faster; ensuring people can use it; and ensuring it is managed, controlled and secured.

- **COOs** mirror this concern with **cyber/data risk** being their top concern, followed by the emerging risk of **embedding AI in market offerings**, and then **workforce**. This indicates that operational leaders are on the front lines focusing on data security as AI is implemented and how the deployment will translate into new products.

Both CFOs and CIOs/CTOs are focused on the financial physics of AI: speed versus investment risk.

- **CFOs** prioritise **competitive pace** and **uncertain returns** as their top two concerns. The CFO's primary mandate is capital stewardship, and the data reflects their concern about the uncertain duration of AI investments. The third risk, **impact of AI on third-party partners**, underscores concern over extended enterprise risk and supply chain financial liability. **Cyber/data**, the exposure to security threats, closely follows third-party risk concerns.

- **CIOs/CTOs** exhibit a hybrid profile, prioritising **competitive pace** but immediately followed by **legal and regulatory challenges related to governing AI.** Technology leaders recognise that the pressure to deploy quickly heightens the exposure to risk. Their focus on **regulations** as a concern indicates the need to future-proof technology deployments against evolving compliance frameworks.

The CRO and CAE roles focus on systemic control matters.

- Interestingly, **CROs** and **CAEs** rank **integration** as their top concern, recognising that a poorly integrated system falls short of realising the expected value. CROs' subsequent concerns are **competitive pace** and **cyber/data**, highlighting a triple threat: a rush to implement, poor organisational integration and the resulting exposure to security threats. CAEs are also concerned with **cyber/data** and, to no surprise, governance.

Executive perception of AI risk is heavily modulated by functional accountability, resulting in distinct risk profiles across the C-suite.

Table 6: Top three AI risk issues — by industry group

Risk	AD	CPS	EU	FS	GOVT	HC	MD	NFPHE	TMT
Risks related to data required for AI use and cybersecurity exposure	21%	39%	32%	24%	27%	41%	31%	41%	38%
Integrating AI with our existing technologies and/or business processes and/or workforce	15%	42%	42%	24%	16%	38%	34%	44%	42%
Equipping our workforce to realise AI's value proposition	23%	38%	37%	22%	19%	33%	33%	34%	44%
Inability to deploy AI at a competitive pace	29%	29%	29%	30%	28%	24%	30%	42%	29%
Significant AI investments with uncertain returns	29%	18%	19%	27%	17%	20%	23%	19%	18%
Impact of AI deployments on third-party partners	27%	11%	8%	24%	19%	11%	12%	10%	5%
Challenges posed by laws and regulations governing AI	20%	12%	20%	23%	29%	18%	18%	15%	14%
AI-driven declines in employee morale and resistance to change	20%	9%	8%	18%	28%	13%	15%	7%	10%

Percentages reflect frequency with which each area was selected among the top three. Top three areas for each industry group are highlighted in blue (ties included).

AI risk perception is sharply defined by the regulatory, trust and business model characteristics of each industry group. In industries where data sensitivity and public trust are paramount, **data and security** often dominate the risk agenda. In industries focused on high-volume transactions, product development and supply chain efficiencies, the **organisational agility** theme often emerges.

- Four industry groups — **Consumer Products and Services, Energy and Utilities, Healthcare,** and **Technology, Media and Telecommunications** — rank the same risks in their top three AI-related concerns: **integration, cyber/data** and **workforce**, with **integration** the top issue for three of the four groups.

- **Cyber/data** is a top three concern overall for the above four industry groups as well as **Financial Services** and **Manufacturing and Distribution**. This is a clear reflection of the catastrophic potential of a data breach or a cyber attack involving critical national infrastructure, sensitive operations or highly protected personally identifiable information. For these sectors, while AI is viewed as a *value creator*, it is also viewed as an *enabler of risk*.

- In addition to **cyber/data, Manufacturing and Distribution** ranks **workforce** and **competitive pace** as significant concerns. For the creators and primary users of AI in these companies, the focus is on fast, controlled and secure deployment through skilling employees expected to leverage AI-powered agents and tools.

- In addition to **cyber/data, Financial Services** reports **competitive pace, uncertain returns, integration** and **impact of AI on third-party partners.** This suggests that financial institutions have accepted the risks related to data required for AI use and cybersecurity exposure as a baseline cost of doing business and are now primarily focused on how quickly and effectively they can realise value by replacing human-driven processes with AI-optimised ones.

- Both **Aerospace and Defense** and **Government** rank **competitive pace** among their top three concerns. Aerospace and Defense also lists **uncertain returns** and **impact of AI on third-party partners** in their concerns, with Government listing **regulations** and AI's **impact on organisational culture**. These industries are heavily reliant on large, decentralised operational workforces (e.g., retail, factory floors, logistics) and recognise that the success of AI hinges on empowering, not alienating, their human capital through targeted upskilling and seamless system integration.

The **Not-for-Profit/Higher Education** sector leads with **integration,** followed by **competitive pace** and **cyber/data** as their top AI risk concerns. For mission-driven organisations that face ongoing challenges for talent and resources, AI integration with existing systems and deployment at a competitive pace are understandable concerns.

> In industries where data sensitivity and public trust are paramount, data and security often dominate the risk agenda. In industries focused on high-volume transactions, product development and supply chain efficiencies, the organisational agility theme often emerges.

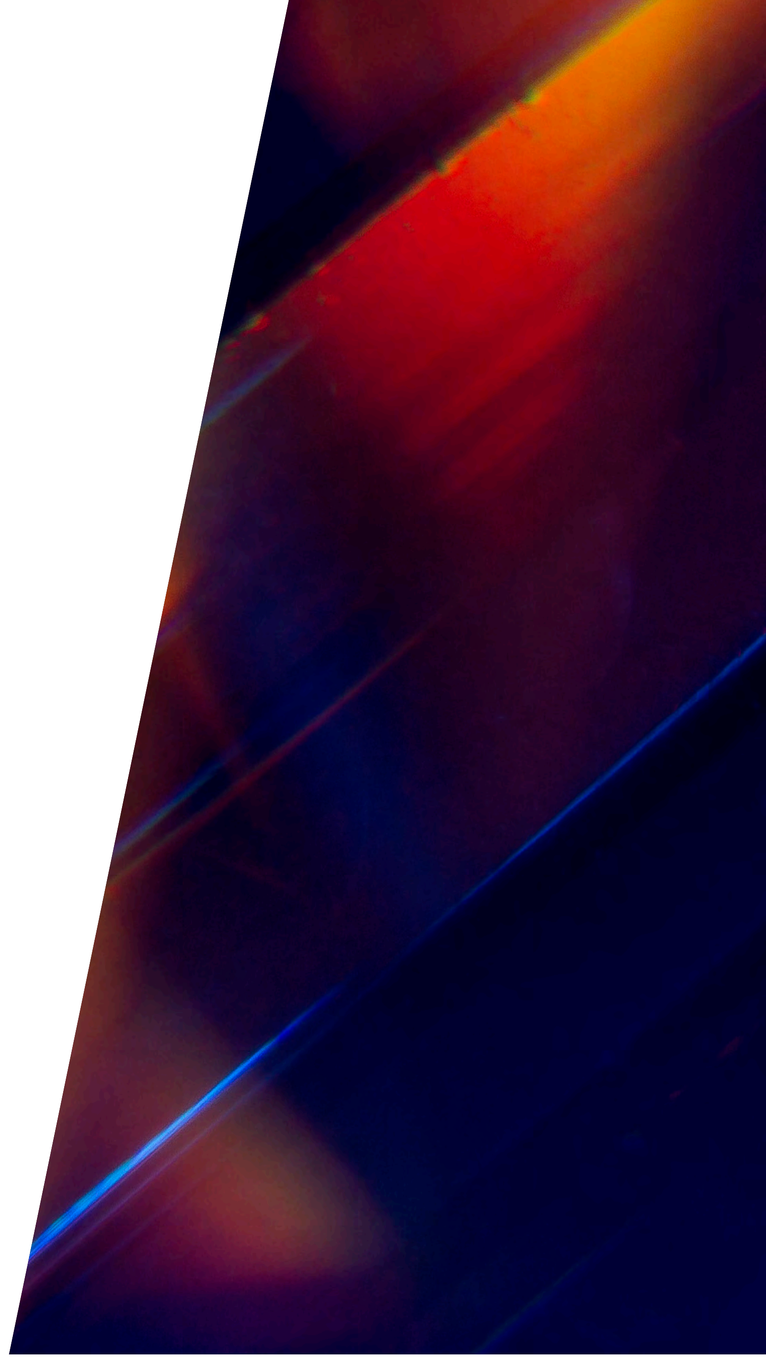


Table 7: Top three AI risk issues — by geographic region

Risk	North America	Latin America	Europe	Middle East & Africa	India	Asia	Australia & New Zealand
Risks related to data required for AI use and cybersecurity exposure	34%	29%	26%	26%	44%	34%	22%
Integrating AI with our existing technologies and/or business processes and/or workforce	38%	30%	26%	34%	28%	29%	15%
Inability to deploy AI at a competitive pace	28%	38%	28%	31%	21%	30%	29%
Equipping our workforce to realise AI's value proposition	32%	32%	23%	25%	20%	43%	26%
Significant AI investments with uncertain returns	19%	17%	26%	25%	23%	17%	30%
Poor decision-making resulting from AI misuse or inaccuracies	22%	8%	23%	15%	29%	13%	29%
Embedding AI in our market offerings	16%	25%	15%	26%	15%	21%	25%
Lack of governance and accountability for AI deployments	24%	25%	22%	25%	19%	30%	22%

Percentages reflect frequency with which each area was selected among the top three. Top three areas for each region are highlighted in blue (ties included).

AI risk is also perceived through a regional, geographic lens, reflecting local economic development, regulatory environments, and political and labour market characteristics.

