

FERMA

Anticipating changes
Shaping the future

In partnership with



Global Risk Manager Survey Report

2026



Foreword

We are delighted to present the 2026 Global Risk Manager Survey report, the latest edition of a study conducted every two years since 2002. Initially focused on Europe, the survey became global in scope in 2024 and now provides a unique overview of the perspectives, priorities and practices of risk professionals worldwide. We warmly thank our partners (ALARYS, Club FrancoRisk, IFRIMA, IRMSA, PARIMA, RIMS and RMIA) as well as the PwC network, whose expertise and support have been instrumental in making this a truly global study and in gathering insights from respondents across 79 countries.

The 2026 Global Risk Manager Survey offers a clear message: risk can no longer be viewed as a series of independent challenges managed in isolation. Organisations now operate in an environment where geopolitical instability, cyber threats, Artificial Intelligence (AI), economic volatility, climate change, and regulatory complexity increasingly interact and reinforce one another, creating a new reality of interconnected, fast-moving and compounding risks.

The findings reveal a striking shift in risk priorities across time horizons. In the short term, geopolitical uncertainty has emerged as the foremost concern for organisations worldwide. Over the medium term, AI has become the defining strategic risk and opportunity. Over the longer term, climate adaptation and natural catastrophes remain dominant concerns, highlighting the need to combine short and medium-term resilience with long-term sustainability and transformation.

Against this backdrop, the role of the Risk Manager is evolving rapidly. Risk Managers are increasingly acting as strategic advisors, helping leadership teams navigate uncertainty, support decision making and strengthen organisational resilience. The survey shows sustained involvement in corporate strategy, growing influence over ESG matters, deeper collaboration with technology and cybersecurity functions, and an expanding contribution to operational resilience, strategic preparedness, and risk culture.

At the same time, the findings expose a paradox. Organisations increasingly recognise the importance of emerging risks, particularly AI and geopolitical disruption, yet many acknowledge that these are among the least adequately managed. This widening gap between awareness and preparedness has become one of the defining challenges of modern risk management. Closing that gap will require stronger governance, more sophisticated risk quantification, greater use of technology and closer integration between risk management and business decision-making.

The survey also highlights a profession in transformation. Risk Managers are investing in digital capabilities, exploring AI-enabled solutions, supporting sustainability agendas and helping organisations rethink their approach to risk financing and insurance. Across these areas, the objective is the same: to build resilient organisations that can absorb shocks, adapt to changes, transform when necessary and continue to create value in an increasingly uncertain world.

Our 2026 survey demonstrates that resilience is becoming a defining source of competitive advantage. Organisations that successfully connect short-term risk management with long-term strategic foresight will be better positioned to navigate disruption, seize opportunities and thrive in an era of permanent uncertainty.

The Risk Manager has a central role to play in making this possible.

Philippe Cotelle,
President of FERMA

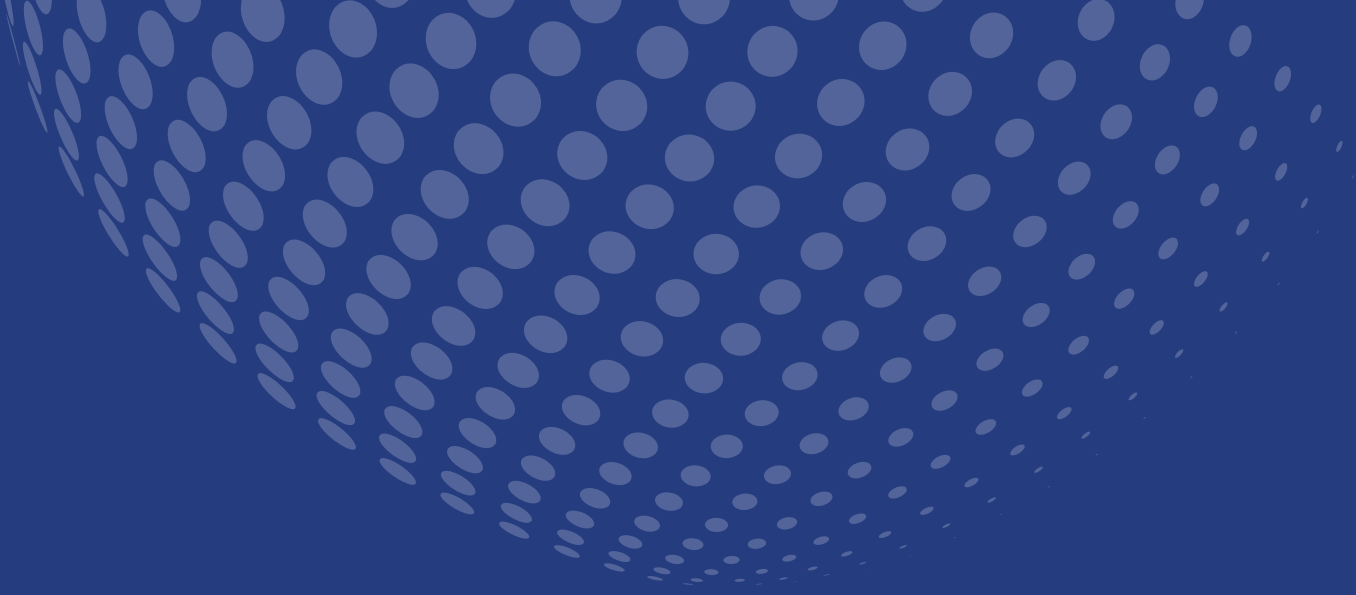
Tadas Cilcius,
FERMA Board Member and Chair
of the Global Risk Manager Survey

Patrice Morot,
Global Risk Services Leader, PwC France

Laure Laheurte,
Risk Services Partner, PwC France

Contents

Key findings	7
Survey respondents	8
Artificial Intelligence emerges as a key threat across all time horizons	9
Risk Managers remain broadly engaged across the organisation and expand their role	11
Risk Managers strengthen ESG governance amid mixed ESG progress	12
Technology use expands across ERM, while AI adoption gains momentum	13
Insurance strategies adapt as market pressure persists	14
Methodology and profile of the survey respondents	17
Methodology	18
Profile of survey respondents	20
Risk priorities shift across time horizons, in an interconnected risk landscape shaped by volatility and AI	29
Top critical threats to the organisation within the next 12 months	30
Top 5 critical threats to the organisation's growth prospects within the next 3 and 10 years	34
Top risks considered as not adequately treated	37
Part I: Risk Managers' role in strategy, resilience and governance	39
Risk Managers remain connected as risk mapping expands and governance involvement varies	40
Risk Managers support strategy and resilience	43
Risk Managers' investment priorities continue to vary by time horizon	45
Geopolitical risk is a key concern, most commonly addressed through monitoring activities	46
Part II: Risk Managers strengthen ESG governance amid uneven progress on climate change and social practices	47
ESG involvement remains steady, while governance responsibilities gain traction	48
Climate-change practices show modest progress, with greater focus on transition impacts	50
Social ESG practices gain ground, but maturity varies	51
Part III: Risk Managers' evolving role in digital and technological transformation	53
Technology adoption is expanding across all risk management activities	54
Risk Managers remain closely connected with tech functions to manage technology-related risks across the organisation	57
Progressive adoption of Artificial Intelligence	58
Part IV: Insurance Managers maintain established risk financing strategies	61
Over the past 12 months, Insurance Managers have adapted to a changing market	62
Over the next two years, risk retention remains dominant as Insurance Managers explore targeted alternative solutions	64
Part V: The maturity of the Enterprise Risk Management model	67



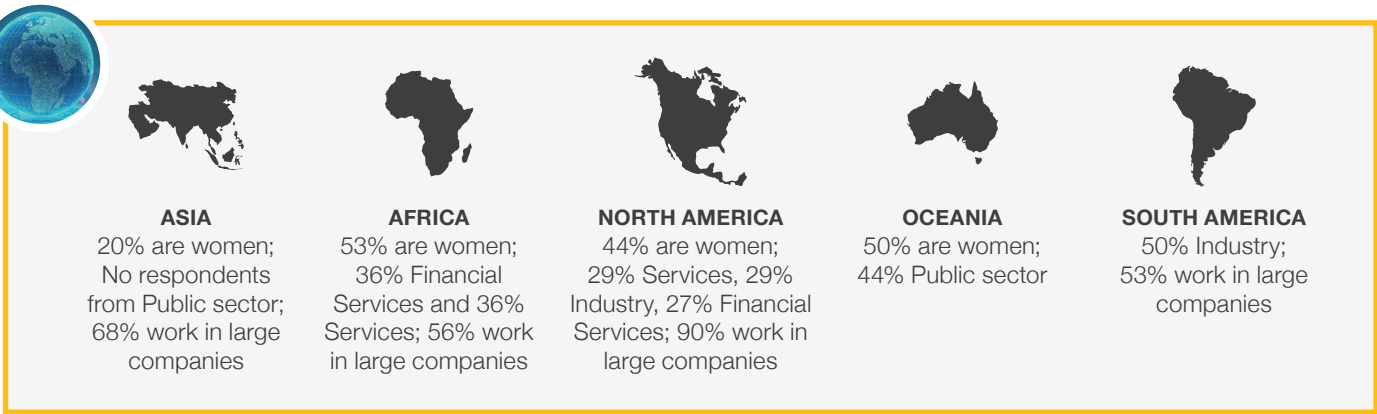
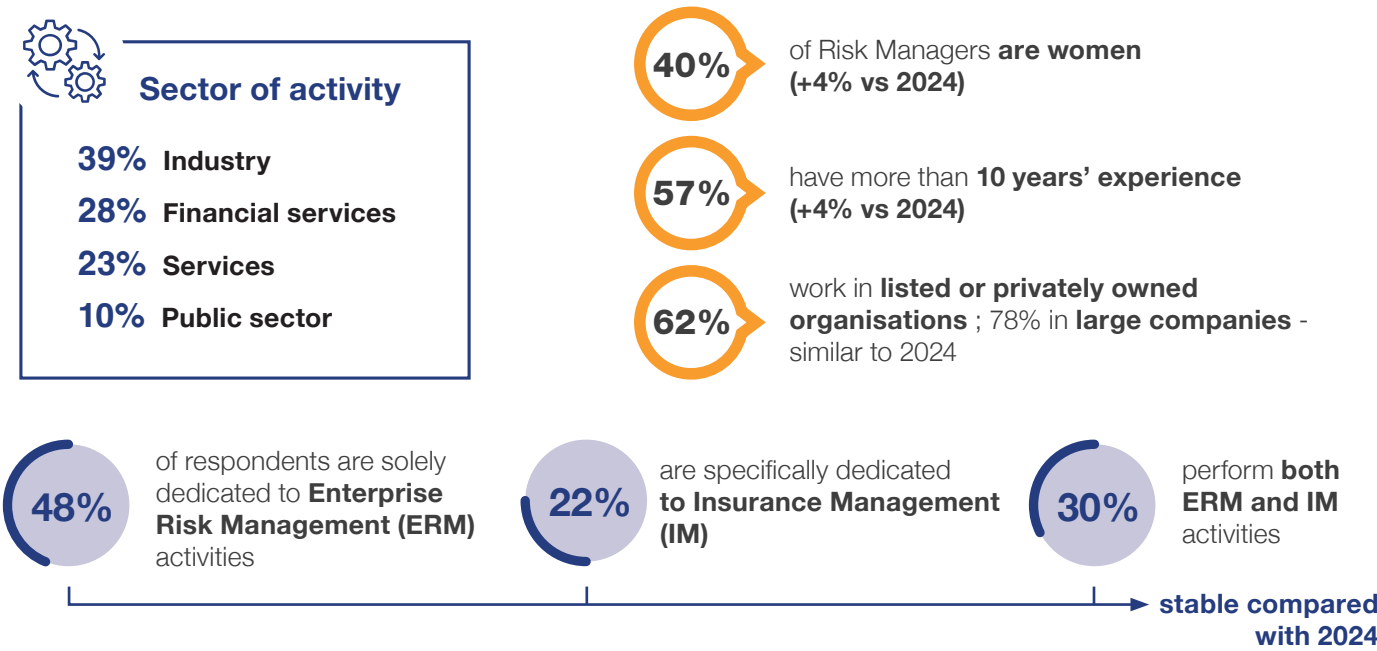
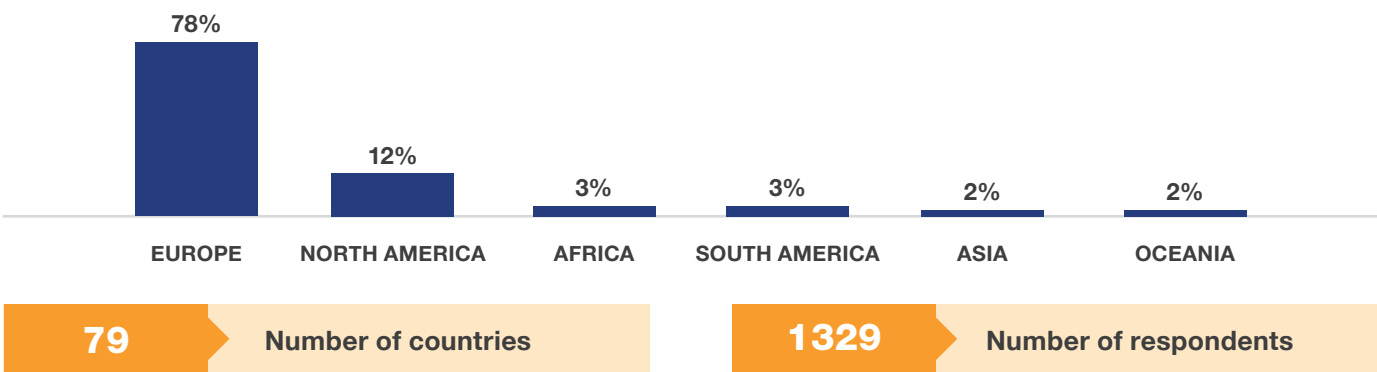
Key findings

Key findings

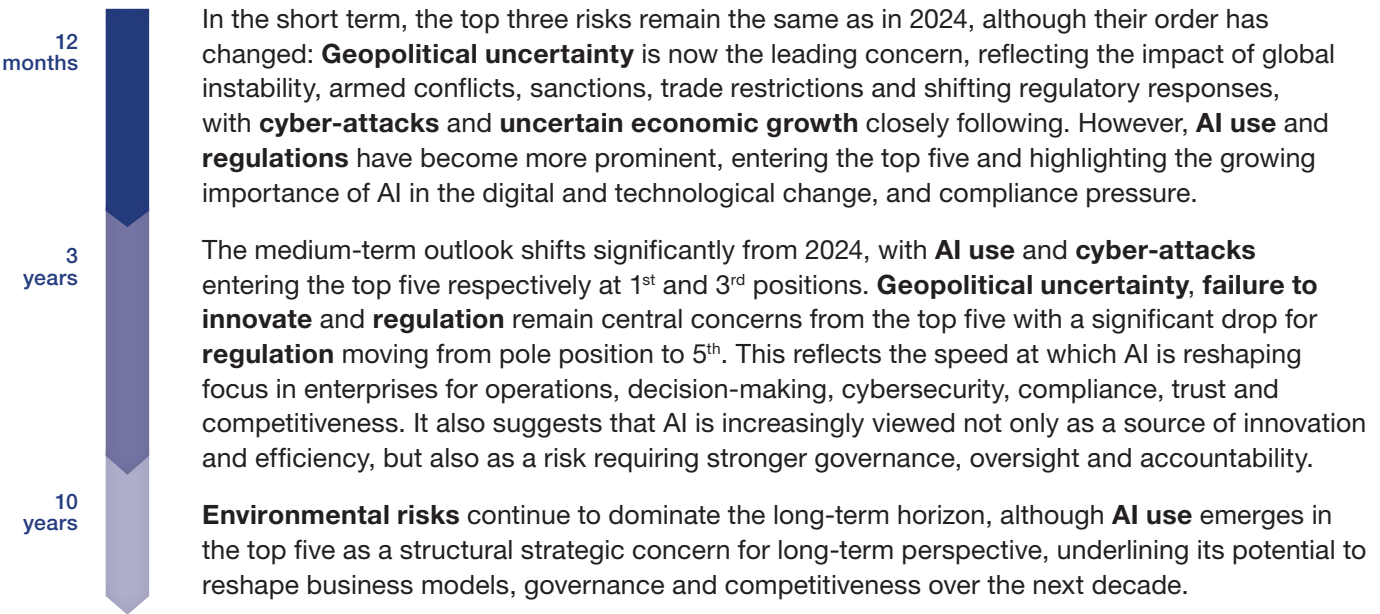
Survey respondents

The 2026 Global Risk Manager Survey reflects a broad global view of the risk management profession, with responses from Risk and Insurance Managers across multiple regions and sectors. The respondent base remains largely composed of experienced professionals, confirming that risk management continues to be a senior and specialised function. The profession is becoming more gender-balanced, with a growing representation of women, particularly among younger professionals.