In **North America** and the **Middle East and Africa (MEA)**, the top priority is **integration**.

- **North America** reflects a sophisticated, rapidly adopting market where the focus has moved beyond *whether* to use AI to *how* to assimilate it into complex corporate structures and make its deployment effective and responsible via talent and security measures.

- **MEA** shows a focus on rapid **integration** combined with a high fear of being outpaced, suggesting these countries view AI as a critical enabler of immediate competitive growth and are willing to take on deployment risk to achieve it.

Europe and **Australia and New Zealand (ANZ)** show a distinct focus on the financial and strategic value of AI.

- **Europe** and **ANZ** both place **competitive pace** and **uncertain returns** high on their list. This is likely driven by a combination of high regulatory oversight (especially

in Europe) and a cultural focus on strategic, controlled investment, where the financial justification of technology is scrutinised rigorously. The recognition of the risk of **poor decision-making** in ANZ suggests a greater concern with the reliability and output quality of deployed AI systems.

India and **Asia** present a profile defined by large populations, rapid digital transformation and a high sensitivity to systemic failures.

- **India** is the only region to prioritise **cyber/data** and **poor decision-making** as its top two concerns. This unique pairing suggests a deep concern over the integrity and reliability of AI systems handling massive volumes of new digital data, where errors can have immediate, cascading effects across large-scale services.

Asia prioritises **workforce**, recognising that the scale of AI adoption demands an enormous and rapidly trained talent base. The combination of this region's top three issues underpins a struggle to train people rapidly and secure data while keeping up with the competitive pace of the region.

Additional subgroup analyses

For brevity, we have omitted tabulation of AI risk concerns for our two remaining subgroups: organisation size and type.

The size and organisational maturity of the enterprise significantly shape the risk outlook, distinguishing between organisations focused on managing immense complexity and those focused on securing competitive viability.

The largest organisations are defined by complexity and scale. Their top AI risk concern is **cyber/data**. The sheer volume and sensitivity of data managed by these global giants make the risk related to AI use and cybersecurity exposure an exponentially increasing one, meaning the widespread impact of AI systems and their potential for errors and omissions can accumulate over time without a human in the loop. Their second and third concerns, **workforce** and **integration**, reflect the challenge of driving massive, systemic change across global divisions and legacy IT systems.

By contrast, **the smallest organisations** are driven by existential urgency. Their top concern is **competitive pace**. For smaller players, the failure to adopt AI quickly is seen as an immediate threat to market survival. Their focus then shifts to the practicalities of deployment — **cyber/data** and **integration** — as they lack the resource buffers of larger firms to absorb implementation failures. For the smallest firms, risk is rooted in their **limited AI agility** and **resource scarcity**.

The sheer volume and sensitivity of data managed by these global giants make the risk related to AI use and cybersecurity exposure an exponentially increasing one.

We also examined variation in AI risk exposure based on organisation type.

- **Public organisations** prioritise **workforce**, then **cyber/data** and **integration**. This is a balanced, operational profile reflecting the need to maximise ROI from publicly scrutinised investments by seamlessly integrating AI deployments with core business processes and upskilling employees to make the new business model work.

- **Private organisations (planning an IPO)** exhibit a unique, high-growth risk profile: **competitive pace, uncertain returns** and **embedding AI in market offerings**. This group is laser-focused on rapid validation of their business model for public markets. Their risks are predominantly **market-facing and financial**, prioritising speed and demonstrable value over internal systemic concerns. Their focus on the market is particularly telling, indicating that AI is not just a tool but also a core, sellable feature of their valuation story.

- **Private organisations with no current plans for an IPO** identify the difficulty of integrating AI with existing technologies and business processes as the most problematic AI risk issue. They also have concerns with cyber-related risks associated with AI data needs and with their ability to deploy AI at a competitive pace.

- **Organisations owned in whole or part by a private equity firm** express the greatest concerns about the inability to deploy AI at a competitive pace, and risks related to data required for AI use and cybersecurity exposure. These challenges are understandable given the private equity market's focus on competitive positioning and growth, as well as on protecting the enterprise, including but not limited to its intellectual property.

- **Governmental and not-for-profit** organisations share a risk foundation of **integration and cyber/data**. These organisations, which often serve critical societal functions, are highly attuned to the risk of poor service delivery and the compromise of sensitive citizen/beneficiary data. Their risk profile is fundamentally about **mission continuity and public trust**.

> The size and organisational maturity of the enterprise significantly shape the risk outlook, distinguishing between organisations focused on managing immense complexity and those focused on securing competitive viability.

Summary

Our results show that AI risks are interconnected and require a broad, coordinated approach. The co-dominance of **cyber/data, integration** and **workforce** issues converge to a single potential failure point. Focusing only on data security without proper workforce training leaves systems unusable, while investing in integration without effective governance may facilitate speed and interconnectedness but can also breed uncontrolled risks.

Insights:

- **From a siloed to an integrated focus:** Given the theme emphasising AI integration in our survey findings, organisations may find value in **shifting investments from sequential, siloed projects (cyber, HR, IT) to a more holistic approach**. For example, a cross-functional AI program office, reporting to a senior executive, could be empowered to evaluate opportunity and risk in the context of the three aforementioned core risks.
- **From deployment to realisation:** The strong showing of **competitive pace** and **uncertain returns**, particularly among the CFO and private organisations, suggests a need to consider recalibrating the deployment narrative. The question is: Should the strategic calculus shift from **speed of deployment** to **speed of realisation**?
- **From broad mandates to targeted outcomes:** Organisations can gain advantages by ensuring that each AI initiative is directly linked to clear, measurable business results associated with a proven financial benchmark, instead of following a wide-reaching technological mandate. The control functions (CRO and CAE) should participate in the initial idea phase, consistent with a **governance-for-value approach** in which control systems facilitate responsible and effective deployment, not simply restricting progress.
- **From prioritising technology and systems to embracing the human component:** Concerns about core **workforce** issues and a related risk, **AI-driven morale declines and resistance to change** (a CHRO concern), highlight human capital's role in successful AI deployment. Employees should be trained not only to use AI, but also to assess its performance, spot errors, decide when to intervene and adapt their roles accordingly. AI should be supervised like human staff, with clear expectations, training to meet expectations, measuring and monitoring against expectations, and corrective actions taken to improve performance when necessary. Companies that prepare employees to work alongside and oversee AI agents are more likely to maximise the technology's potential.

The variance in industry-specific risk priorities necessitates the development of customised security frameworks. Our findings indicate that executive leadership recognises that AI risk is an operational reality and competitive advantage will be achieved not by organisations deploying the greatest number of AI models, but by those offering solutions that are **safest, most integrated** and **highly trusted**. A unified strategy led by senior management is needed to achieve this focus.

05

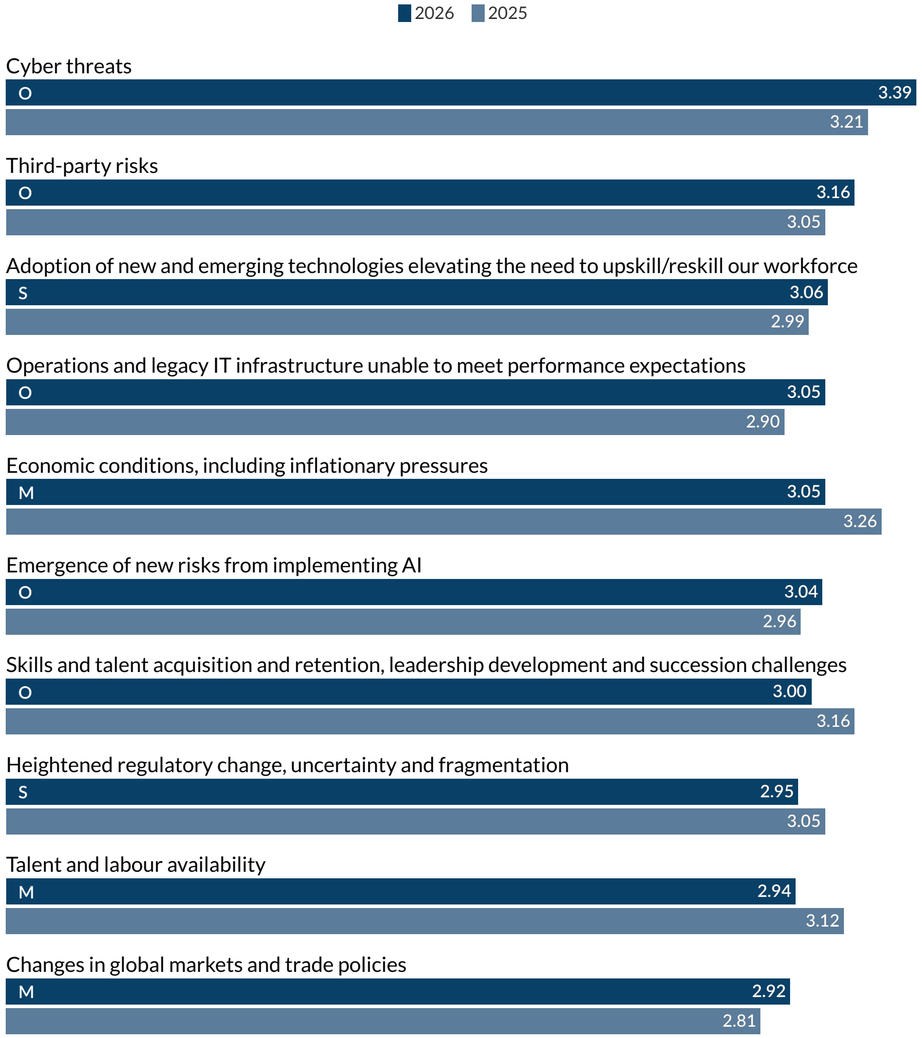
Navigating the near-term risk landscape

Relative to the prior year, the overall impression among the 1,540 respondents is that the magnitude and severity of the overall risk environment their organisations will face in executing their strategy and achieving their performance goals over the next two to three years is higher compared to last year. Using a 5-point Likert scale where 1=extremely low and 5=extremely high, the average risk score is 3.30 relative to 3.13 one year ago. This signals an overarching impression among respondents that the overall risk environment seems more challenging than views expressed in our prior year survey.

The top 10 near-term risk results from our study offer insights as to why the risk environment is slightly elevated. Figure 3 summarises the rank-ordered list of top 10 risks over the next two to three years for the full sample of 1,540 C-suite executive and board member respondents, compared to the prior year. These risks, while dominated by operational risks, span macroeconomic, operational and strategic categories and are ranked based on their average Likert scores. The findings reveal a strong emphasis on operational vulnerabilities, talent challenges and the disruptive potential of emerging technologies.

Overall, 11 of the 28 risks rated by respondents are operational in nature, while nine are macroeconomic and eight are strategic.

Figure 3: Top 10 risks for the near-term



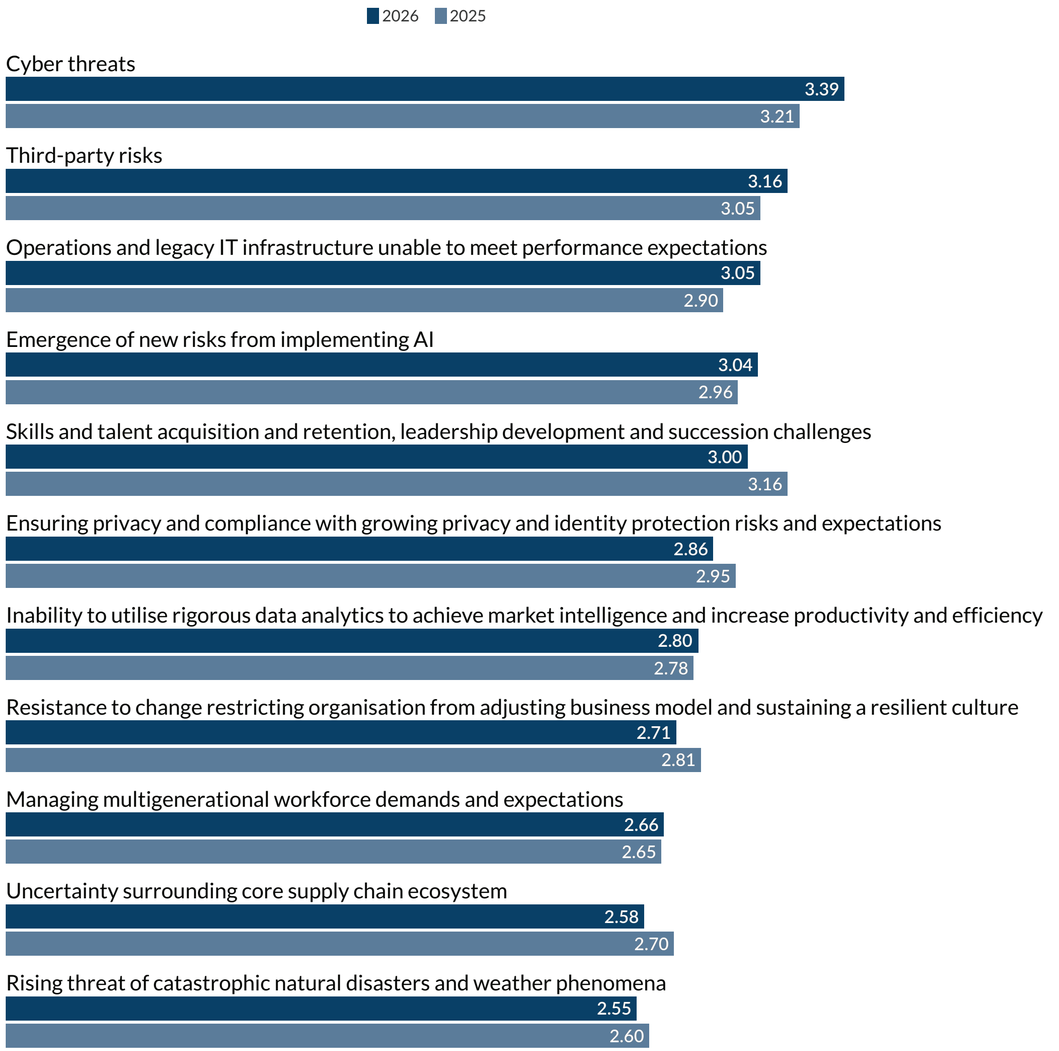
Dominance of operational risk concerns

Five of the top 10 near-term risks are operational in nature, signalling executive focus on **internal resilience and executional reliability**. These risks — cyber threats, third-party dependencies, legacy IT infrastructure, emerging IT and AI implementation challenges, and skills acquisition/retention — are deeply interconnected and reflect the pressure organisations face to deliver consistent performance in a world that is being disrupted digitally. Operational risks are no longer "back-office" concerns — they are front-and-centre in strategic planning and execution. Operational risk management must now be integrated with enterprise strategy and aligned with technology-driven transformation goals.

Cyber threats are the top concern globally, reflecting a growing recognition that digital vulnerabilities are not just technical issues; they are existential threats. Executives are increasingly aware that cyber resilience must be embedded into enterprise strategy. Concern about cybersecurity was the number one risk concern for respondents across all sizes of organisations. Addressing evolving cybersecurity threats must be treated as a strategic imperative, with organisations needing to integrate cyber risk metrics into C-suite and boardroom performance dashboards.

Reliance on **third-party** external vendors and ecosystem partners introduces systemic vulnerabilities. Third-party risk spans cybersecurity, compliance, reputation and operational continuity. Executives are concerned about the lack of visibility into vendor practices, especially in multitiered supply chains and cloud-based services. Holistic third-party risk management frameworks, including continuous monitoring and scenario-based stress testing, are becoming more critical than ever. When considered together, **cyber threats** and **third-party risks** highlight the fragility of IT infrastructures and the need for robust governance across extended enterprises with a multiplicity of attack vectors.

Figure 4: Operational risks — near-term outlook



Legacy infrastructure and **AI implementation** risks underscore the tension between innovation and operational readiness. Operations and outdated legacy IT infrastructure systems and insufficient digital capabilities hinder innovation and competitiveness. Legacy infrastructure affects data integration, process efficiencies, customer experiences, time-to-market and the ability to pivot in the face of change. Prioritising digital modernisation along with clear ROI metrics will help ensure IT investments align with strategic goals and elevate digital capabilities across the enterprise. Of note, this issue is the highest elevated risk of this year's study, moving from the 13th-rated risk last year to the fourth-rated risk this year.

AI adoption is accelerating, but concerns about ethical dilemmas, regulatory uncertainty and operational disruption are growing. The rapid evolution of AI capabilities combined with the lack of governance frameworks makes the management of risk associated with AI difficult to identify, track and manage. Organisations may benefit from establishing cross-functional AI oversight committees to monitor and manage risks associated with AI deployments.

Talent challenges remain a critical concern, although the level of risk has abated slightly relative to views expressed in our last survey. **Attracting and retaining skills needed** and **developing leadership talent** are key concerns among executives surveyed, as they create challenges to building and sustaining the strong executive bench so critical to succession planning and long-term success. The decline from last year may reflect a number of factors — short-term hiring improvements and the effects of AI deployments, for example — but long-term concerns persist nonetheless. Talent-related risks reflect the **strategic importance of human capital** in sustaining competitive advantage and highlight the importance of integrating talent strategy with business strategy. Metrics on employee engagement and retention and the evolving leadership pipeline health will help senior management monitor emerging talent challenges.

Top macroeconomic concerns

Three of the top 10 near-term risks reflect macroeconomic concerns — economic conditions, labour availability and global trade policy shifts — that can disrupt strategic momentum. While these risks are somewhat outside the organisation's control, their impact on cost structures, supply chains and market access is profound.