Respondents by continent



Artificial Intelligence emerges as a key threat across all time horizons



Overall, the survey shows that organisations feel least prepared to manage fast-moving and complex risks, particularly AI, geopolitical uncertainty and technological change. This complex risk landscape reinforces the need for Risk Managers to act as strategic partners, helping leadership connect short-term disruption with long-term resilience through stronger governance, clearer accountability, scenario planning, risk quantification and more integrated risk management.

Aligning growth ambitions with resilience priorities
“It’s often said that successful leaders need both a microscope and a telescope to help them identify near-term threats while spotting long-term opportunities. This tension across time horizons is a recurring theme in PwC’s 29th Global CEO Survey...”
Source: PwC, 29th Global CEO Survey: Leading through uncertainty in the age of AI, 2026

Risk Managers and CEOs are seeing the same disruption, but from different angles. CEOs are focused on growth, reinvention and investment decisions; Risk Managers are focused on preparedness, governance, resilience and risk treatment. Bringing the two perspectives together strengthens the case for Risk Managers as strategic partners to leadership.

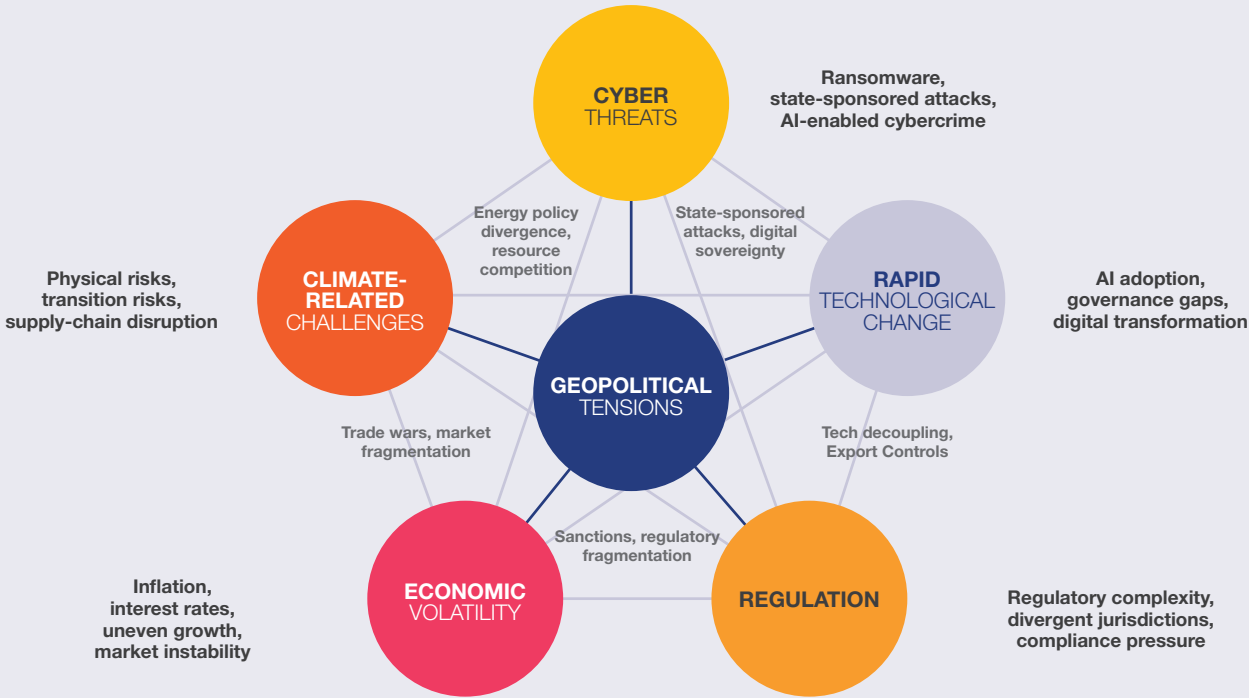
The opportunity for Risk Managers is to help organisations bridge this gap — enabling growth and innovation while strengthening resilience, governance and long-term viability.

Key findings



Interconnected risks require an integrated management approach

The risk landscape is becoming increasingly complex, driven by the growing interconnectedness and layering of risks across key areas such as technology and regulation, as well as the global nature of today’s businesses and supply chains. Geopolitical uncertainty, cyber-attacks, AI development, macro-economic volatility, the intensity of regulatory oversight and climate change can no longer be managed separately, as developments in one area often amplify risks in another. Geopolitical uncertainty acts as a central amplifier intensifying cyber, economic, technological, regulatory and climate-related risks simultaneously. This interconnectedness requires an integrated, cross-functional approach to risk management.

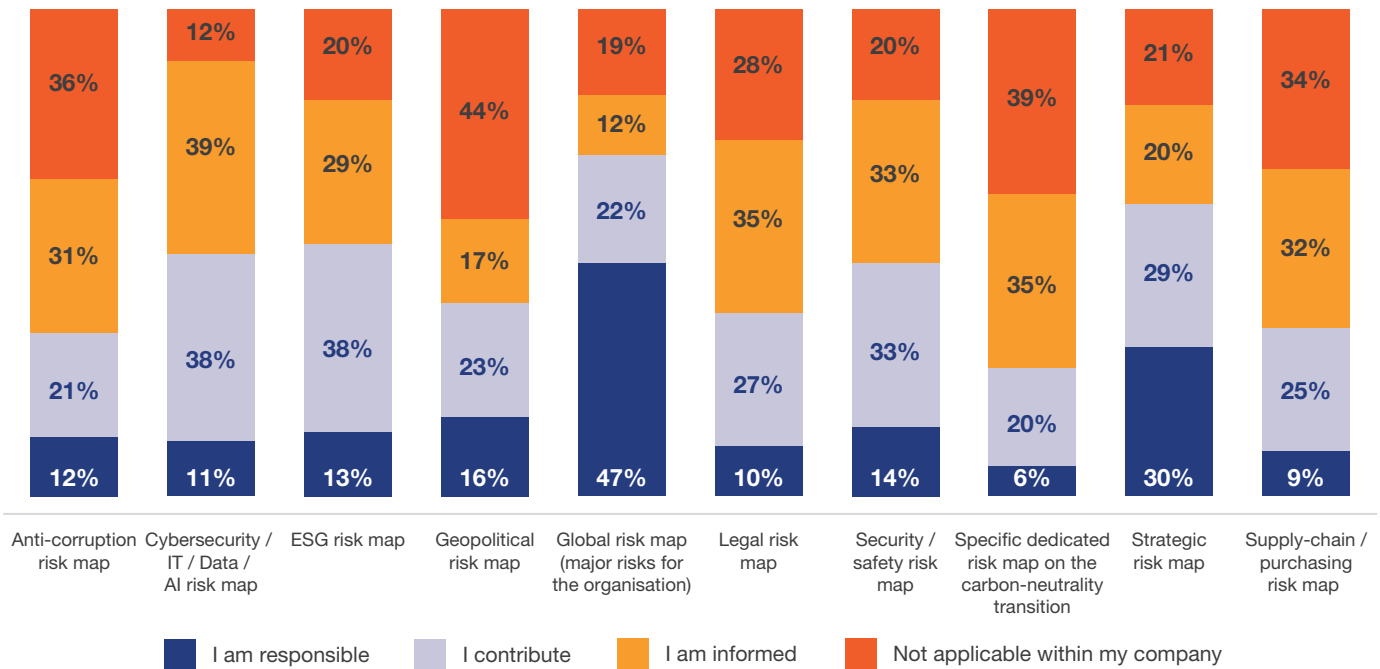


Risk Managers remain broadly engaged across the organisation and expand their role

The 2026 survey underscores the broad contribution of Risk Managers, notably in risk mapping exercises:

- Around 2/3 of respondents are heavily involved in global and strategic risk maps
- Around 50% are either responsible for or contributing to ESG, cyber / IT / data / AI, or security risk maps
- 1/3 to the anti-corruption, geopolitical, supply-chain, or legal ones
- 1/4 to the carbon-neutrality transition risk map

Risk Managers’ level of involvement in different risk maps



41% of Risk Managers are invited to, and participate in, **Board, Executive and Audit committees.** They mainly report to CFO (25%), CEO (19%) or directly to the Board (20%).

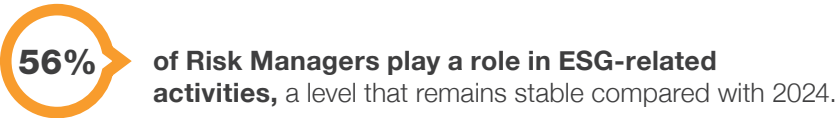
92% of Risk Managers are **involved in corporate strategy**, stable compared with 2024. Strategic risk response, operational resilience, sustainability risks, geopolitical and business impacts analysis (value chain models) and unveiling opportunities are **key focus areas of corporate strategy** in 2026.

In 2026, risk assessment remains a **short term priority** for Risk Managers, however it is now on a equal footing with risk mitigation and resilience, closely followed by risk culture and risk governance. Risk identification, evaluation and monitoring remain **core ERM responsibilities**, but Risk Managers complete the process with risk quantification, risk training and culture initiatives to support the development of risk maturity across organisations. **They are not only assessing risks, but also integrating, quantifying and governing them.**

Key findings

🎯 Risk Managers strengthen ESG governance amid mixed ESG progress

Risk Managers’ ESG involvement remains stable, while their role in structuring ESG risk governance is expanding



1/4 of those involved in ESG play a central role, being fully responsible for mapping ESG risks, defining the risk-related framework and reporting ESG risks to the Board, compared with around 20% in 2024.

Almost 1/2 make at least some contribution to these activities, as well as to double materiality assessments, CSR reporting, the development of climate-change mitigation and adaptation measures, scenario definition and analysis, and the integration of ESG risks into corporate strategy.

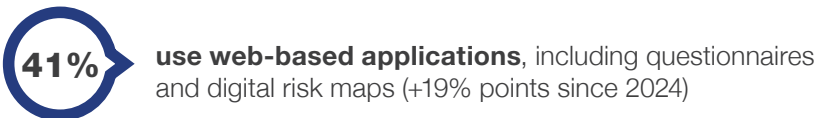
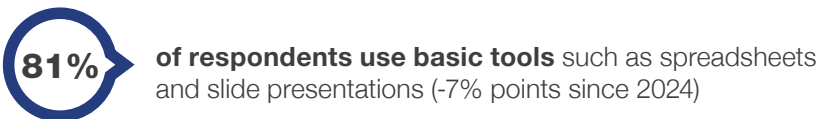
This confirms the pivotal role of Risk Managers in bringing the methodology, framework and consistency required to identify, assess, map and report ESG risks across the organisation. Nevertheless, quantifying sustainability risks remains the main challenge in 2026.

Climate-change practices are improving, while progress on Social aspects of ESG appears to be slowing



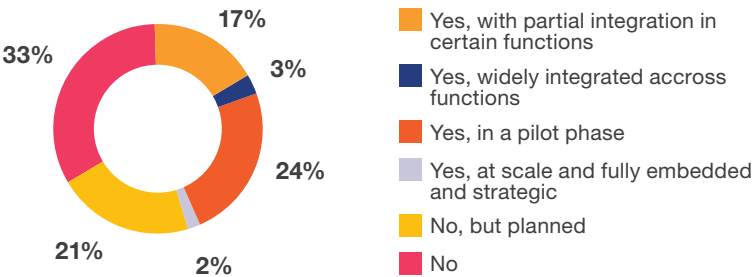
🎯 Technology use expands across ERM, while AI adoption gains momentum

Use of technology in risk management activities



Generative AI use has increased
(+7% points since 2024), confirming the growing role of AI, although the use of other AI technologies slightly decreased (by 3%)

Do you use AI for risk management?



2/3 of respondents are either **using or planning to use AI for risk management**, with 34% applying it to operational risk management, notably for process automation and anomaly detection.

The adoption of technology in ERM continues to be constrained by high investment requirements (47% cited cost as a top adoption constraint vs 50% in 2024).

Managing Artificial Intelligence as a transversal organisational risk



AI now appears across multiple dimensions of the risk agenda: among the top short- and long-term risks, among the risks considered least adequately managed, and across areas such as technology adoption, governance and operational resilience.

This confirms the emergence of AI as a transversal organisational risk, requiring a more integrated response across risk management, technology, governance, compliance and resilience frameworks.

Key findings

Insurance strategies adapt as market pressure persists

Over the past 12 months

Insurance market conditions remained challenging in 2025, influenced by broader economic trends, regulatory changes and the evolving risk landscape. The most impactful trends observed in the past 12 months were:

- 1 | the increase in premium
- 2 | the exclusion of specific risks
- 3 | wording changes (new in the top three this year)

In response, Insurance Managers adjusted their insurance strategies through four main levers:

- **Changing insurance buying patterns** — cited by 43% of respondents
- **Buying higher limits** — cited by 36% of respondents, entering the top strategies this year
- **Negotiating long-term agreements or roll-overs** — cited by 34% of respondents
- **Strengthening loss prevention activities** — cited by 31% of respondents, as a strategy to remain attractive to insurers and anticipate further market hardening

Overall, the findings show that Insurance Managers continue to use similar strategic levers as in 2024, while placing greater emphasis on long-term stability, adequate coverage and alternative approaches to managing risk financing.