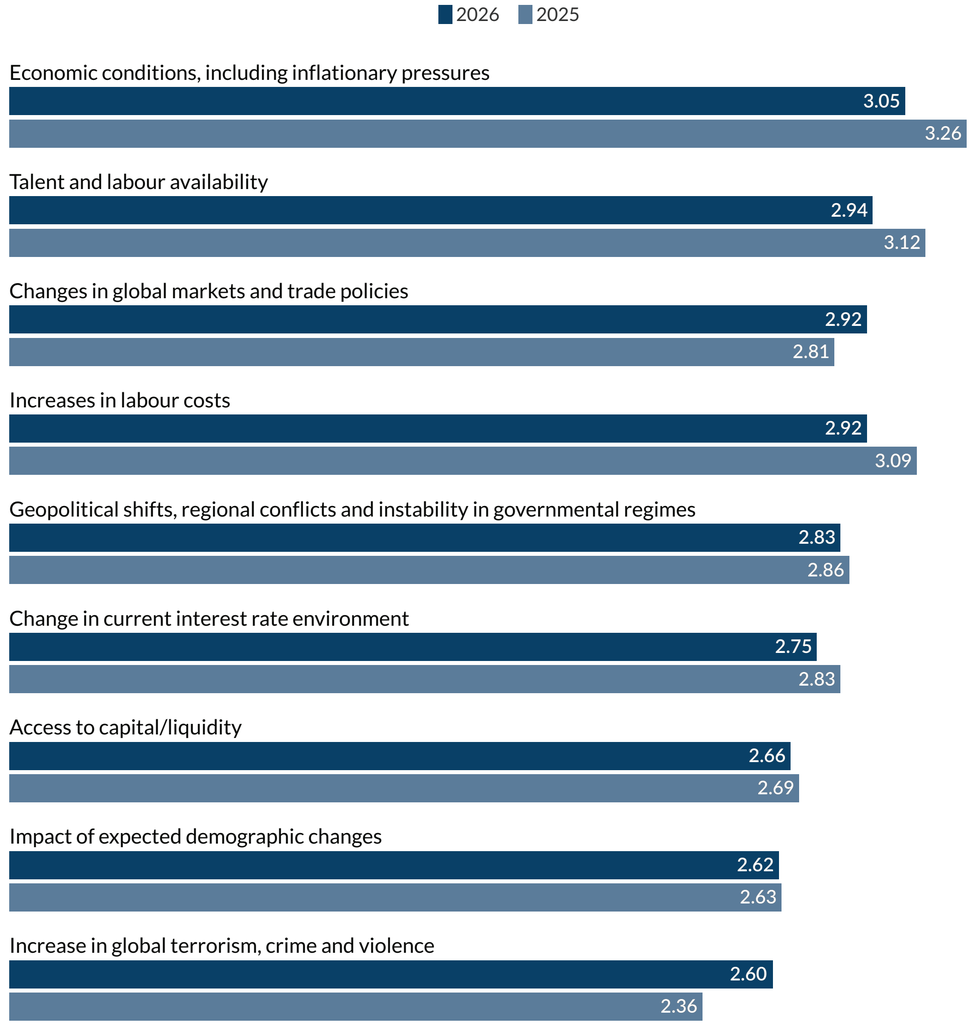
While economic uncertainty has declined somewhat relative to last year's survey, where this was the top-ranked risk, it continues to threaten margins, strategic investments and hiring decisions. Executives are navigating interest rate uncertainty, shifting consumer demand and geopolitical tensions. The slight decline in concern over inflation may suggest short-term stabilisation, but executives remain cautious about long-term volatility. **Labour availability** and **global trade policies** are other factors impacting concerns over the economy.

The **availability of talent in the marketplace** is tied to demographic shifts, evolving immigration policy, workforce ageing and shifts in needed skills in light of new AI and other digital capabilities — issues that require long-term strategic workforce planning. The decline in this risk may reflect some short-term improvements, but long-term uncertainty persists as the impact of AI on workforce requirements is causing companies to rethink hiring plans with reductions in some skills due to AI benefits coupled with a growing need for talent and new skills to leverage AI capabilities.

Geopolitical tensions and shifting trade alliances are heightening concerns about **global markets and trade policies**. Executives are focused on managing the effects of fluctuating tariff policies, border restrictions and regionalisation of trade. Organisations that diversify their supply chains to nearshore and reshore as well as monitor geopolitical developments can improve their ability to pivot in response to frequent and unexpected geopolitical shifts. In today's global markets, organisations are searching for ways to ensure their global strategies are achievable and resilient.

Risk-adjusting strategy is all about being able to withstand external shocks. As organisations navigate the above challenges, it becomes increasingly important to leverage advanced analytics, scenario planning and stress testing to anticipate potential market opportunities and emerging risks. Prioritising transparency in forecasting, enhancing financial planning and cost optimisation, and fostering open communications across the organisation help leaders pivot their strategies and maintain flexibility in capital deployment.

Figure 5: Macroeconomic risks — near-term outlook



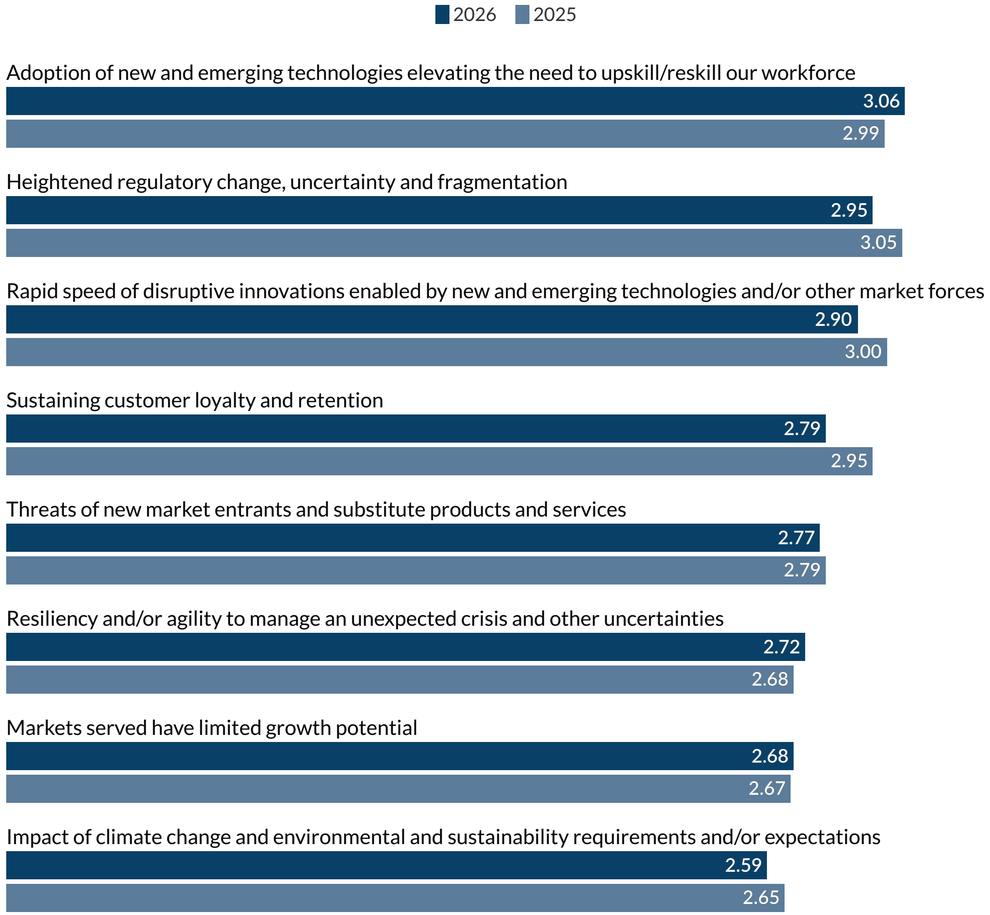
Top strategic risks

Though fewer in number among the top 10 near-term concerns, strategic risks — emerging technologies requiring workforce transformation and regulatory fragmentation — carry **high-impact potential**. These risks challenge the organisation's ability to adapt, innovate and comply in a fast-changing environment. The **need to upskill/reskill** in response to emerging technologies is a strategic imperative, not just an HR issue. **Regulatory fragmentation** across jurisdictions increases complexity in designing and developing new innovation strategies and requires agile compliance approaches.

Respondents signalled an overarching concern that their organisations may struggle to **adopt new and emerging technologies** due to challenges they face in competing for the talent and skills needed to realise fully the value proposition used to justify investing in these promising capabilities. As the rapid pace of technological change outstrips workforce capabilities, a strategic talent gap arises, requiring organisations to train employees and align the culture with new capabilities. Generative AI, agentic AI and other forms of automation are reshaping job roles, workforce architecture and workflows. Organisations are recognising that workforce transformation and talent readiness are core components of an effective digital strategy.

Regulatory change and complexity across jurisdictions increase operational burdens. Executives are concerned about fragmented landscapes in how data privacy, ESG, AI and other aspects of the business are regulated. Organisations should invest in regulatory intelligence to ensure compliance risk management is fully responsive to applicable laws and regulations and integrated into operations and operational and strategic decisions.

Figure 6: Strategic risks — near-term outlook



To provide insights about how different types of executives view near-term risks, we examined individual rankings of top risks across nine different positions. The table below highlights those risks that are ranked in the top five list of risks by position. The numbers (1 through 5) reflected in each column of the table indicate the relative rank within the top five for that risk by individuals in those positions.

Table 8: Top five near-term risks — by executive position*

Risks	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
Cyber threats	1		1	1	1	1		1	1
Third-party risks			2	2	2	2		4	3
Emergence of new risks from implementing AI			4	5		3		5	4
Economic conditions, including inflationary pressures	4	5			5		4	3	
Skills and talent acquisition and retention, leadership development and succession challenges	2	2					2		5
Operations and legacy IT infrastructure unable to meet performance expectations			3	3	3	4			
Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce		4	5		4	5			
Talent and labour availability	3	1					1		
Increases in labour costs	5	3					3		
Heightened regulatory change, uncertainty and fragmentation								2	2
Changes in global markets and trade policies				4					
Impact of expected demographic changes							5		
Managing multigenerational workforce demands and expectations							5		

Note: The number in each cell indicates the rank order of the top five risks by each executive position. Instances where the same rank is shown for more than one risk issue reflect ties.

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group. More extensive analyses across executive positions are available in a separate online appendix — visit www.protiviti.com or erm.ncsu.edu.

Across the board, **cyber threats** stand out as the most consistently ranked concern. This widespread prioritisation underscores the almost universal recognition that cybersecurity is no longer a siloed IT issue but rather a strategic enterprise risk with implications for brand reputation, operational continuity and regulatory compliance. The fact that it tops the list for roles as diverse as the board, CIO/CTO and CRO suggests a shared understanding of its systemic nature and the need for cross-functional mitigation strategies.

Economic concerns also made it to the top five list of risks for the board and CEO along with several other members of the C-suite team. Uncertainties about inflation, government policies (including the evolving tariff landscape) and interest rates are triggering risk concerns across the executive team and board.