Natural catastrophe coverage remains under pressure, with **24% of Risk Managers reporting a reduction in coverage in 2025**. However, **13% observed an increase in coverage for the same line**. Political risks remain the least covered line, with **27% of respondents indicating that no coverage is available**.

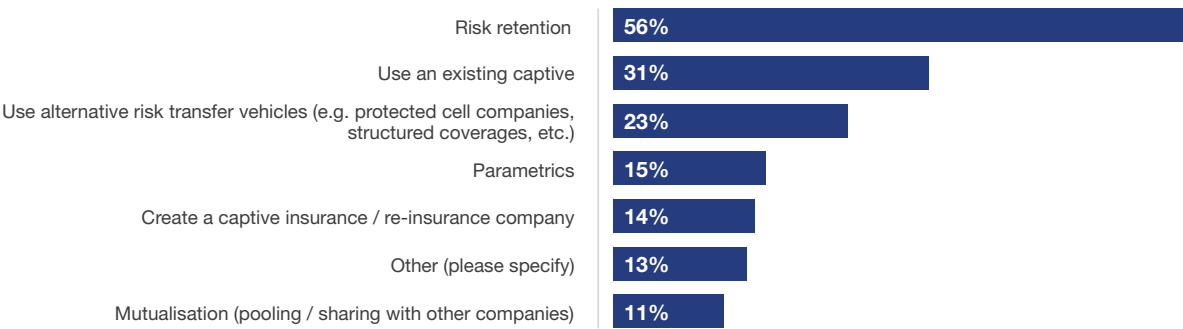
27%

A smaller proportion - 27% - of respondents report that they have been using a captive or similar vehicle (vs 37% in 2024), with a further 9% (vs 10% in 2024) saying they were considering implementing this risk transfer solution.

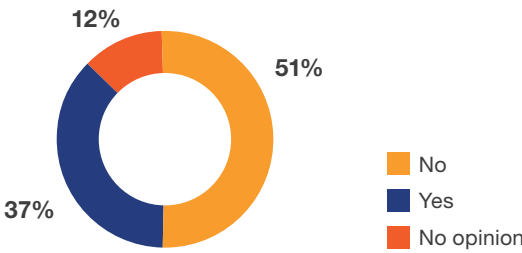
Over the next two years

Risk retention remains the primary strategy at **56%** in 2026 (62% in 2024), closely followed by the **use of an existing captive** (31% vs 35% in 2024), or an **alternative risk transfer vehicle** (23% vs 28% in 2024).

Planned risk financing strategies



Do you think some of the risks will become "uninsurable" in the future ?

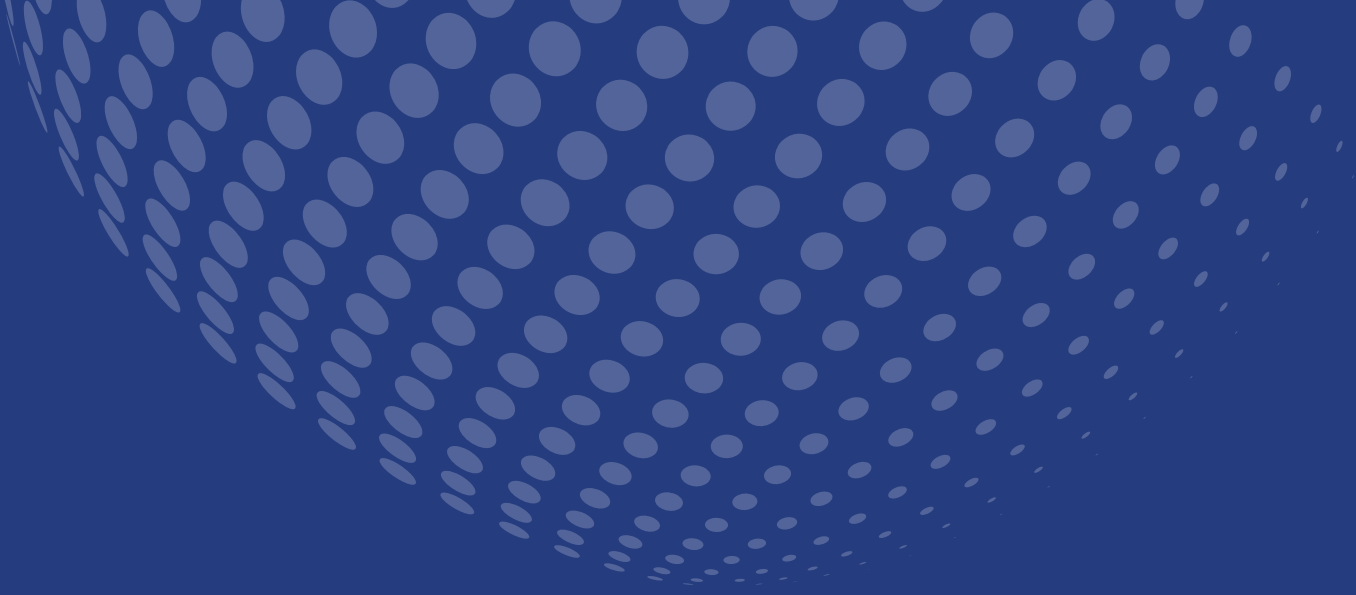


Insurance Managers appear to be more optimistic with **37%** thinking the risks of their business activities or locations will become uninsurable in the near future, compared with **53%** in 2024.



From reacting to shaping

Compared with the previous survey, one clear message emerges: Risk Managers are progressively shifting from reacting to crises towards shaping organisational resilience. While geopolitical instability, cyber threats and AI dominate today's agenda, organisations are simultaneously investing in stronger governance, improved quantification, closer integration with strategy and alternative approaches to risk financing. Rather than replacing traditional risks, new uncertainties are expanding the role of the Risk Manager: from technical specialist to strategic partner helping organisations navigate an increasingly interconnected world.

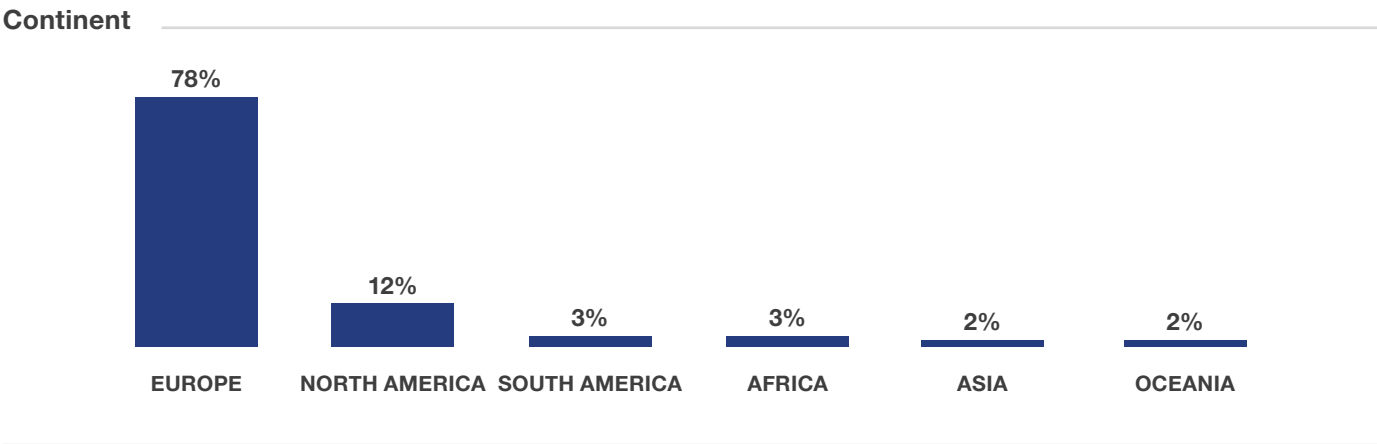


Methodology and survey respondents

Methodology

The data presented in this report were collected through an anonymous web-based survey distributed via FERMA's member associations, risk management associations in other regions, and the PwC global network between January and April 2026.

As in 2024, the survey was conducted globally, whereas it was previously distributed only in Europe. In 2026, responses were gathered from **1,329 respondents across 79 countries**, representing a **28%** increase compared with 2024, when 1,041 respondents from 77 countries completed the survey.



The analysis of the results is conducted at the global level to provide a comprehensive view of overall trends and insights; however, responses remain largely concentrated among European Risk Managers (**78%**). The comparatively lower number of respondents from other regions, including Africa, South America, Asia and Oceania, limits the ability to draw robust conclusions by geography.



Differences between continents are therefore presented in dedicated inserts, to distinguish global results, which are mainly driven by Europe, from observations specific to other regions.

The survey included 48 questions divided into nine categories:

1. Your profile (3 questions)
2. Your organisation (3 questions)
3. Your perimeter (5 questions)
4. The strategic position of the Risk Manager within the organisation (8 questions)
5. Your vision of threats/ risks (3 questions)
6. Insurance Management: market trends, coverage evolution, and risk financing (9 questions)
7. Sustainability: assessment and management of ESG risks (5 questions)
8. Digital technologies and Artificial Intelligence in Risk Management (6 questions)
9. ERM maturity model - optional section (6 questions)

Some questions were triggered by responses to previous questions. As a result, the number of respondents may vary from one question to another. In addition, some questions were optional, which also explains variations in the number of responses by question.

Specific survey questions were tailored to each profile — Enterprise Risk Manager (ERM) and Insurance Manager (IM) — to provide insights into their respective risk management activities.

The report includes a detailed profile of survey respondents, a summary of how Risk Managers perceived risks in 2026 in an uncertain geopolitical and economic environment, and an analysis of responses to the question categories.

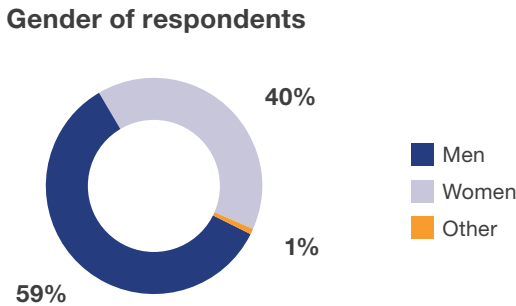
To accompany the report, we have produced 11 files summarising the data per country, continent, or group of countries. The distribution of countries within these files is as below:

- **One file per continent except Europe:** North America (154), South America (34), Africa (32), Asia (25), Oceania (22)
- **Western Europe (292):** France (58), Germany (56), Switzerland (53), Belgium (52), Netherlands (39), Luxembourg (13), United Kingdom (12), Andorra (4), Austria (3), and Ireland (2)
- **Northern Europe (178):** Sweden (65), Finland (46), Norway (26), Lithuania (19), Denmark (18) and Latvia (4)
- **Spain (143)**
- **Turkey (124)**
- **Central, Eastern and Mediterranean Europe (114):** Greece (52), Malta (25), Portugal (11), Bulgaria (6), Albania (4), Romania (4), Cyprus (3), Poland (3), Azerbaijan (2), Kosovo (2), Czech Republic (1) and Slovenia (1)
- **Italy (104)**

Profile of survey respondents

Gender and age diversity continue to improve

The gender distribution among Risk Managers continues to evolve, with the proportion of women increasing steadily over successive survey editions. In 2026, women represented 40% of respondents, up from 36% in 2024 and 32% in 2022.

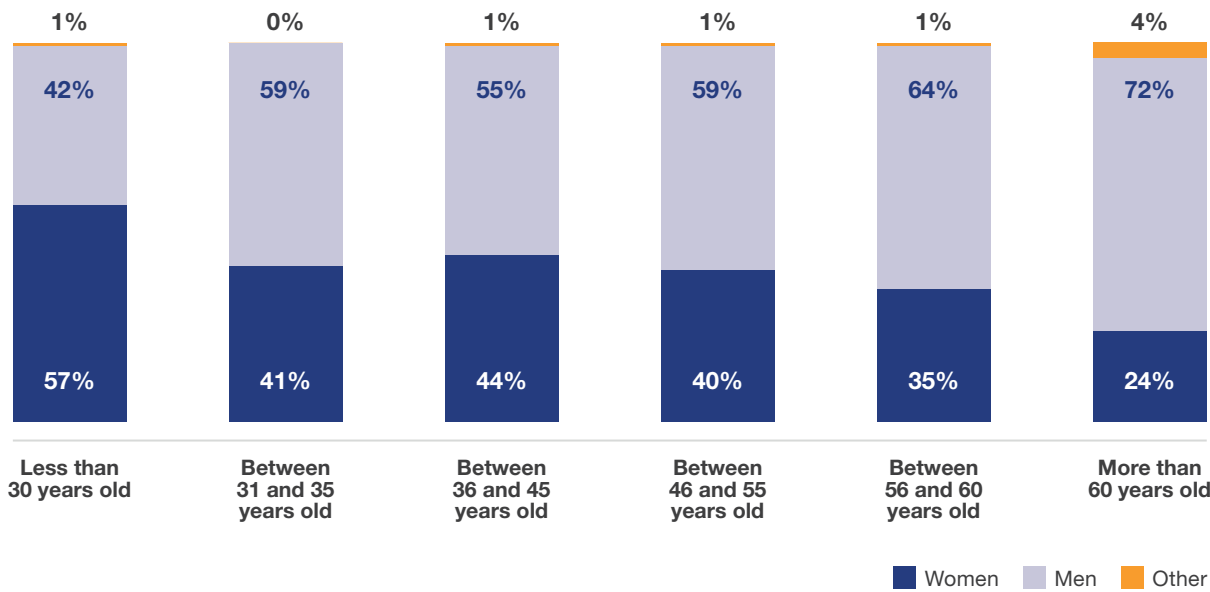


Women remain less represented in certain geographic areas. For example, they account for only 20% of Risk Managers in Asia and 38% in Europe. Other regions show a more balanced distribution, with women representing 53% of Risk Managers in Africa, 50% in Oceania, 44% in North America and 41% in South America.

The proportion of women in the profession continues to rise, with the strongest increases observed among respondents aged 36 to 45 (+5 percentage points versus 2024), 31 to 35 (+4 percentage points), and under 30 (+5 percentage points).

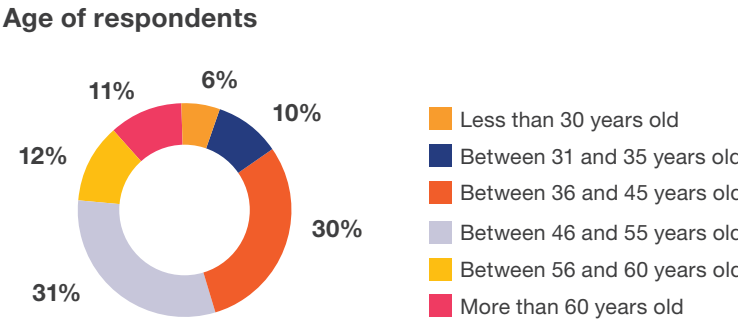
This points to a generational shift in gender distribution, with younger age groups showing a stronger trend towards gender balance.

Gender repartition by age range



The profession remains characterised by experienced professionals, reflecting both the seniority of the role and the level of expertise expected from Risk Managers.

In 2026, a majority of risk management professionals had substantial experience, with 61% of respondents aged between 36 and 55, broadly stable compared with 2024 (62%). However, Risk Managers under the age of 36 now represent 16% of respondents, an increase of 3 percentage points compared with 2024.



As in 2024, participants from Asia, Africa and South America tend to be younger overall: 24% of Asian respondents are under 36 years of age, while 36% from South America and 23% from Africa also fall in this age bracket.

Both Europe (64%) and North America (54%) have the majority of respondents in the age group between 36 and 55 years.

Professional experience

The profession remains suited to experienced profiles, only 15% (13% in 2024) of respondents having less than 3 years' experience.

More than half of respondents have over 10 years of experience, increasing to 57% in 2026 from 53% in 2024. A further 14% report between four and six years of experience, while another 14% have between seven and ten years' experience, both down from 17% in 2024.

By profile, Insurance Managers show the highest level of experience, with 73% reporting more than 10 years of experience. Combined ERM/IM profiles are also highly experienced, at 66%, while 49% of Enterprise Risk Managers report more than 10 years of experience.



Experience levels vary significantly by region. Asia and Africa have a higher proportion of respondents with fewer than three years of experience, at 22% and 28% respectively. Conversely, several regions exceed the global average for respondents with more than ten years of experience, including Oceania (64%), South America (65%) and North America (68%).

Profile of survey respondents

Organisation and sector

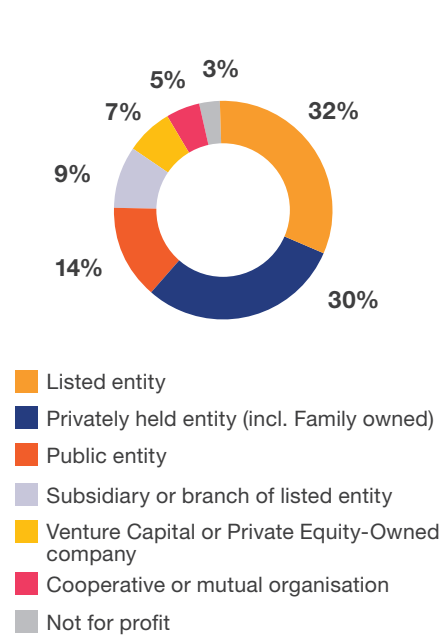
High representation of listed or privately-owned entities

As in previous editions, respondents are mainly Risk or Insurance Managers from large organisations (78% in both 2026 and 2024) and from listed or privately held organisations (62% in 2026 vs 71% in 2024). In small and mid-sized organisations, risk management responsibilities may be covered by other functions, such as Finance or Legal.



Small organisations are more prevalent among respondents from South America (29%), Africa (28%) and Asia (24%), but are only marginally represented in Oceania (5%), where public entities predominate (36%). In North America, privately held and listed entities account for 50% of respondents, while public entities represent 29%. Africa has the highest proportion of venture capital or private equity-owned companies, at 19%.

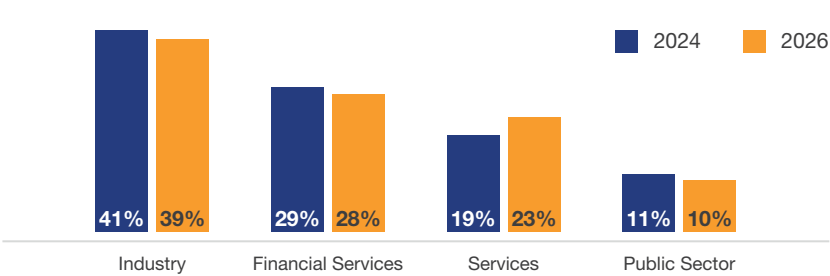
Distribution of respondents by type of organisations



A similar spread of sector of activity within the respondents

- **Industry** remains the largest sector represented, accounting for 39% of respondents, stable compared with the 2024 survey.
- **Financial services** follows closely, representing 28% of respondents, also stable compared with 2024. This category includes insurance, which accounts for 13% of total respondents, and banking, at 8%.
- **Services** accounts for 23% of respondents, up from 19% in 2024, covering areas such as professional and business services, technology, retail, tourism, media, healthcare and private education.
- The **public sector** represents 10% of respondents, including government entities, infrastructure, public services, regulators and non-profit organisations.

Distribution by sector of activity



This global distribution is largely driven by Europe, while other regions show more pronounced differences from the global average. In Africa, respondents are mainly from Financial Services and Services, each representing 36%. In Asia, there are no respondents from the public sector, while Industry and Services each account for 38%. South America is most strongly represented by Industry, at 50%. In Oceania, the public sector is the largest group, at 44%. North America shows the most balanced distribution across sectors.

Type of profiles and teams

This year shows a stable representation of the three profiles compared with 2024

48%

Enterprise Risk Management (ERM) profile: oriented towards overall risk management of the organisation, to identify, analyse, treat, and reduce business risks.

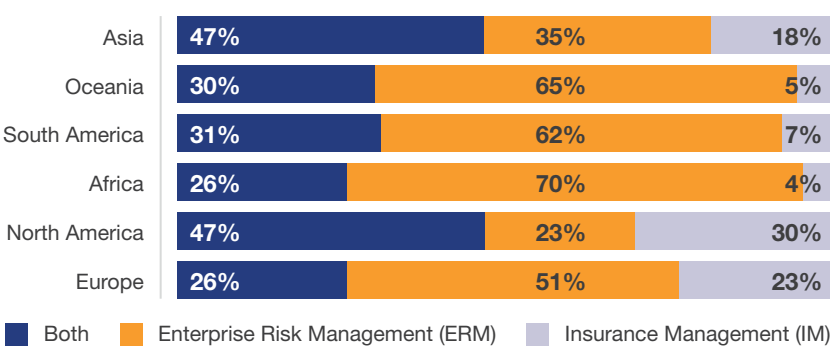
22%

Insurance Management (IM) profile: oriented towards insurable risks, including loss prevention and risk transfer.

30%

Mixed ERM / IM profiles work on insurance, loss prevention and wider risk management issues.

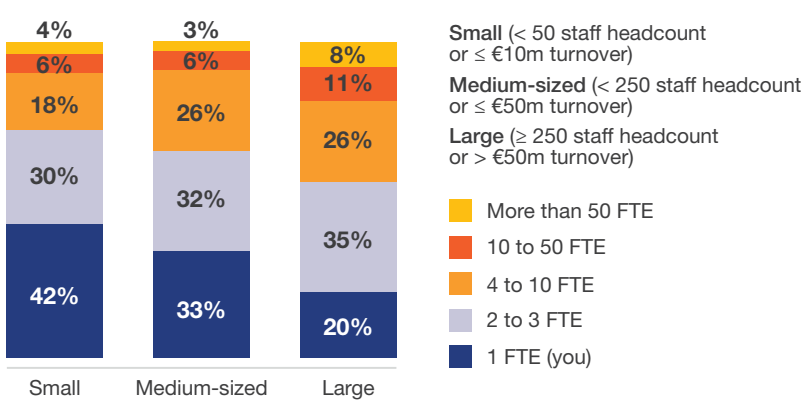
Type of profiles by continent



In North America and Asia, nearly half of respondents (47%) combine ERM and IM responsibilities, suggesting a strong integration of insurance management within broader risk management practices. By contrast, respondents in Oceania, South America and Africa are more predominantly ERM-oriented, with fewer dedicated IM profiles represented.

Risk management teams are typically composed of two to three full-time equivalents (FTEs), representing 36% of respondents. This is closely followed by teams of either one FTE or four to ten FTEs, each representing 24% of respondents. Team size varies significantly depending on the size of the organisation, as shown in the graph below.

Number of FTE by organisation size



Asia and South America report the highest proportions of teams with more than 10 FTEs, at 28% and 24% respectively, and also show highest proportions of teams with more than 4 FTEs, at 51% and 57%. Asia also has the highest proportion of one-person departments, at 31%.

ERM teams are broadly aligned with the global distribution. **Insurance Management teams** tend to be larger, with only 19% reporting one FTE, 36% reporting two to three FTEs, 25% reporting four to ten FTEs, 13% reporting 10 to 50 FTEs, and 6% reporting more than 50 FTEs.

By contrast, **combined ERM/IM teams** tend to be smaller, with 31% reporting one FTE, 38% reporting two to three FTEs, and only 10% reporting more than 10 FTEs.

Financial Services have the largest risk management teams among large companies, with 39% reporting more than 10 FTEs, compared with between 8% and 15% in other sectors.

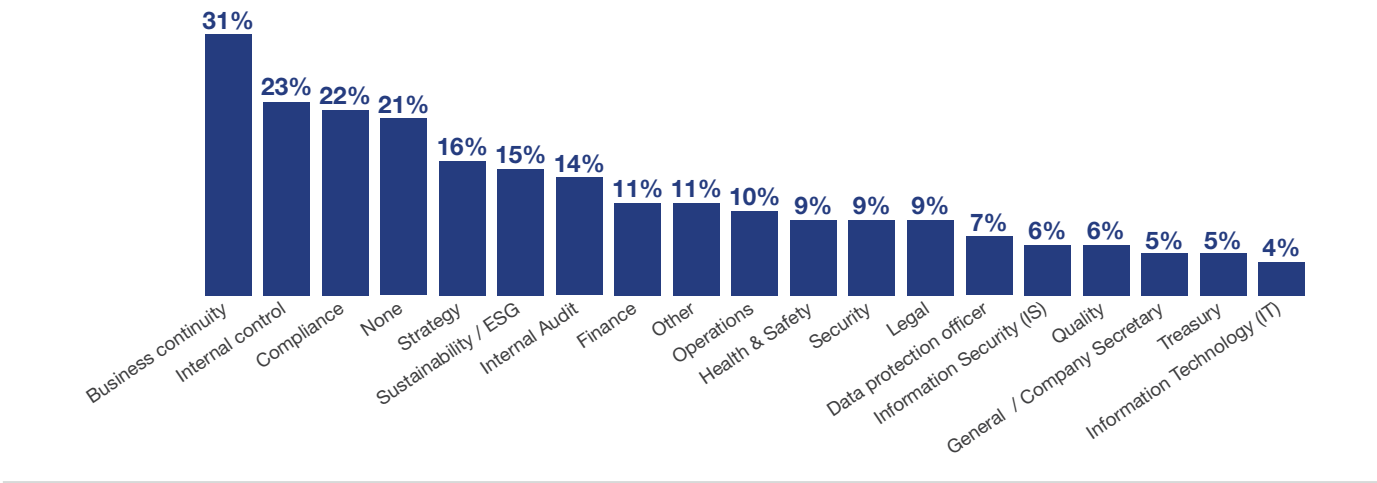
These percentages remained relatively stable compared with the 2024 survey.

Profile of survey respondents

Risk Managers’ other responsibilities

A large majority of respondents (79%) have responsibilities beyond ERM/IM, compared with 72% in 2024 and 60% in 2022. This highlights the breadth of Risk Managers’ scope and their ability to apply a risk-based approach more widely across their organisations.

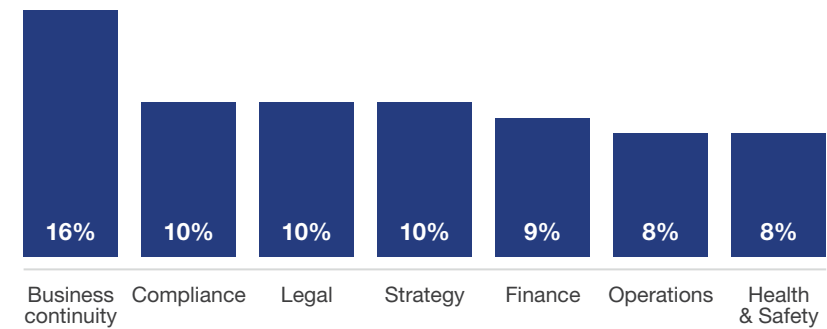
Other activities within all respondents’ scope of responsibilities



Among the main additional responsibilities, **business continuity**, **internal control** and **compliance** remain key areas for Risk Managers, consistent with 2024. The most notable increase concerns **sustainability/ESG**, which rose from 1% in 2024 — one of the lowest-ranked activities — to 15% in 2026, reaching fifth position. This suggests that ESG considerations are increasingly becoming part of Risk Managers’ remit and reflects the broader integration of sustainability and ethical considerations into risk management frameworks, alongside more traditional activities.

Strategy also remains within the responsibilities of 16% of Risk Managers, confirming the continued link between strategic planning and risk management activities.

Focus on Insurance Managers’ other responsibilities in scope



In observing differences between ERM and IM profiles, it appears **Finance** and **Legal** responsibilities are predominant for IM profiles rather than **Internal Audit and Control**, that tend to be more in the scope of ERM functions.

Despite rising geopolitical tensions, these figures remain stable. This may appear counterintuitive, as Business Continuity is increasingly exposed to geopolitical disruption and Compliance remains critical in a more complex and demanding regulatory environment.

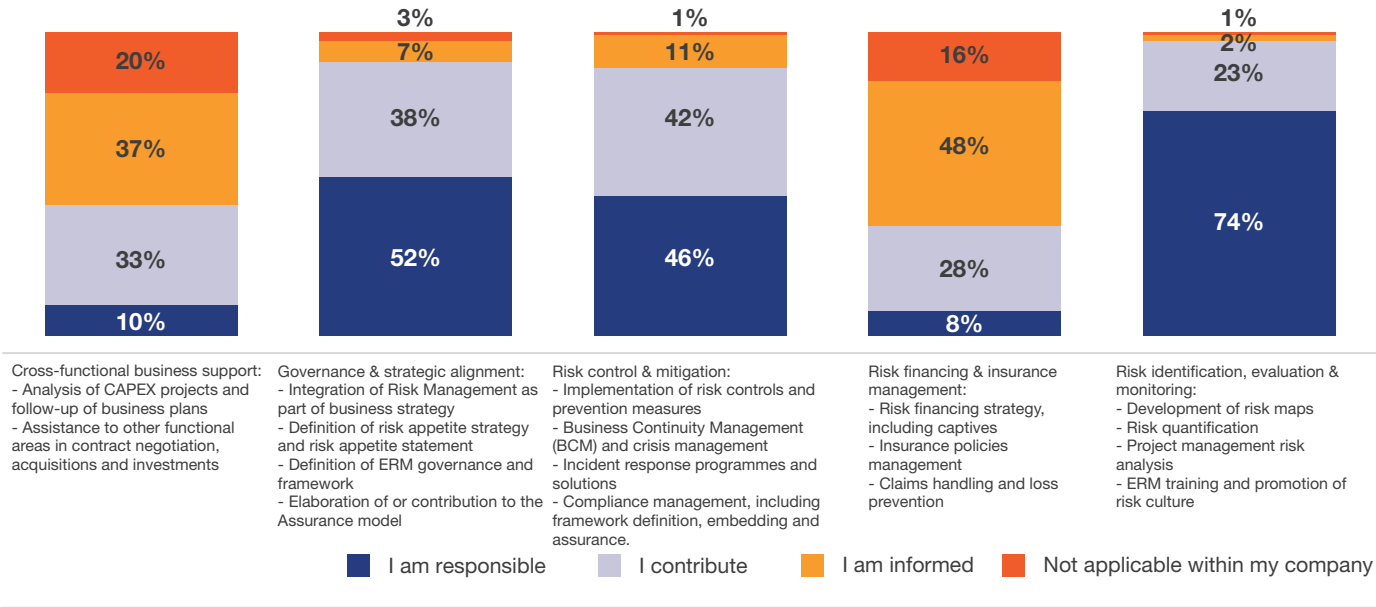


Across all regions, Business Continuity and Compliance remain key areas of focus for this year’s respondents. In North America, Health & Safety is the second most frequently cited additional responsibility, reported by 24% of respondents.