Talent-related risks — including labour availability, talent acquisition, upskilling and leadership development — also show strong representation, particularly among the CEO, CHRO and board. These concerns reflect the growing pressure to attract and retain mission-critical talent in a competitive and evolving labour market. Interestingly, CHROs rank "talent and labour availability" as their top concern, signalling the strategic importance of workforce planning in conjunction with digital transformation initiatives. The CEO's prioritisation of both talent and labour availability and skills development further reinforces the strategic importance of human capital.

Differences in risk prioritisation reveal how each role's functional lens shapes their risk perspective. For example, **regulatory change and fragmentation** is a top concern for the CRO and CAE — roles with responsibilities for compliance and governance support, oversight and assurance — while it does not appear in the top five for the CEO or COO. Similarly, **third-party risks** are more prominent for the CFO, CIO/CTO, CAE and COO, reflecting their respective focus on operational and financial exposure to vendors, service providers and other ecosystem partners.

Overall, the analysis reveals a **core set of shared concerns** — cybersecurity, talent and economic conditions — while also illustrating how **role-specific responsibilities** shape risk prioritisation. This diversity of perspectives is valuable for enterprise risk management (ERM), as it ensures that risk oversight is both comprehensive and nuanced. Boards and executive teams should leverage these insights to foster cross-functional dialogue, align risk mitigation strategies and ensure that ERM reflects the full spectrum of leadership concerns.

Across the board, cyber threats stand out as the most consistently ranked concern. This widespread prioritisation underscores the almost universal recognition that cybersecurity is no longer a siloed IT issue but rather a strategic enterprise risk with implications for brand reputation, operational continuity and regulatory compliance.

The following table summarises the top five risks across the nine different industries we analysed. Based on the comparative analysis of top five near-term risks across nine industry sectors, several key insights emerge that highlight both convergence and divergence in risk priorities.

Table 9: Top five near-term risks — by industry group*

Risks	AD	CPS	EU	FSI	GOVT	HC	MD	NFPHE	TMT
Cyber threats	1	1	5	1	1	1	2	4	1
Third-party risks	2	5	2	2	2	3	4		
Heightened regulatory change, uncertainty and fragmentation			4			2		1	
Economic conditions, including inflationary pressures		3		5	5		5	5	
Emergence of new risks from implementing AI		5		3	4				3
Increases in labour costs	4	2					3		
Operations and legacy IT infrastructure unable to meet performance expectations	3				3				5
Talent and labour availability						4		3	
Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce				4		5			2
Rising threat of catastrophic natural disasters and weather phenomena			3						
Increase in global terrorism, crime and violence	5								
Impact of climate change and environmental and sustainability requirements and/or expectations			1						
Skills and talent acquisition and retention, leadership development and succession challenges								2	
Changes in global markets and trade policies							1		
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces									4
Sustaining customer loyalty and retention		4							

Note: The number in each cell indicates the rank order of the top five risks by each industry group. Instances where the same rank is shown for more than one risk issue reflect ties.

* More extensive analyses across industry groups are available in a separate online appendix — visit www.protiviti.com or erm.ncsu.edu.

Cyber threats are the most universally recognised risk, ranked first in six of the nine industry groups. This widespread concern reflects the pervasive nature of digital vulnerabilities across sectors. The consistency of this ranking suggests that cybersecurity is now viewed as a foundational risk that transcends industry boundaries, driven by increasing digitalisation, data dependency and growing sophistication of threat actors.

Third-party risks also show broad relevance, appearing in the top five for seven of the nine industries. This reflects the growing reliance on external vendors, cloud providers, online platforms, distribution channels and communications channels in the ecosystem that introduce operational and reputational vulnerabilities. Interestingly, industries with complex supply chains or regulatory oversight — such as **Manufacturing and Distribution** and **Financial Services** — rank this risk high, indicating heightened sensitivity to vendor performance and compliance.

Differences in risk prioritisation reveal how industry-specific dynamics shape risk perception. For example, **Energy and Utilities** uniquely ranks **impact of climate change and sustainability requirements** and **threats of natural disaster** as top concerns, reflecting regulatory pressures and environmental exposure. Meanwhile, **Not-for-Profit/Higher Education** prioritises **skill and talent acquisition** and **talent availability**, reflecting the connectivity of policy shifts in public funding and related workforce challenges.

Finally, **technology-driven risks** — such as AI implementation and workforce upskilling — are more prominent in **Technology, Media and Telecommunications, Financial Services,** and **Healthcare,** where innovation cycles are rapid and digital transformation is core to strategy. The TMT sector, in particular, ranks multiple technology-related risks in its top five, underscoring the pressure to stay ahead of the curve.

These findings suggest that while some risks are universal, others are deeply shaped by industry context, operational models and strategic priorities. Organisations that use these insights to tailor risk management strategies and opportunity pursuits to their sector's unique exposure remain vigilant to cross-industry threats.

While some risks are universal, others are deeply shaped by industry context, operational models and strategic priorities.

The following table summarises the top five risks across the different geographic regions we analysed.

Table 10: Top five near-term risks — by geographic region

Risks	North America	Latin America	Europe	Middle East & Africa	India	Asia	Australia & New Zealand
Cyber threats	1	1	1	2	1	4	
Third-party risks	2	4	2	5	2		5
Emergence of new risks from implementing AI	4	5		3		5	1
Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce		3		4	3	2	3
Operations and legacy IT infrastructure unable to meet performance expectations				1		1	2
Economic conditions, including inflationary pressures	3	2					4
Skills and talent acquisition and retention, leadership development and succession challenges			5			3	
Increases in labour costs			4		4		
Talent and labour availability			3				
Ensuring privacy and compliance with growing privacy and identity protection risks and expectations					5		
Heightened regulatory change, uncertainty and fragmentation	5						

Note: The number in each cell indicates the rank order of the top five risks by each geographic region.

Based on the comparative analysis of the top five near-term risks across seven global regions, several important patterns and regional nuances emerge that offer valuable insights into how geography shapes risk perception and prioritisation.

Cyber threats are the most universally recognised concern, ranking in the top five for six of the seven regions and occupying the top spot in North America, Latin America, Europe and India. As with the industry groupings we examined, this widespread prioritisation reflects the global nature of cyber risk. Interestingly, Australia and New Zealand did not rank cyber threats in their top five, likely due to the respondents in that region being heavily concentrated in government (57%) and mining (26%), indicating a different prioritisation of relative risks in those sectors.

As with the industry groupings, **third-party risks** also show broad concern, appearing in the top five for six regions. North America, Europe and India rank it as their second-highest risk, highlighting its strategic importance in these regions. The presence of this risk in Latin America, the Middle East and Africa, and Australia and New Zealand suggests that supply chain vulnerabilities and partner dependencies are a shared global challenge, though the intensity of concern varies.

Regional differences become more pronounced when examining risks tied to **technology adoption and workforce transformation**. Latin America, Asia, India, and Australia and New Zealand all rank the need to upskill/reskill in response to emerging technologies within their top three, suggesting a strong regional focus on digital capability building. In contrast, this risk does not appear in the top five for North America or Europe, which may reflect more mature digital capabilities. However, concerns about talent and labour availability are high in Europe.

Other notable divergences include the **emergence of AI-related risks**, which are ranked highest in Australia and New Zealand (the top risk) and appear in the top five for North America, Latin America, the Middle East and Africa, and Asia. This suggests global concern about unintended consequences of AI deployments, though the degree of that concern varies. Meanwhile, concerns regarding **economic conditions and inflationary pressures** are more prominent in the Americas and Australia and New Zealand.

Overall, while some risks — like cyber threats and third-party dependencies — are globally recognised, others reflect **regional distinctions** in viewing **economic uncertainties, technological maturity** and **regulatory environments**. These insights underscore the importance of tailoring ERM strategies to regional contexts while maintaining a global view on systemic risks.

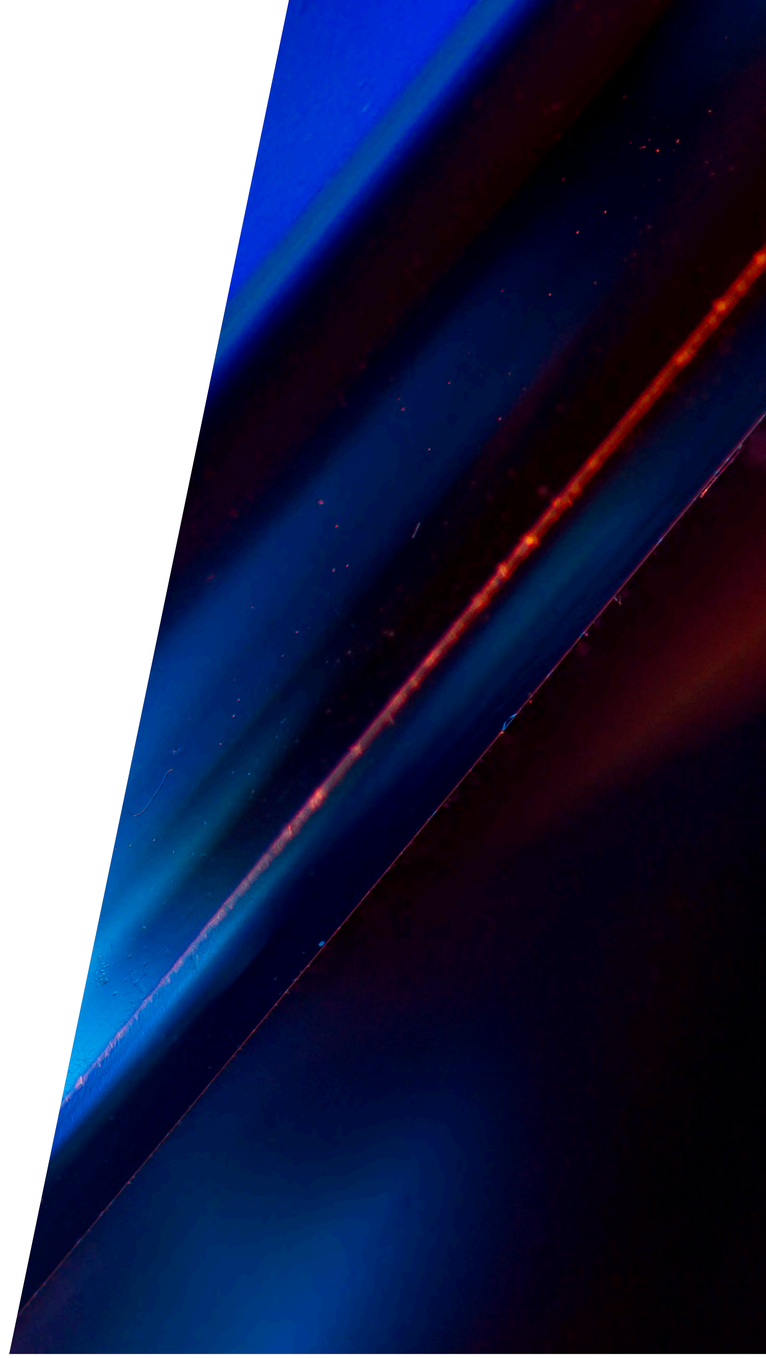
While some risks — like cyber threats and third-party dependencies — are globally recognised, others reflect regional distinctions in viewing economic uncertainties, technological maturity and regulatory environments.