Risk Managers’ activities by type of profile

The global results show that risk identification, evaluation and monitoring is the main activity performed by respondents, with 57% being responsible for it and 30% contributing. Risk control and mitigation ranks second, with 85% of respondents either responsible for or contributing to it, closely followed by governance and strategic alignment, at 80%.

Focus on ERM profile activities



Risk identification, evaluation and monitoring is the activity most clearly owned by ERM in 2026, with 74% of respondents responsible for and 23% contributing to it. Compared with 2024, when risk mapping led at 63%, training and culture followed at 60%, and risk quantification entered the top three at 45%, the 2026 results suggest these activities are converging into a core ERM mandate. Risk quantification has therefore moved from an emerging capability to a more central responsibility, with ERM teams expected to translate identified risks into measurable outputs such as risk scores, heatmaps, scenarios, exposure estimates and prioritised action plans.

Governance and strategic alignment is the second most frequently owned activity, with 52% of respondents responsible for and 38% contributing to it. This is broadly consistent with both the global results and the 2024 findings, when ERM governance also stood at 52% and alignment with strategy at 42%. The 2026 results reinforce the strategic role of ERM profiles, with quantified risk insights increasingly used to calibrate risk appetite, support strategic decision making and inform discussions on acceptable exposure levels.

Risk control and mitigation also remains a significant ERM responsibility, with 46% of respondents responsible for and 42% contributing to it, up from 31% direct ownership of controls and prevention in 2024. This suggests stronger ERM involvement in translating quantified risks into mitigation actions, control frameworks and follow-up

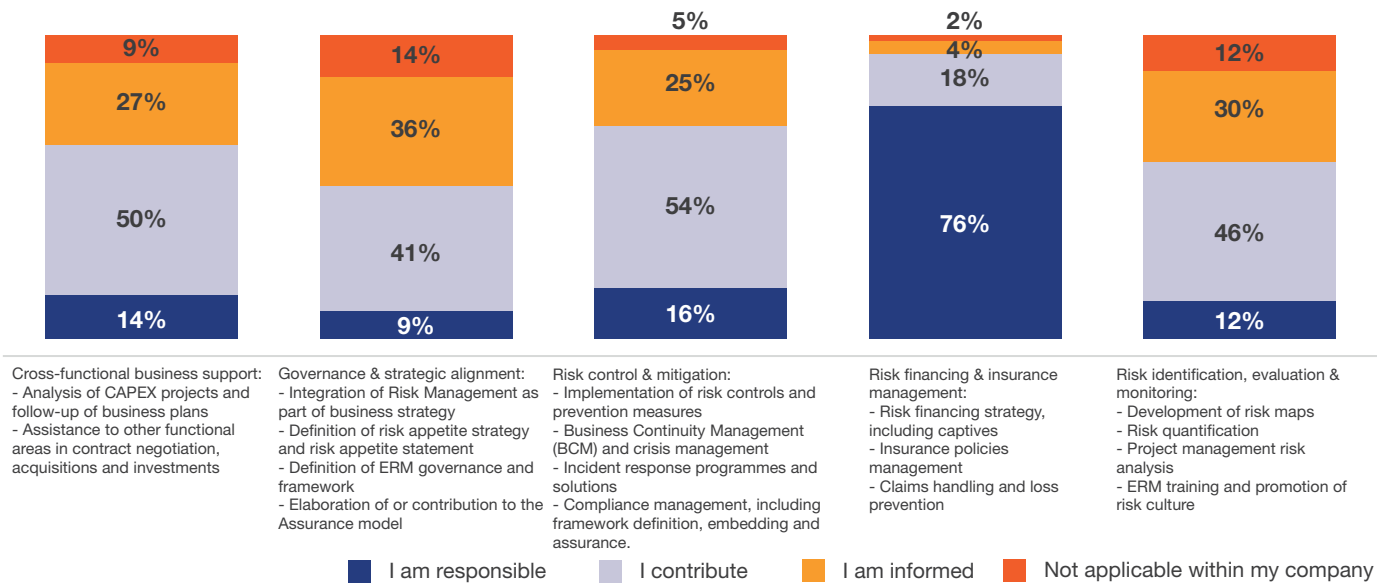
processes. The balanced split between responsibility and contribution also reflects the cross-functional nature of mitigation, where business units often own controls while ERM provides methodology, prioritisation, monitoring and assurance.

By contrast, **cross-functional business support** and **risk financing and insurance management** are less frequently owned by ERM profiles. For cross-functional business support, only 10% of respondents are responsible, while 33% contribute and 20% consider it not applicable. Only 8% of respondents said they are responsible for risk financing and insurance management, compared with 28% who contribute to it and 16% who consider it not applicable. These areas therefore remain mainly advisory or informational for ERM, although they offer opportunities to apply quantified risk analysis to investment decisions, project assumptions, insurance coverage, retention levels and the trade-off between mitigation, transfer and risk acceptance.

Overall, ERM ownership is strongest where risks are identified, assessed, quantified and embedded into governance. Compared with 2024, risk quantification has moved further into the core ERM agenda, governance remains stable and strategically important, and risk control shows increased ERM involvement. This reinforces ERM’s central value in 2026: **quantifying, prioritising and translating risk into decisions on governance, mitigation and financing.**

Profile of survey respondents

Focus on IM profile activities



In 2026, **risk financing and insurance management** remains the core responsibility of Insurance Managers, with 76% responsible for and 18% contributing to it. This is consistent with 2024, when insurance policy management, claims handling and loss prevention were the leading activities, at 78%. This reflects the central role of Insurance Managers in translating risk exposures into financing decisions, including insurance limits, deductibles, retentions and the balance between risk transfer and retention.

Beyond this core mandate, Insurance Managers play a contributing role. Their involvement in **risk control and mitigation** has increased, with 16% responsible for and 54% contributing to it, up from 7% and 42% in 2024. This suggests greater use of loss and exposure data to support prevention efforts. **Cross-functional business support** remains largely advisory, with 14% responsible and 50% contributing, broadly in line with 2024 (12% and 49%), particularly in contract negotiation, projects, acquisitions and investments.

An increased proportion - 12% - of Insurance Managers said they were responsible for **risk identification, evaluation and monitoring**, while 46% said they contribute to it. This compares with 2024, when risk quantification was mainly a contributory activity (53%) and only 9% reported full ownership. **Governance and strategic alignment** is also less frequently owned, with 9% responsible, 41% contributing and 36% informed.

Overall, the 2026 results show the complementary roles of Insurance Managers and Enterprise Risk Managers: **Insurance Managers own risk financing and insurance management**, while contributing to mitigation, business support and risk quantification. Compared with 2024, their core insurance mandate remains stable, while their involvement in prevention and quantified risk decision-making appears to be increasing.



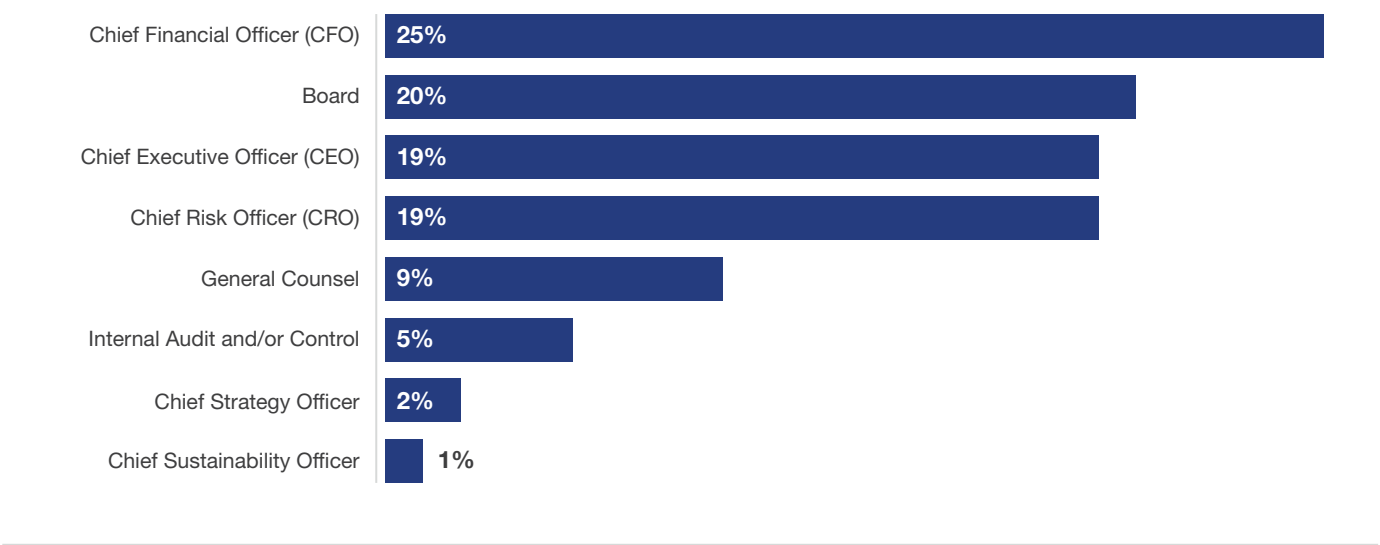
The findings are broadly aligned with global trends across regions. However, Africa, Asia and South America show a higher proportion of respondents for whom cross-functional business support is not applicable, at 41%, 29% and 31% respectively, compared with 15% globally. For ERM profiles, the main activities remain broadly consistent, although regional differences are visible in the balance between responsibility and contribution. North America and Oceania show stronger ownership of governance and strategic alignment, while North America and South America show lower direct responsibility for risk control and mitigation. This suggests that the maturity and mandate of ERM functions continue to vary by region.

Reporting lines

Reporting lines remain stable across all profile types

Insurance Managers and Enterprise Risk Managers show distinct reporting patterns. Insurance Managers are more likely to report directly to the CFO, with 47% doing so, while only 8% report to the Board. By contrast, Enterprise Risk Managers tend to have more direct links with governance bodies and senior leadership, reporting more frequently to the Board (25%) or the CEO (21%) than to the CFO (13%). Another notable difference is the reporting line to General Counsel, which applies to 17% of Insurance Managers compared with only 3% of Enterprise Risk Managers.

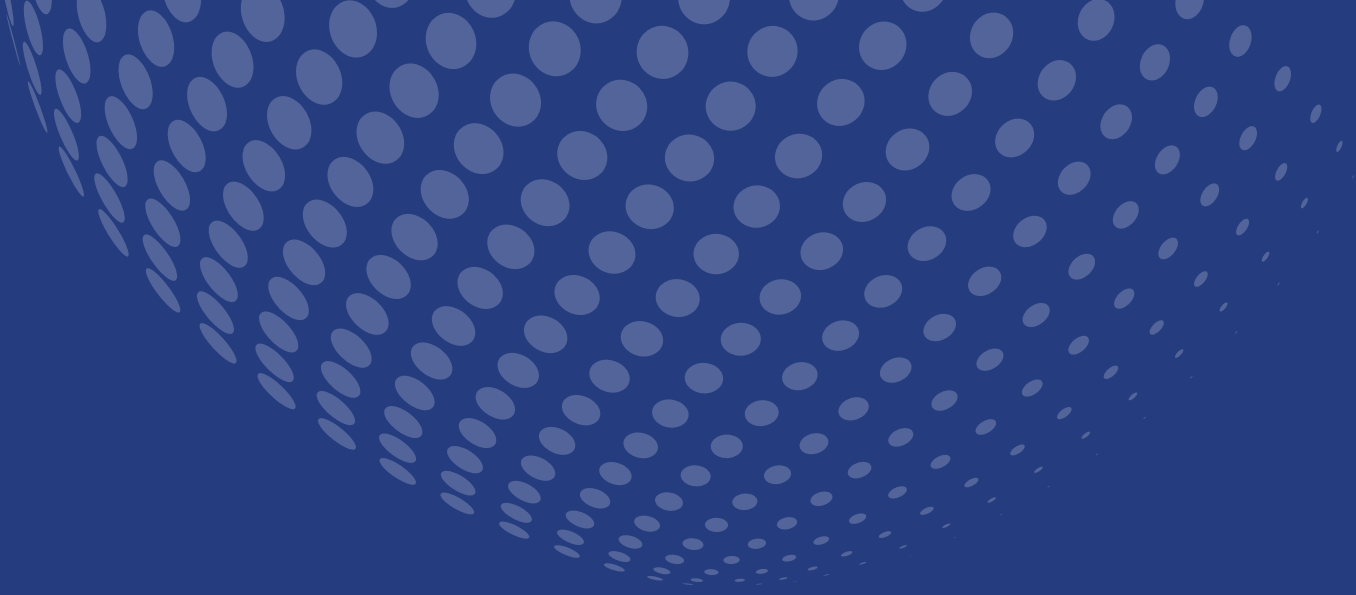
Reporting lines of respondents



Only a small proportion of respondents report to Internal Audit and/or Internal Control (5% in 2026, compared with 6% in 2024), suggesting a clear separation between these functions and the risk management function. A small share of Risk Managers reports to the Chief Strategy Officer (2% in 2026, compared with 3% in 2024). This remains marginal as direct reporting into strategy functions is not a common model, even though Risk Managers increasingly contribute to strategy execution and the alignment of risk management with business objectives.



In Africa and Asia, respondents mainly report to the CEO (40% and 54%, respectively) or to the Board (20% and 23%, respectively). In South America, respondents are more likely to report to assurance functions, either the CRO (35%) or Internal Audit and Control (24%), than to the Board (18%).



**Risks priorities shift
across time horizons,
in an interconnected
risk landscape shaped
by volatility and AI**

Top critical threats to the organisation within the next 12 months

Our survey asked respondents to rank the main threats to their organisation’s growth prospects across different time horizons. The findings show that risk priorities are no longer static: they evolve over time horizons and are increasingly shaped by interconnected risks.

The 2026 report highlights an increasingly complex and interconnected risk landscape, with geopolitical uncertainty, cyber risk and economic volatility remaining top concerns. At the same time, AI is rapidly emerging as a strategic risk, reshaping governance, compliance, cybersecurity and competitiveness.

These findings underscore that disruption is now a constant. As short-term pressures converge with longer-term challenges, organisations must strengthen resilience and further embed risk into strategic decision-making.

The 2026 survey results show both continuity and change in the Top 5 short-term risk landscape

Top 5 risks in 2022

- Cyber threats
- Supply chain or distribution failure
- Geopolitical uncertainties
- Uncertain economic growth
- Over-regulation

Top 5 risks in 2024

- Cyber-attacks
- Geopolitical uncertainties
- Uncertain economic environment
- Talent management
- Data breach

Top 5 risks in 2026

- Geopolitical uncertainty
- Cyber-attacks
- Uncertain economic growth
- Artificial Intelligence use
- Regulation

Geopolitical uncertainty, cyber-attacks and uncertain economic growth remain the three most critical threats, although **geopolitical uncertainty** has moved into first place. This reflects the continued impact of global instability, armed conflicts, tensions between major powers, sanctions, trade restrictions and regulatory shifts, all of which affect business continuity, supply chains, market access and strategic planning.

Cyber-attacks remains a prominent threat, ranking second, as organisations continue to face ransomware, data breaches, third-party vulnerabilities, state-sponsored attacks and increasingly sophisticated AI-enabled cybercrime. **Uncertain economic growth** ranks third, driven by inflationary pressures, interest-rate volatility, uneven growth prospects and market instability, with direct implications for investment, cost management and long-term planning.

AI use represents the most notable upward movement in 2026, now ranking fourth among the top threats. Its rise reflects its growing role as a transversal risk, combining opportunities for innovation and efficiency with challenges related to governance, ethics, data protection, cyber exposure, regulatory compliance and accountability. **Regulation** complete the top five, as organisations navigate increasingly complex and divergent requirements across cyber resilience, data protection, AI, sanctions, sustainability and corporate governance.

Overall, the 2026 results point to a reprioritisation of risks, with greater emphasis on external uncertainty, technological disruption and regulatory complexity. Compared with 2024, **talent management** and **data breach** no longer appear in the top five, while **AI use** and **regulation** have entered the ranking. This shift suggests that organisations are increasingly focused on external volatility, digital transformation and compliance pressure as key determinants of resilience and long-term viability.

Geopolitical uncertainty and cyber-attacks rank among the top five risks across all sectors. Uncertain economic growth also features in the top five in every sector except the public sector, while **AI use** and **Regulation** appear in all sectors except Industry, where they rank seventh and sixth respectively.

Financial Services presents a risk profile broadly consistent with the global ranking, confirming the sector’s exposure to the same major external and technological pressures. However, the order of priorities differs slightly: AI use ranks third, ahead of Regulation and Uncertain economic growth. This suggests that Financial Services organisations are particularly focused on the governance, control, compliance and trust implications of AI adoption, given their high regulatory exposure, reliance on data and increasing use of automated decision-making.

In the **Public Sector**, Regulation rank as the second biggest perceived threat, while **Talent management** appears in fifth position, replacing uncertain economic growth in the top five. This points to a distinct risk profile, where public organisations are more exposed to regulatory obligations, public accountability, digital-transformation challenges and workforce constraints.

Industry differs markedly from the global ranking. In this sector, concerns are largely concentrated around **Supply chain or distribution failure** and **Trade / tariffs evolution**, while AI use and Regulation rank lower. This reflects the sector’s direct exposure to physical flows, sourcing constraints, production continuity and international trade conditions. Geopolitical uncertainty, ranked as the leading risk, acts as a key amplifier of these vulnerabilities through sanctions, trade restrictions, logistics disruption and tariff changes.

Services remains closely aligned with the global results, although the relative ranking of certain risks differs. Cyber-attacks rank ahead of geopolitical uncertainty, while AI use ranks ahead of uncertain economic growth. This indicates that Services organisations are particularly exposed to digital dependency, client data protection, technology-enabled delivery models and the need to maintain trust and continuity in highly competitive markets.



From a regional perspective, the top five risks reveal several clear patterns. North America and Europe are closely aligned with the global ranking, with the same main threats appearing in their top five. **Artificial Intelligence use** is the only risk to appear in the top five across all regions, and ranks first in both North and South America.

Cyber-attacks feature in the top five of all regions except Africa, where **Climate change adaptation** is instead identified as a leading concern. This likely reflects Africa’s high exposure to climate impacts, combined with more limited infrastructure and institutional capacity to adapt. **Natural disasters** also appear in the top five in Oceania, South America and Asia, consistent with these regions’ exposure to acute physical hazards such as floods, cyclones, droughts, wildfires, earthquakes and sea-level rise.

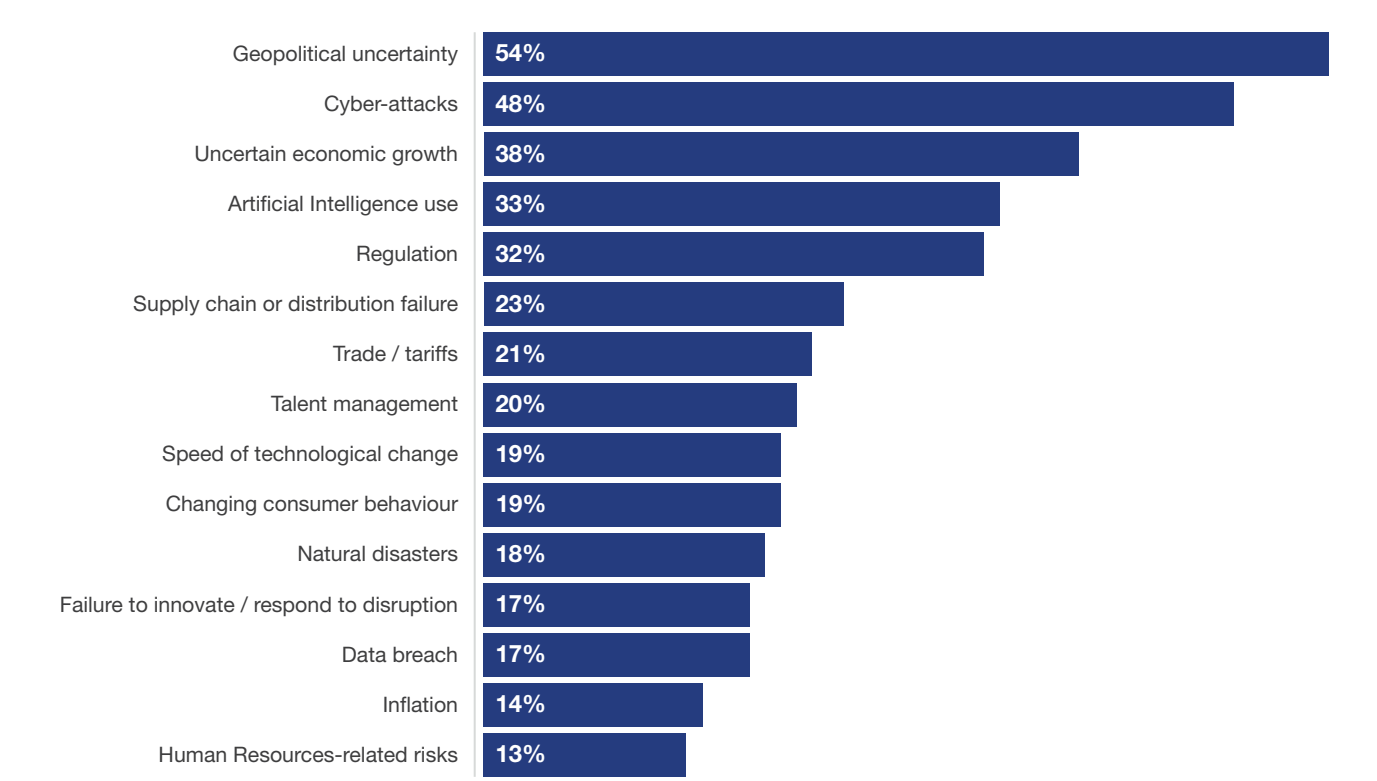
Uncertain economic growth appears in the top five in Europe, North America and Oceania, while **Regulation** rank in the top five only in Europe and North America, which may reflect more mature, complex and strongly enforced regulatory environments.

Finally, **Failure to innovate or respond to disruption** appears only in South America and Oceania, suggesting heightened concern in regions where adaptability, productivity and technological competitiveness are critical to long-term market positioning. Asia is the only region to rank **Misinformation / disinformation** in its top five, while Africa is the only region to prioritise both **Speed of technological change** and **Talent management**, pointing to specific challenges around digital transformation and workforce capabilities.

Beyond the Top 5, the 2026 ranking points to a shifting short-term agenda

Trade and tariff developments emerge as a new concern, alongside Geopolitical uncertainty as a major threat. AI and technological change move sharply upward, while Inflation, Data breach, Talent management and Fraud lose relative momentum.

Top critical risks to organisations’ growth prospects over the next 12 months



The survey highlights notable shifts in the risks expected to affect organisations over the next 12 months.

A new risk appears in the 2026 ranking: **Trade and tariffs**, which enters in 7th position. Its emergence is closely linked to geopolitical uncertainty and reflects a year in which trade measures, tariff changes and protectionist policies evolved rapidly and, in many cases, unexpectedly. Together with the top five short-term threats, this highlights that **external volatility** has become a major concern for organisations. By contrast, **Inflation**, which entered the ranking in 2024 in 6th position, has fallen to 14th, decreasing by 15 percentage points. This suggests that, while inflationary pressure has not disappeared, it is now perceived as less acute than broader geopolitical, technological and regulatory risks.

In 2026, **technological disruption** risks are becoming increasingly prominent. **Artificial Intelligence use**, referred to as generative AI use in 2024 and ranked 13th, has moved up to 4th place, recording the largest increase at 14 percentage points. By contrast, **Data breach** has fallen sharply, decreasing by 18 percentage points and moving from 5th to 13th position. Nevertheless, at 17%, **Data breach** remains a relevant threat, reflecting continued exposure to cyber-related incidents. Combined with the **Speed of technological change**, which moved from 15th to 9th position, this suggests that technology-related concerns are not declining, but are becoming more concentrated around AI adoption, governance and control.

The continued presence of **Failure to innovate**, also at 17%, further illustrates the pressure on companies to

keep pace with technological advancement in order to preserve the viability and **resilience of their business models**. Organisations are increasingly expected not only to adopt and leverage new technologies effectively, but also to do so while maintaining competitiveness, oversight and long-term control.

Talent management also remains prominent, despite decreasing by 16 percentage points and moving from 4th to 8th position in the ranking. This suggests that companies are still navigating changing workforce expectations, remote and hybrid working models, employee well-being and continued retention challenges, particularly as demand grows for technology- and AI-related capabilities. **Human Resources-related risks**, which were new in 2024 and ranked 10th, now appear at the bottom of the top 15. This may indicate that people-related risks remain important, but are increasingly being viewed through more targeted lenses such as talent retention, skills transformation and workforce adaptation rather than as a broad standalone HR risk category.

Finally, **Fraud or theft** has moved out of the top-ranked critical risks, falling from 9th to 18th position and decreasing by 20 percentage points, the largest drop in the ranking. This does not mean that fraud risk has disappeared, but rather that it is being relatively deprioritised compared with faster-moving external, technological and strategic risks that are currently reshaping organisations’ short-term agendas.



The **World Economic Forum’s (WEF) Global Risks Report** takes a macroeconomic and societal perspective, identifying risks that could affect global stability, economies, populations, and governance systems. In contrast, our **Global Risk Manager Survey** reflects the views of corporate risk managers and focuses on risks that have a direct impact on organisations’ performance, operations, and strategic objectives. As a result, while the two studies converge on certain underlying trends, they differ in their analytical lens: the WEF report primarily examines global systemic risks, whereas the Global Risk Manager Survey focuses on the business and operational risks that organisations face in practice.

A comparison between the results of the 2026 Global Risk Manager Survey and those of the WEF 2026 Global Risks Report confirms that **geopolitical uncertainty** has become a leading concern worldwide. **Misinformation and disinformation**, introduced as a new suggested risk in our 2026 survey, ranks only 16th over the short term, while it appears among the WEF report top five risks, ahead of economic downturn — a category broadly comparable to **Uncertain economic growth** in our survey. By contrast, Risk Managers place greater emphasis on **Cyber-attacks** and **AI-related risks** in the short term: cyber insecurity ranks 9th in the WEF report and adverse outcomes of AI 8th, whereas both topics are ranked higher by Risk Managers among short-term threats. Finally, **Natural disasters** are ranked 11th by Risk Managers, while they are identified as the third most critical short-term concern by WEF report’s respondents. They are also the only environmental risk to appear among the top short-term risks in both reports.

Global Risk Landscape for 2026

1	Geo-economic confrontation
2	State-based armed conflict
3	Extreme weather events
4	Societal polarization
5	Misinformation and disinformation
6	Economic downturn
7	Erosion of human rights and/or of civic freedoms
8	Adverse outcomes of AI technologies
9	Cyber insecurity
10	Inequality

■ Economic ■ Societal ■ Technological
■ Geopolitical ■ Environnemental

Source: World Economic Forum Global Risks Perception Survey 2025-2026

Top 5 critical threats to the organisation’s growth prospects within the next 3 and 10 years

AI becomes the leading medium-term risk, reshaping the three-year threat landscape.

Top 5 critical threats within the next 3 years



In 2026, medium-term threats are closely aligned with short-term concerns. Four of the top five risks are common to both horizons, with **Failure to innovate / respond to disruption** being the only medium-term risk that does not appear in the short-term top five.

This marks a significant shift compared with 2024, when the top three medium-term risks were **Regulation**, **Geopolitical uncertainty** and **Speed of technological change**, followed by **Climate change adaptation** and **Failure to innovate**. Two years later, **AI use** has become the leading medium-term risk and **Cyber-attacks** have entered the top three, while speed of technological change and climate change adaptation have moved out of the top five.

AI now concentrates several dimensions of **technological disruption**: it creates opportunities for efficiency and innovation, while raising concerns around governance, accountability, **cyber vulnerabilities**, data privacy, misinformation, **regulatory uncertainty** and opaque decision-making. Its rise confirms that organisations increasingly view AI as a multi-dimensional strategic risk, requiring clear ownership, robust oversight and continuous adaptation of operating models, governance frameworks and business models. It also reinforces the importance of innovation capabilities, as **failure to adapt / respond to disruption** (AI-driven or not) may directly affect competitiveness and long-term resilience.

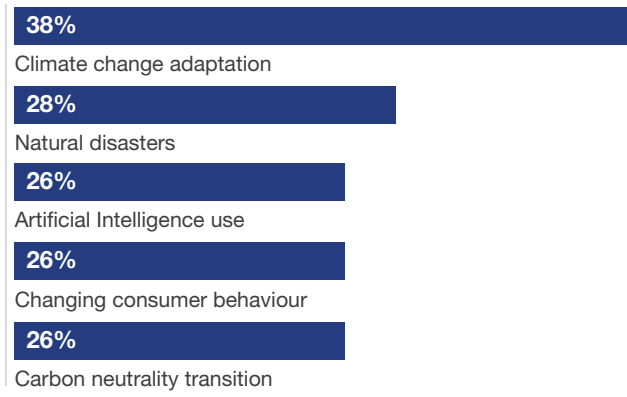
Cyber risk has also become a defining medium-term concern as digital dependency, interconnected supply chains and geopolitical tensions increase exposure. The threat landscape is evolving quickly, with ransomware, state-sponsored attacks, third-party breaches and **AI-enabled cybercrime** raising both the frequency and sophistication of incidents. For global organisations, uneven security maturity and **diverging regulatory requirements** further complicate response strategies, making cyber resilience a priority across governance, technology, crisis preparedness and business continuity, at short- and medium-term perspectives.