The following table summarises the top five risks across the different categories of organisational size.

Table 11: Top five near-term risks — by organisation size

Risks	Largest organisations	Medium-to-large organisations	Small-to-medium organisations	Smallest organisations
Cyber threats	1	1	1	1
Third-party risks	2	2	3	
Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce	3		2	5
Emergence of new risks from implementing AI	5		4	4
Operations and legacy IT infrastructure unable to meet performance expectations	4	4	5	
Economic conditions, including inflationary pressures		3		2
Skills and talent acquisition and retention, leadership development and succession planning		5		3

Note: The number in each cell indicates the rank order of the top five risks by each group of organisations.



Based on the analysis of risk perceptions across four organisational size categories, several key insights emerge that highlight both shared concerns and distinct priorities shaped by scale and complexity.

Once again, **cyber threats** are the most universally recognised risk. Being ranked the top risk across all four size categories underscores the pervasive nature of cybersecurity concerns, regardless of organisational scale. Also, **third-party risks** are prominent among all categories except for the smallest organisations (in fact, the risk does not appear in their top five). Larger companies likely have more complex vendor networks and outsourcing arrangements, making them more vulnerable to disruptions or reputational damage stemming from external partners.

Our findings suggest that while some risks are universal, others are shaped by the structural realities of organisation size, resource availability and strategic complexity.

For example, the results for **economic conditions and inflationary pressures** may reflect greater sensitivity to margin pressures and resource constraints among midsized and smaller entities. Similarly, the results for **skills and talent acquisition and retention** suggest that workforce challenges are particularly acute in medium-to-large and the smallest organisations, possibly due to competition for specialised talent or succession planning concerns.

Interestingly, **technology-related risks**, including the need to upskill for emerging technologies and the risks associated with AI implementations, are more widely recognised among the largest and smallest organisations. Large organisations are likely to face pressure to innovate at scale, while small organisations may be grappling with how to adopt new technologies without the benefit of deep internal expertise.

Being ranked the top risk across all four size categories underscores the pervasive nature of cybersecurity concerns, regardless of organisational scale.

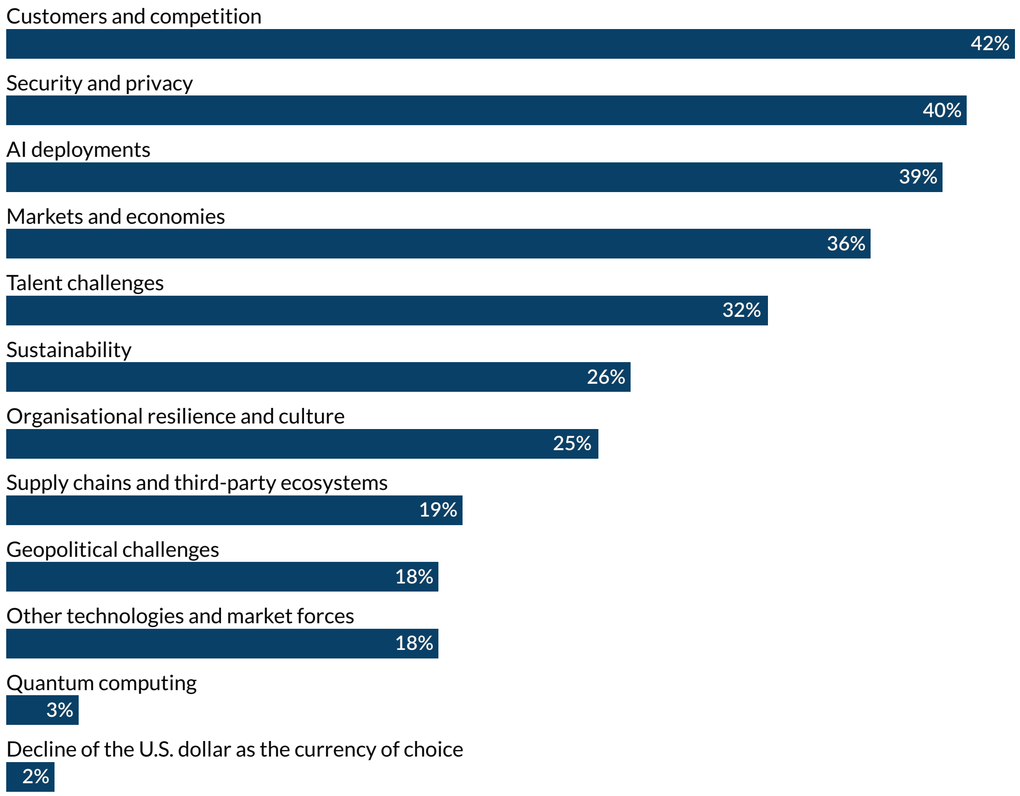
06

Managing long-term risks (next 10 years)

In addition to obtaining an understanding of near-term concerns, we also asked respondents to select from a list of 12 risk themes what they believe represent the top three risk areas their organisations are likely to consider most when evaluating strategies and making investments over the next 10 years. We formulated the risk themes considering the 28 specific risk areas we examined over the near-term to simplify the survey participants' long-term risk assessment.

Participants provided a rank-ordered list of their top three risk themes important to their organisation over a 10-year time horizon. Figure 7 shows the risk themes listed in rank order based on the frequency that each risk theme was included in the respondents' top three choices. This list provides an indication of what our 1,540 respondents perceive to be their organisation's most significant long-term risk concerns in light of their organisation's business model and strategy.

Figure 7: Long-term risks



Percentages reflect frequency with which each area was selected among the top three.

Based on the rank-ordered list of long-term risk themes, here are several key insights that would be particularly valuable for boards and executive teams to monitor and discuss as they look out over the next decade:

- **Strategic focus on market positioning and trust:** The top four long-term concerns — customers and competition, security and privacy, AI deployment, and markets and economies — reflect a clear emphasis on maintaining competitive relevance and stakeholder trust in a rapidly evolving digital landscape. Executives are signalling that long-term strategy must prioritise customer experiences, data protection and responsible innovation. These themes are deeply interconnected with an emphasis on growth, market share and brand credibility.

- **Talent and technology as dual enablers — and risks:** Talent challenges combined with AI deployment both rank highly, suggesting that the workforce implications of emerging technologies are persistent long-term as well as near-term concerns. The dual focus on enabling tools and potential risks implies that long-term investments must include robust workforce development, responsible AI governance and cultural transformation to support innovation.

- **Broader systemic risks are rising — but unevenly prioritised long-term:** Themes like sustainability, organisational resilience, supply chains and geopolitical challenges reflect growing awareness of systemic disruptions — from climate change to global instability. However, their lower rankings suggest that while these risks are acknowledged, they may not yet be fully integrated into strategy setting and execution. Management and boards should consider whether these areas are underweighted in current risk frameworks, especially given their potential to reshape markets and supply chains long-term.

- **Emerging and peripheral risks require strategic foresight:** Risks such as quantum computing and the potential decline of the U.S. dollar are currently viewed as peripheral with their low prioritisation. Nonetheless, forward-looking organisations should monitor these developments and consider scenario planning to ensure strategic agility as the question of their relevance and potential impact is clarified. If either of these developments become a reality, it will be too late for the unprepared.

These insights suggest that a long-term view of risk is truly strategic and must encompass market positioning, technological expansion, workforce transformation and systemic resilience so that new opportunities and emerging risks are not overlooked. This forward-thinking approach helps executive teams adapt more quickly to shifts in the external environment through better anticipation of market trends and technological advancements, challenging underlying strategic assumptions, formulating plausible as well as extreme scenarios, stress testing strategic alternatives, and making more informed decisions about resource allocation, capability building and prioritising investments. Such vigilance is table stakes in the C-suite and boardroom.

Table 12: Top three long-term risks — by executive position*

	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
AI deployments	36%	39%	36%	40%	49%	46%	38%	37%	33%
Markets and economies	43%	31%	38%	37%	33%	45%	33%	37%	36%
Customers and competition	47%	48%	37%	31%	30%	24%	37%	59%	60%
Security and privacy	32%	19%	45%	50%	50%	64%	42%	23%	25%
Talent challenges	36%	43%	33%	30%	23%	30%	33%	29%	30%
Sustainability	14%	14%	36%	33%	34%	30%	21%	15%	14%

Percentages reflect frequency with which each area was selected among the top three. The top three areas for each executive role are highlighted in blue (ties included).

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group.