Geopolitical risk remains a persistent concern, even at medium-term, affecting operations, supply chains, market access and employee safety through conflicts, sanctions, trade restrictions and regulatory shifts. Its importance also lies in its role as a risk amplifier: geopolitical developments can intensify cyber threats, economic volatility, **regulatory pressure** and supply-chain disruption simultaneously. Managing this risk therefore requires continuous monitoring, scenario planning and close coordination between risk, legal, compliance, security and strategy and business teams.

By contrast, **climate change adaptation** now ranks 9th, suggesting that medium-term attention is shifting towards more immediate operational and technological pressures, even though climate-related risks remain structurally significant over the longer term.

Environmental risks continue to dominate the long-term horizon, while AI joins climate-related challenges as a structural strategic concern.

Top 5 critical threats within the next 10 years



Over a 10-year horizon, environmental risks remain the dominant long-term concerns for organisations. **Climate change adaptation** continues to rank first, increasing to **38%** of responses from **35%** in 2024, confirming the growing importance of both physical and strategic climate impacts. **Natural disasters** have moved into second place at **28%**, up from third position and **24%** in 2024, reflecting increasing concern around the frequency and severity of extreme weather events and their impact on operations, infrastructure, supply chains and business continuity. **Carbon-neutrality transition** remains a major priority

at **26%**, although it has fallen from second place in 2024 to fifth in 2026, as new long-term concerns have entered the top five.

The inclusion of **Artificial Intelligence use** in the long-term top five reflects that AI is now viewed as an immediate operational and technological issue, and as a structural strategic challenge for the decade ahead. Organisations are increasingly considering both the opportunities created by AI and the risks associated with its adoption, governance, ethics, regulation and impact on competitiveness.

Changing consumer behaviour, now in the top five after ranking sixth in 2024, also highlights the need for organisations to adapt to evolving expectations around sustainability, digitalisation, transparency, convenience and social responsibility.

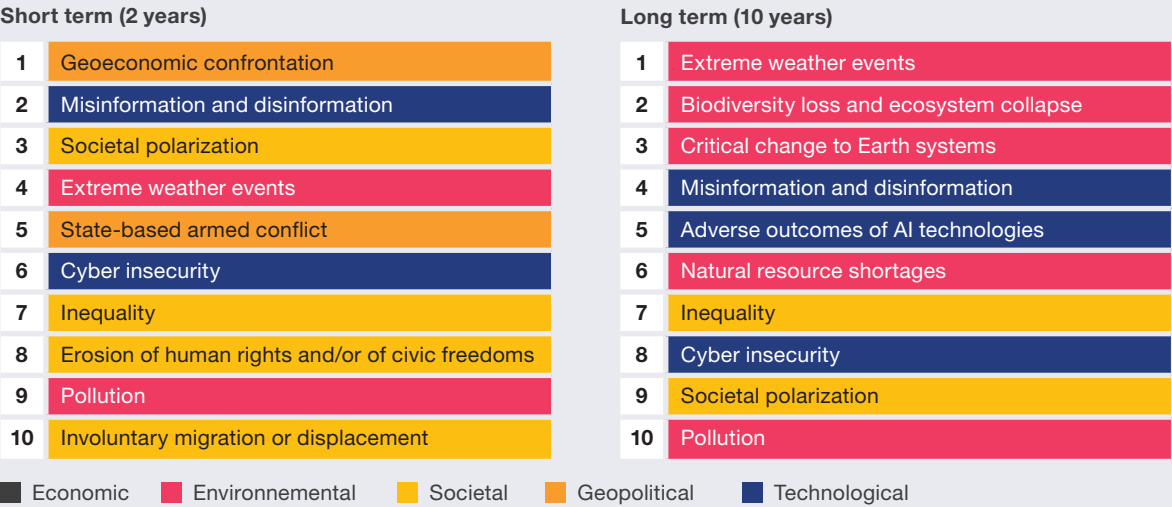
Overall, the 10-year horizon shows that long-term resilience depends on organisations’ ability to address climate adaptation and low-carbon transition while also responding to technological disruption and changing market expectations. Risk Managers have a key role to play in bringing these topics into strategic planning, investment decisions and broader organisational transformation.



Compared with the 2026 WEF Global Risks Report, medium-term risks are perceived differently by Risk Managers. However, several common themes emerge: the topics of geoeconomic confrontation and state-based armed conflict in the WEF report broadly echo geopolitical uncertainty in the Global Risk Manager Survey report, while cyber-related threats also feature prominently in both reports.

Over the long term, both reports point to the predominance of environmental risks, while adverse outcomes of AI technologies also enter the WEF top five this year. By contrast, geopolitical and economic risk categories do not appear in the WEF’s long-term top ten, which is dominated by environmental, technological and societal risks.

Global risks ranked by severity, short term (2 years) and long term (10 years)



Source: World Economic Forum Global Risks Perception Survey 2025-2026



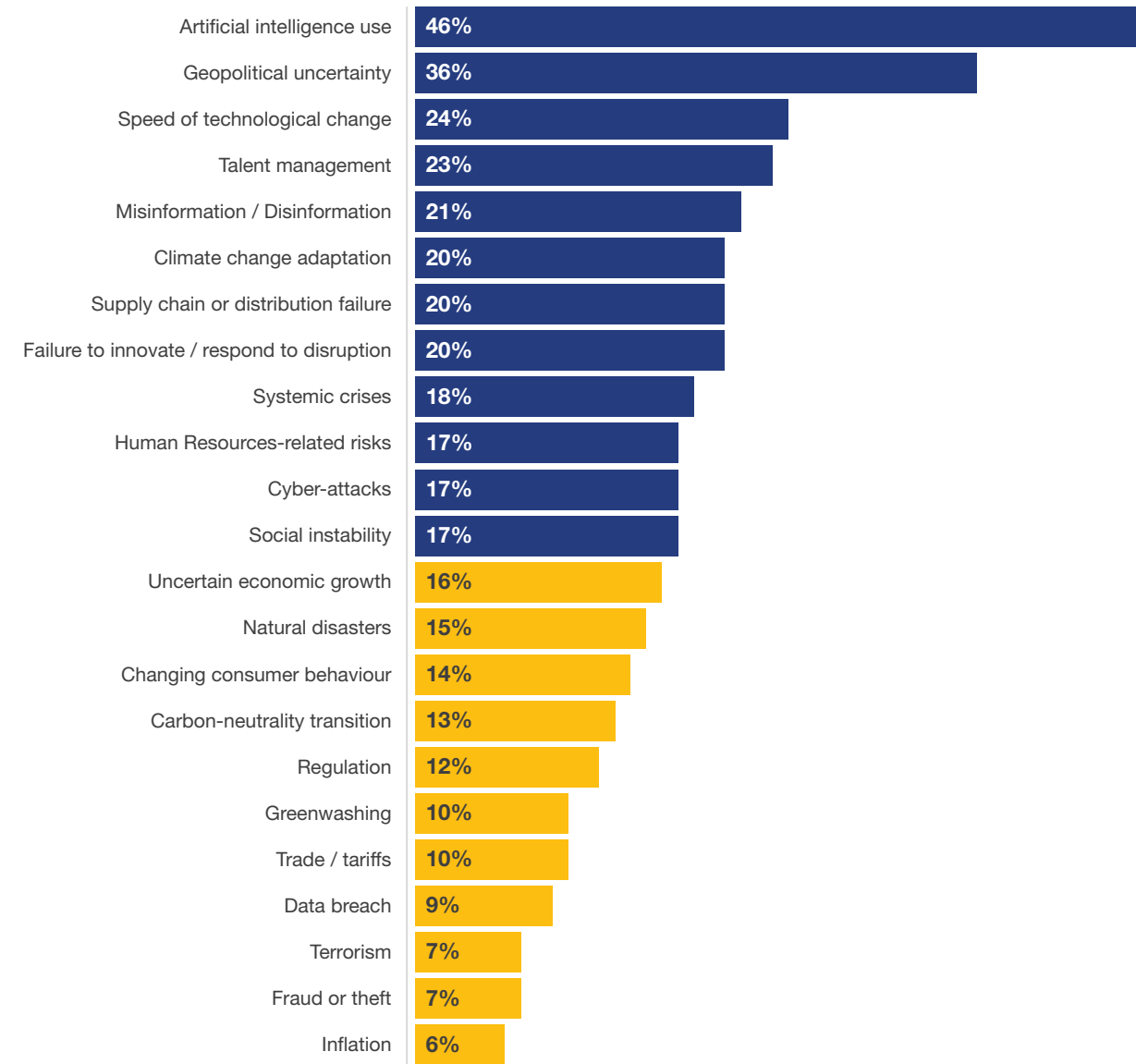
Looking at the medium-term horizon, regional results show more differentiated risk profiles than the global ranking. While AI, cyber and geopolitical uncertainty dominate globally, several regions place greater emphasis on environmental, technological or workforce-related risks.

- In Africa, Speed of technological change ranks first, while AI use is 5th and HR-related risks also appear in the top five, pointing to significant concerns around digital transformation, skills and workforce adaptation.
- In Asia, Natural disasters are perceived as the main threat, with Climate change adaptation ranking fourth, while AI use appears only in 11th position.
- In South America, natural disasters and Climate change adaptation both rank among the top five, alongside Systemic crises in third position. Failure to innovate follows closely in sixth place, while Geopolitical uncertainty and Regulation rank lower, at 11th and 16th respectively.
- In Oceania, Natural disasters also appear in the top five, whereas Geopolitical uncertainty ranks only 11th, suggesting a stronger focus on physical and environmental disruption.
- In North America, Talent management replaces Regulation in fifth position, with regulation falling to 10th, highlighting the continued importance of workforce and skills-related challenges.

At the 10-year horizon, Climate change adaptation appears across all regions. It ranks first in Africa, Asia and Europe, and remains among the top four risks in North America, Oceania and South America. Other environmental risks also feature prominently: Natural disasters are ranked in the top five in Europe, Oceania and South America, while Carbon-neutrality transition appears among the leading long-term concerns in Asia and Europe. Overall, environmental risks are a shared long-term priority across regions, although their relative weight and specific expression vary by geography. More detailed regional differences are presented in the country and regional files.

Looking across time horizons raises a key question for organisations: **how can organisations balance immediate risk priorities with longer-term structural challenges?** Short-term operational concerns, such as regulatory compliance, cyber risk and supply-chain disruption, remain critical. However, risks such as climate adaptation, natural disasters, AI use and changing consumer behaviour require sustained attention, even when their impacts unfold gradually and remain uncertain. Over the next decade, these risks have the potential to reshape business models, stakeholder expectations and organisational viability and need to be addressed and adequately treated by organisations.

Top risks considered as not adequately treated



In 2026, **AI use** remains by far the most inadequately addressed risk, cited by **46%** of respondents, up from **43%** in 2024. This highlights that many organisations are still struggling to keep pace with AI adoption and to establish effective governance, controls and risk management frameworks. **Geopolitical uncertainty** has also increased sharply, rising to **36%** from **27%** in 2024 and remaining in second place. This reflects the continued impact of global instability, conflicts, sanctions and trade tensions, as well as the need to adapt resilience models across both operations and strategy. **Speed of technological change** now ranks third at **24%**, up from fifth place and **17%** in 2024, highlighting the pressure on organisations to respond

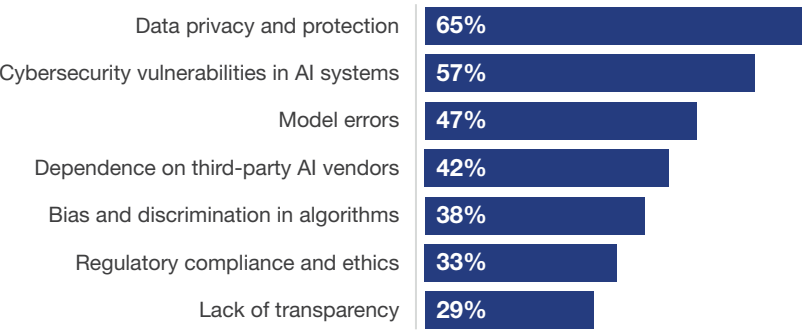
more quickly to technological disruption. **Talent management** remains a key concern, ranking fourth at **23%**, as organisations face growing challenges in attracting, retaining and developing the skills needed in a rapidly evolving technological environment. By contrast, **climate-change adaptation**, which ranked third in 2024 at **22%**, has moved down to sixth place at **20%**, suggesting a slight improvement in how Risk Managers perceive this risk to be addressed. **Human Resources-related risks** have also declined from sixth to tenth place, although the decrease is limited to one percentage point.

Five risks enter the top ten risks considered inadequately treated this year, underlining the growing importance of trust, supply-chain resilience, systemic disruption and innovation capabilities:

- 5th** **Misinformation / disinformation**, cited by **21%** of respondents, reflects growing concerns around trust, reputation and AI-enabled information risks, and highlights the need for organisations to strengthen their monitoring and response capabilities.
- 6th ex aequo** **Supply chain or distribution failure**, rising from **15%** to **20%**, points to continued pressure on sourcing, logistics and distribution networks, driven by geopolitical tensions, armed conflicts, trade restrictions and protectionist measures.
- 6th ex aequo** **Failure to innovate or respond to disruption** highlights the difficulty for organisations to ensure they do not fall behind in adapting their business models, capabilities and technologies to changing market conditions and emerging competitive pressures.
- 9th** **Systemic crises** reflects growing concern about the interconnectedness of risks and the potential for cascading impacts that are difficult for organisations to anticipate, assess and manage.
- 10th ex aequo** **Social instability** highlights growing concerns around social tensions, polarisation and unrest, which can affect organisations’ workforce stability, business continuity, reputation and ability to operate in certain markets.

▶ **AI-related risks are primarily driven by cybersecurity and data protection concerns**

Main concerns related to the use of Artificial Intelligence



This new question for 2026 reveals a broad range of AI-related concerns, suggesting that organisations are now less focused on whether to adopt AI than on how to govern, control and use it responsibly.

This shift is visible throughout the survey: AI now appears among the top short-, medium- and long-term risks, ranks as the most inadequately managed risk, and is a recurring theme across the technology chapter.

Taken together, these findings highlight that AI has moved beyond the status of an emerging technology to become a transversal business risk, requiring coordinated action across governance, technology, compliance, cybersecurity and operational resilience.



From ranking risks to managing uncertainty

Compared with 2024, one message clearly emerges: organisations are no longer managing isolated risks but increasingly navigating interconnected uncertainty across different time horizons. Immediate resilience is shaped by geopolitical instability, cyber threats and economic volatility, while long-term competitiveness depends on successfully integrating AI, climate resilience and broader business transformation into strategic decision-making. The challenge for Risk Managers is therefore evolving from identifying individual threats towards helping organisations balance short-term resilience with long-term adaptability.