Directors and most C-suite leaders share concerns about long-term AI deployment risks and potential impacts from shifting markets and economies. The same thing can be said regarding concerns related to customers and competition, with the exception of COOs, CIOs/CTOs and CISOs, who prioritise data, technology and market dynamics — in that order. Interestingly, CEOs and board members focus more on talent challenges than other members of the C-suite, recognising the importance of talent to organisational success. Effective strategic oversight at the highest level requires a comprehensive approach to talent management to ensure the organisation has the right people in place to execute its shared vision and address future challenges.

Table 13: Top three long-term risks — by industry group

	AD	CPS	EU	FSI	GOVT	HC	MD	NFPHE	TMT
Security and privacy	58%	28%	35%	47%	56%	37%	22%	29%	57%
AI deployments	41%	43%	20%	47%	30%	45%	29%	29%	53%
Markets and economies	37%	34%	37%	40%	39%	34%	39%	19%	32%
Customers and competition	25%	55%	29%	48%	21%	48%	45%	59%	30%
Sustainability	38%	19%	43%	19%	48%	12%	31%	15%	25%
Supply chains and third-party ecosystems	14%	30%	37%	8%	6%	15%	34%	10%	8%
Organisational resilience and culture	25%	24%	26%	25%	23%	29%	20%	49%	18%
Talent challenges	25%	30%	26%	33%	31%	32%	33%	41%	30%

Percentages reflect frequency with which each area was selected among the top three. The top three areas for each industry group are highlighted in blue.

Three industry groups place higher emphasis on sustainability matters:

- Many governments prioritise sustainability matters over commercial sectors due to their public accountability, regulatory authority, commitment to long-term stewardship and the need to address pressing global challenges. By leading the way, they can create a framework that encourages commercial sectors to adopt responsible sustainability practices.
- The Energy and Utility sector's elevated focus on sustainability is driven by responses from our 70 respondents representing non-U.S. companies due to the scale of their environmental impact, regulatory pressures, resource management challenges, stakeholder expectations and the essential nature of their services. By prioritising sustainability, these companies not only comply with legal and societal demands but also secure the viability of their long-term market permission to operate.
- Companies in Aerospace and Defense are driven by regulatory compliance, market demands, technological advancements and the need to sustain long-term viability. Given the commercial airline sector's cross-border operations, a sustainability focus makes sense because of requirements across the globe.

Energy and Utility companies emphasise supply chains and third-party ecosystems to drive efficiencies due to the complexity of their operations that encompass various interconnected stages, including extraction, generation, transmission, distribution and retail. The integration of smart grid technologies and the Internet of Things necessitates collaboration with various technology providers and service partners. In addition, these companies are increasingly focused on sustainability and reducing their carbon footprints, which often involves working with suppliers and third parties that share similar goals and practices.

Table 14: Top three long-term risks — by geographic region

	North America	Latin America	Europe	Middle East & Africa	India	Asia	Australia & New Zealand
Security and privacy	38%	28%	45%	47%	50%	30%	51%
Customers and competition	45%	43%	36%	37%	49%	48%	30%
Markets and economies	36%	37%	31%	43%	37%	43%	43%
AI deployments	44%	41%	39%	37%	47%	33%	24%
Sustainability	16%	23%	34%	44%	23%	21%	54%
Talent challenges	28%	36%	27%	29%	20%	53%	36%

Percentages reflect frequency with which each area was selected among the top three. The top three areas for each geographic region are highlighted in blue.

Two regions place a higher priority on sustainability matters.

- **Middle East and Africa:** Many Middle Eastern countries struggle with water scarcity and desertification, while climate change brings extreme temperatures and unpredictable weather. Traditional reliance on oil exports calls for economic diversification as global energy demand shifts to renewables. Africa's large youth population is more environmentally conscious. Many nations in the Middle East and Africa region have joined international climate change agreements because of mutual interest in compelling developed economies to reduce carbon emissions.

- **Australia and New Zealand:** This year's concentration of the region's respondents in government and mining is the likely reason for the stronger emphasis on sustainability.

Asia places a higher priority on talent challenges, likely because of demographic trends (ageing population). Other factors include economic growth priorities, competitive pressures for talent with Western economies and the need for innovation.

Table 15: Top three long-term risks — by organisation size

	Largest organisations	Medium-to-large organisations	Small-to-medium organisations	Smallest organisations
Customers and competition	43%	40%	41%	47%
AI deployments	40%	40%	38%	41%
Security and privacy	41%	39%	45%	34%
Markets and economies	40%	35%	35%	36%
Talent challenges	27%	33%	31%	37%

Results across organisation size are reasonably consistent. The largest organisations report a slightly stronger focus on markets and economies, and the smallest, to no surprise, recognise talent challenges as a top long-term risk.

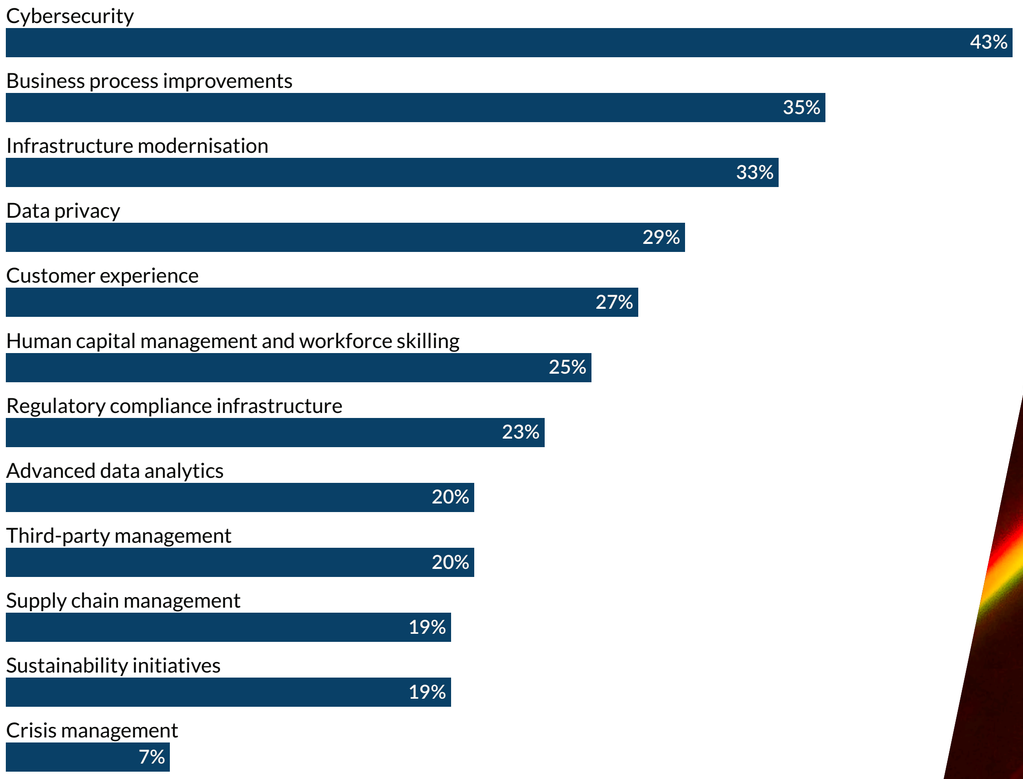
07

Strategic investment priorities

We asked respondents to identify the top three strategic investment priorities, in rank order, in which their organisations are likely to invest the most over the next two to three years given the opportunities and risks our report has highlighted. We provided a list of 12 investment areas that relate to some of the strategic and operational near-term risk issues our survey examined.

Figure 8 shows the number of times each investment area was included among the top three choices by the 1,540 respondents.

Figure 8: Top strategic investment priorities



Percentages reflect frequency with which each area was selected among the top three.

The consensus in the overall results confirms that leaders are focusing on **resilience, relevance** and **execution**. Capital is being dedicated to fixing the operational core, ensuring security compliance and building the necessary infrastructure to scale AI and other advanced digital capabilities. With **data privacy** and **customer experience** ranked fourth and fifth, respectively, the propensity to invest in all of these areas suggests that many leaders are thinking and acting digitally. The overall survey results define the baseline investment thesis, clustering the top priorities into a clear hierarchy of foundational needs, operational levers and growth engines.

As organisations adopt AI and connect more devices, the surface area for attacks expands exponentially, making **cybersecurity** the highest-priority non-discretionary area of spending. It is a **fiduciary obligation** and **brand protection** necessity. The high ranking of **data privacy** reinforces this defensive posture. With regulatory shifts like GDPR in the EU and CCPA in California, investment in privacy infrastructure is seen as inseparable from security, forming a comprehensive **digital defence layer**.

In tandem, **infrastructure modernisation** is another investment priority. Legacy systems cannot support the computational demands of AI, the data volumes of modern operations or the speed required for competitive redeployment. Evolving the infrastructure is therefore the necessary antecedent investment that unlocks the value of cybersecurity (security-by-design), process automation and digital disruption.

The high prioritisation of **business process improvements** confirms that investment focus is being directed to operational leverage. Process automation and enhanced decision-making offer the most direct path to realising ROI from AI and automation tools. This investment is aimed squarely at **removing friction, accelerating cycles, lowering the cost-to-serve (reducing labour costs) and speeding up quality decision-making.**

While **human capital management and workforce skilling** ranks sixth overall, its high prioritisation by roles such as the CHRO and in labour-intensive industries demonstrates it is the **critical bridge investment** and an essential indicator of strategic alignment. Organisations wisely recognise that defensive and infrastructural spending and process improvements are useless without the human capital to manage the new systems and drive the change. This spending acts as an **enabling investment** to ensure the benefits of technology investments are fully realised. Organisations that fail to align their investments with aggressive talent upskilling will risk turning capital expenditures into potentially high-risk, low-return assets.

As a top five priority, **customer experience** clearly demonstrates that even amid intense defensive spending, executives are dedicating budget to market differentiation and revenue growth. Improving customer experiences is the primary external-facing metric of the firm's overall digital maturity. That focus drives foundational investments channelled toward improving customer-facing processes and creating demonstrable customer value.

Table 16: Top three strategic investment priorities — by executive position*

	Board	CEO	CFO	COO	CIO/CTO	CISO	CHRO	CRO	CAE
Cybersecurity	32%	27%	39%	39%	42%	53%	25%	51%	51%
Business process improvements	48%	60%	21%	20%	32%	24%	46%	48%	51%
Customer experience	36%	42%	19%	15%	21%	17%	25%	33%	43%
Infrastructure modernisation	32%	32%	32%	34%	30%	21%	37%	44%	33%
Data privacy	21%	10%	40%	42%	39%	54%	25%	7%	7%
Human capital management and workforce skilling	40%	50%	18%	19%	16%	15%	63%	23%	33%
Regulatory compliance infrastructure	12%	13%	30%	26%	32%	26%	8%	20%	17%

Percentages reflect frequency with which each area was selected among the top three. Top three areas for each executive role are highlighted in blue (ties included).

* Does not include 3 roles (CSO, CDO, CLO) for which there were low numbers of responses, and does not include the OCS group.

Strategic priorities diverge significantly when viewed through the lens of functional accountability, reflecting the primary duties and immediate pressures of each C-suite role.

The roles responsible for high-level strategy and overall outcomes — **board members and CEOs** — exhibit a strong focus on **business process improvements** and **human capital,** followed by **customer experience.**

- The **CEO** and **board** prioritise execution and impact. The focus is on how the organisation operates and the capability of the team to deliver superior outcomes. They delegate the primary technical defence to the CFO and CIO/CTO, but demand results in operational excellence.

The executives responsible for protecting the balance sheet and ensuring operational stability have a distinctly defensive investment profile.

- The top investment priorities for **CFOs** and **COOs** are aligned: **data privacy, cybersecurity** and **infrastructure modernisation.** This is a clear **"protect the fortress"** strategy. For the CFO, these are non-negotiable costs of fiduciary duty. For the COO, system stability and data integrity are prerequisites for reliable operations. The relative de-prioritisation of growth-related spending (like customer experience) shows a current preference for operational integrity over immediate expansion.

- **CIOs/CTOs** and **CISOs** also prioritise **data privacy, cybersecurity** and **regulatory compliance.** This is a profile dominated by the **technical defence layer.** They recognise that the pressures of digital deployment necessitate a robust, compliant foundation to manage increasing complexity and fragmented regulatory oversight.

- **CROs and CAEs** focus on **cybersecurity** and **business process improvements.** The oversight and control functions are interested in the areas most critical for risk reduction and assurance: securing the system and ensuring the underlying processes and platforms are relevant, stable, reliable and resilient.

- The **CHRO** is the only executive to lead with **human capital management and skilling** as their top strategic investment priority, followed by **business process improvements** and **infrastructure modernisation.** This is a sophisticated understanding of the value chain: The best investment is in employees, who will then optimise the processes with a strong focus on operational improvements.

Table 17: Top three strategic investment priorities — by industry group

	AD	CPS	EU	FSI	GOVT	HC	MD	NFPHE	TMT
Cybersecurity	42%	41%	33%	57%	36%	38%	30%	37%	55%
Infrastructure modernisation	36%	24%	63%	25%	43%	29%	39%	44%	20%
Business process improvements	26%	33%	30%	40%	15%	42%	42%	54%	28%
Data privacy	48%	23%	9%	33%	50%	20%	12%	9%	52%
Customer experience	7%	42%	16%	37%	9%	31%	20%	49%	24%
Supply chain management	18%	36%	34%	4%	2%	13%	43%	0%	10%
Regulatory compliance infrastructure	30%	18%	37%	23%	35%	24%	16%	19%	19%
Sustainability initiatives	21%	14%	27%	11%	38%	16%	23%	9%	19%

Percentages reflect frequency with which each area was selected among the top three. The top three areas for each industry group are highlighted in blue.

An industry context defines the most pressing investment priority, shaped by the sector's regulatory environment, asset base and customer engagement model. Industries dealing with highly sensitive data or critical infrastructure place an existential premium on defence.

- **Financial Services** and **Technology, Media and Telecommunications:** Both include **cybersecurity, data privacy** and **business process improvements** in their top three strategic investment priorities. For Financial Services, this investment focus protects customer assets and system integrity. For Technology, Media and Telecommunications, it protects proprietary IP and product platforms.

- **Government:** The Government sector leads with **data privacy,** prioritising the protection of citizen data and public trust over all other areas. This is followed by **infrastructure modernisation** and **sustainability initiatives,** confirming the urgent need to replace legacy technology and manage cyber threats.

Sectors relying on vast physical assets and complex logistics prioritise the underlying platforms.

- **Manufacturing and Distribution** and **Energy and Utilities:** Both rank **infrastructure modernisation** as a high priority. This is the prerequisite for deploying any smart factory, grid optimisation or supply chain tracking technology. Without a modern infrastructure backbone, automation efforts are at risk of being stalled. Manufacturing and Distribution also includes **business process improvements** and **supply chain management,** focusing on efficiency and protecting operational technology systems. Energy and Utilities follows with **regulatory compliance infrastructure** and **supply chain management.**

Customer- and patient-centric industries focus their primary investment on improving the experience and delivery of services.

- **Consumer Products and Services:** Leads with **customer experience**, the clearest revenue driver. This is followed by **cybersecurity** to protect brand trust and **supply chain management** to ensure product availability. This investment focus is designed for **brand growth and fulfilment**.

- **Healthcare** and **Not-for-Profit/Higher Education:** Both prioritise **business process improvements** and **customer experience** as top investments. In these environments, this focus offers an effective strategy to combat administrative inefficiencies and optimise resource deployment. These are followed by **cybersecurity** for Healthcare and **infrastructure modernisation** for Not-for-Profit/Higher Education, confirming a universal focus on streamlined service delivery.

Overall, our survey results identify three critical, interlocking insights for investment strategy over the next two to three years.

- **The inseparability of defence and transformation:** The data shows a unified, three-part digital foundation investment: cybersecurity, data privacy and infrastructure modernisation. These three areas must be funded and executed as a single, coherent program, not as siloed departmental budgets. Failure in any one area — a cyber breach, a privacy violation, a system outage or an inability to innovate in a rapidly evolving marketplace — will neutralise gains made in process or customer experience improvements. Investment in this digital foundation is now the core enabler of transformation, not a separate cost centre.

- **The bottleneck of talent skilling:** While human capital management and workforce skilling ranks sixth overall, it functions as a strategic bottleneck for the entire investment portfolio. Technology systems are being funded and processes are being reimagined as disruptive innovation continues, but the people required to operate and optimise the new systems and processes are a mid-tier priority. Organisations must prioritise human capital management in planning transformation initiatives. Skilling should be viewed as an expedited prerequisite for achieving ROI in process improvements and enhancing customer experiences. The true value of a large infrastructure investment is only realised when the workforce can fully utilise the new capabilities, demanding a proportional investment in human capital and workforce development to capture the expected value and returns.
- **The shift from project-based to platform investment:** The high ranking of infrastructure modernisation (and its elevation as a near-term risk) suggests executives are recognising the limits of tactical, project-based IT spending. The move to modern infrastructure (cloud, modular systems, centralised data platforms) is a commitment to a platform-based operating model. This platform approach facilitates continuous **business process improvements** and provides a robust engine for **advanced data analytics**, which, while a mid-tier investment priority, is the long-term engine for competitive differentiation. Executives must ensure their infrastructure modernisation investments are guided not just by cost savings, but also by the ability to iterate and scale new AI-driven processes rapidly.

In summary, the most successful organisations over the next two to three years will be those that master the alignment between their defensive and offensive investments, secured by a dedicated and upskilled workforce.

Organisations must prioritise human capital management in planning transformation initiatives. Skilling should be viewed as an expedited prerequisite for achieving ROI in process improvements and enhancing customer experiences.

Closing comments

The results of this year's survey of 1,540 board members and C-suite executives reveal optimism about growth opportunities despite economic, workforce and technological challenges. The findings emphasise that organisations must pursue strategic growth and business resilience together in today's complex, dynamic risk landscape.

The most successful organisations will be those that treat opportunity and risk as interdependent forces — embedding agility, foresight and cross-functional collaboration into the core of their strategic agenda. This report is intended to catalyse those conversations and support leaders in building organisations that thrive amid uncertainty and change.

For more detailed results from our survey based on executive role and industry, appendices are available at www.protiviti.com and erm.ncsu.edu.

Research team and authors

NC State University's ERM Initiative

Mark Beasley
Professor and Director of the ERM Initiative

Bruce Branson
Professor and Associate Director of the ERM Initiative

Don Pagach
Professor and Director of Research of the ERM Initiative

Protiviti

Carol Beaumier
Senior Managing Director

Matthew Moore
Managing Director

Jim DeLoach
Managing Director

Kevin Donahue
Senior Director

Shaun Lappi
Research Manager

Shannon West
Project Manager

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

About NC State University's ERM Initiative

The Enterprise Risk Management (ERM) Initiative in the Poole College of Management at NC State University provides thought leadership about ERM practices and their integration with strategy and corporate governance. Faculty in the ERM Initiative frequently work with boards of directors and senior management teams helping them link ERM to strategy and governance, host executive workshops and educational training sessions, and issue research and thought papers on practical approaches to implementing more effective risk oversight techniques (erm.ncsu.edu).

protiviti®

NC STATE Poole College of Management
Enterprise Risk Management Initiative

www.protiviti.com

erm.ncsu.edu