01

Risk Managers’ role in strategy, resilience and governance

Risk Managers remain connected as risk mapping expands and governance involvement varies

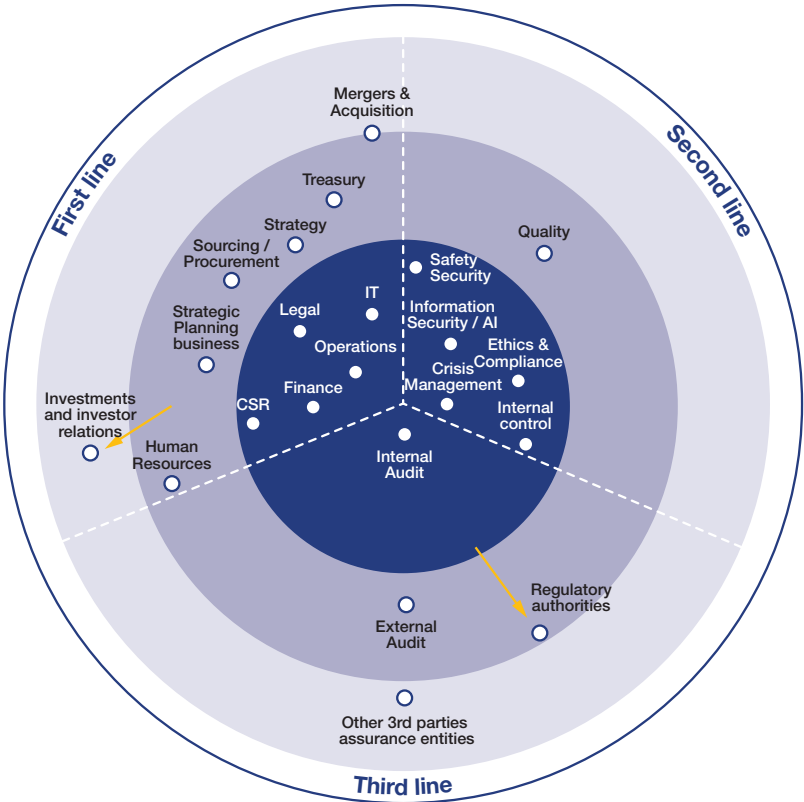
Overall, interactions between Risk Managers and other functions remain broadly stable compared with 2024 across all lines.

Level of relations by line

Evolution since 2024

The radar shows the lines by levels of interactions:

- First rank partners – with whom the risk management function has a regular or close relationship, based on a clear mandate
- Second rank partners – with whom the risk management function has a more distant relationship and occasional collaboration
- Third rank partners – with whom relationships can be improved, as there is little or no relationship or involvement.



Collaboration is strongest with the **second line**: 16% of respondents indicate that the relevant function falls under Risk Management responsibility, 35% report a regular close relationship, and only 16% report no relationship. Interaction with the **first line** is also well established, with 5% of functions under Risk Management responsibility and a high level of collaboration, split between occasional collaboration (39%) and regular close collaboration (38%). By contrast, engagement with the third line remains more limited, with 38% reporting occasional collaboration, 29% regular close collaboration, and 26% no relationship at all.

Collaboration with **Investment and Investor Relations** functions has decreased slightly, after having increased modestly between 2022 and 2024. Interaction with **Mergers & Acquisitions** is now evenly split between occasional collaboration and no relationship. Collaboration with **regulatory authorities** has decreased, with respondents now almost evenly split between regular close collaboration, occasional collaboration and no relationship, whereas only 18% reported no relationship in 2024. This suggests that interaction with regulators may depend on the ongoing regulations deployment.

This confirms that the Risk Manager's influence is increasingly defined by the ability to connect traditional risk governance with emerging and cross-functional risk

topics. While interactions with core governance bodies and assurance functions remain well established, the more contrasted relationships with regulators, investment teams and M&A functions suggest that Risk Managers are not yet systematically embedded in all strategic decision points. Strengthening these links would help organisations move from risk identification to more proactive risk anticipation, ensuring that regulatory developments, capital allocation decisions and transformation initiatives are assessed through a consistent risk lens.

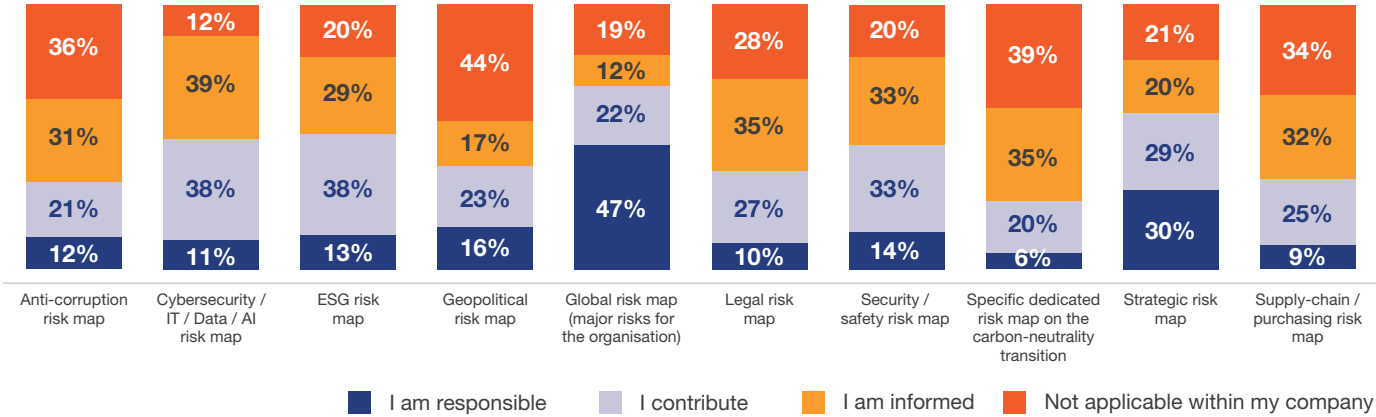


In North America, relationships with the third line appear less developed: 37% of respondents report no relationship, while another 37% report only occasional collaboration. Oceania stands out for the highest proportion of second line functions falling under Risk Management responsibility, at 32%.

Risk Managers broaden their organisational influence through cross-functional engagement and active involvement in risk mapping exercises.

Risk Managers are most frequently fully responsible for the global risk map and the strategic risk map.

Level of involvement in different risk maps



For most risk mapping exercises, around one quarter of respondents report that they contribute, while full ownership varies significantly by risk map. It ranges from 6% for the carbon-neutrality transition risk map to 47% for the global risk map.

Most types of risk maps are performed by at least 61% of respondents' organisations, compared with 70% in 2024. The only exception is the geopolitical risk map, introduced in this year's survey, which is performed by 56% of organisations. Cybersecurity / IT / data / AI risk maps are the most widely implemented, at 88%, followed by global risk maps (81%), ESG and security / safety risk maps (both 79%), and strategic risk maps (78%).



Across regions, geopolitical risk maps are among the least performed exercises. They are not performed by a majority of respondents' organisations in Africa (63%), North America (58%), Oceania (65%) and South America (64%). In Asia and Europe, they are also the least performed risk maps, although a majority of organisations still conduct them, with non-performance rates of 36% and 40% respectively. In North America and Oceania, however, anti-corruption risk maps show the largest gaps, with 68% and 82% of organisations respectively not performing them, compared with 58% and 27% in 2024.

In North America, several risk maps are still not performed by around half of respondents' organisations: net-zero transition risk maps (58%, compared with 61% in 2024), ESG risk maps (46%, compared with 47% in 2024), supply-chain risk maps (44%, compared with 48% in 2024).

In Oceania, carbon-neutrality transition and supply-chain risk maps are each not performed by 53% (compared to 27% for both in 2024). By contrast, cyber risk maps are performed by all respondents' organisations, security / safety risk maps by 88%, and both global and strategic risk maps by 76% (both at 82% in 2024).

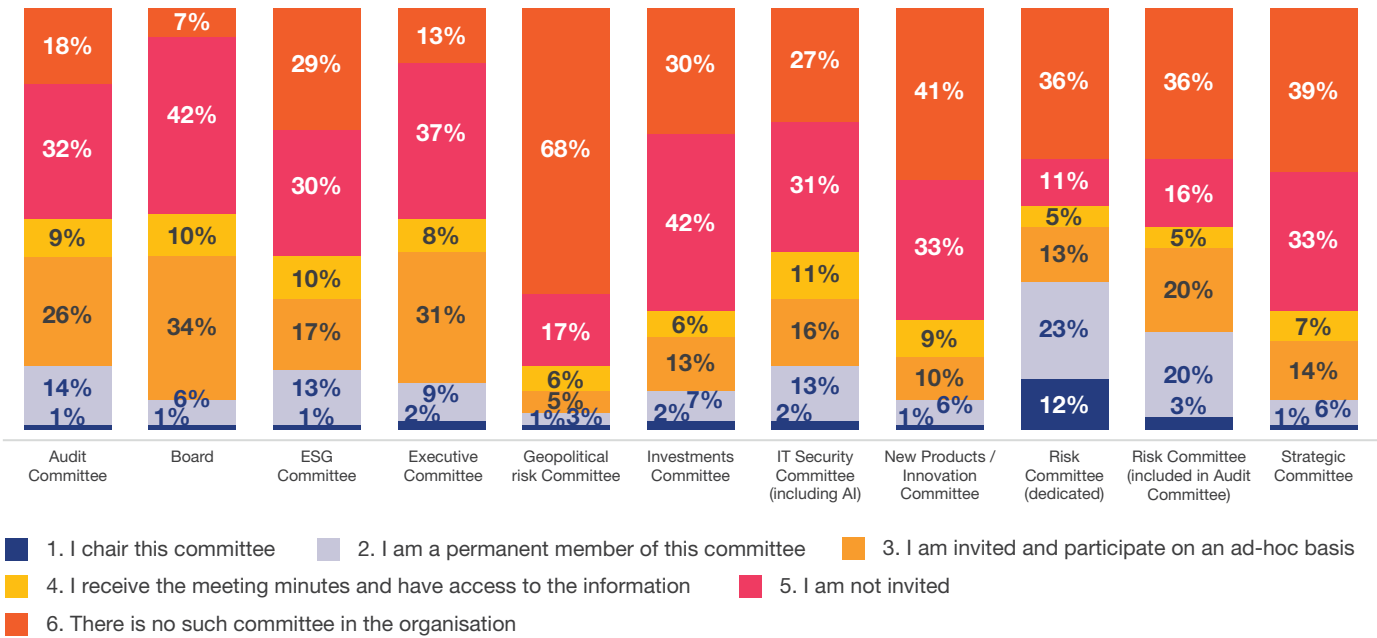
In South America, net-zero transition risk maps are not performed by 57% of organisations, compared with 45% in 2024, while ESG risk maps are not performed by 43%. By contrast, anti-corruption and supply-chain risk maps appear more established in 2026, with 36% and 21% respectively not performed, compared with 44% and 40% in 2024.

Asia is broadly aligned with the global results, with a few notable differences: ESG risk maps are less frequently performed, at 64%, while legal and supply-chain risk maps are more widely implemented, each performed by 91% of respondents' organisations.

Africa broadly follows the global trends and ranking of risk maps performed. However, performance rates are lower across all types of risk maps, except for the global risk map.

► Risk Managers maintain visibility in governance committees, but their strategic involvement could be further strengthened.

Risk management function participation in committees



In 2026, **40%** of Risk Managers are either permanent members of, or invited to participate in, Board and Executive Committees. This represents a decrease from **46%** and **45%** respectively in 2024, suggesting that, while the risk management function remains visible, its position at the centre of strategic decision-making could be further strengthened.

Risk Managers’ presence in Strategic Committees also remains an area for improvement: **21%** are either permanent members or invited to participate, while **33%** report that they are not invited.

Participation in Audit Committees remains broadly stable, with **40%** of Risk Managers either permanent members or invited to participate on an ad hoc basis, compared with **43%** in 2024.

Around two thirds of respondents’ organisations have a Risk Committee, either as a dedicated body or as part of the Audit Committee. Direct involvement is strongest when the Risk Committee is dedicated: **12%** of Risk Managers chair it and **36%** are permanent members or regular participants. Where the Risk Committee is embedded within the Audit Committee, **3%** chair it and **40%** are either invited or permanent members.

ERM profiles and profiles with both ERM and IM responsibilities are more represented in these committees than IM profiles.



Regional differences are notable. Risk Managers appear more strongly represented in these committees in Oceania, where 20% to 60% of respondents report permanent membership, and in Asia, where the range is 10% to 45%. In Africa, Risk Managers also play a more prominent leadership role, with 13% to 31% of respondents indicating that they chair these committees.

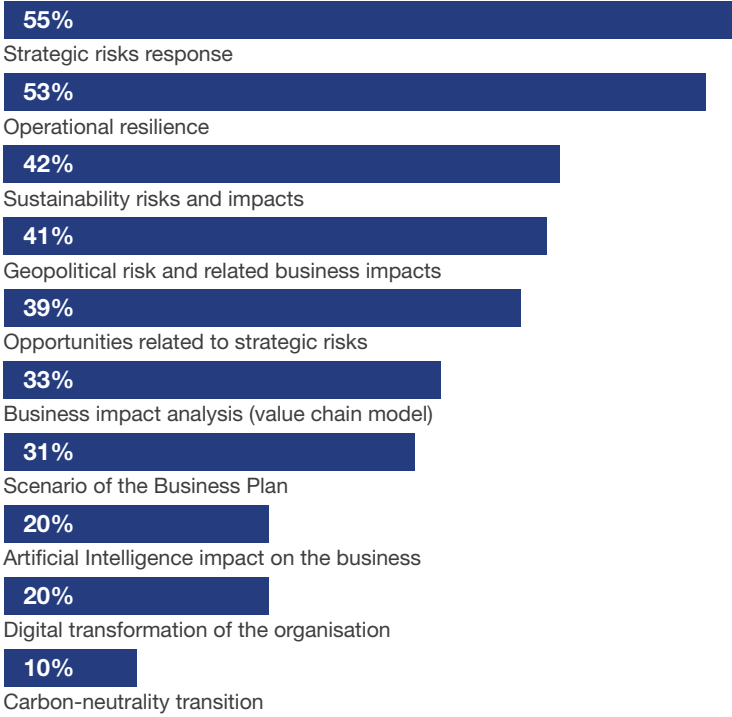
Risk Managers’ support strategy and resilience

► Almost all (92%) of risk managers are being involved in corporate strategy (fully, mostly, or partially).

This ranking remains stable compared with 2024, with one new priority emerging in 2026:

- **Strategic risk response** remains the leading area of focus, cited by **55%** of respondents.
- **Operational resilience** is cited by **53%** of respondents. Introduced in this year’s survey, it reflects the growing importance of organisations’ ability to anticipate, withstand, adapt to and recover from disruption as part of corporate strategy.
- **Sustainability risks and impacts** are analysed by **42%** of respondents.
- **Geopolitical risk and related business impacts** are a focus for **41%** of respondents, stable compared with 2024.
- **Opportunities linked to strategic risks** remain in the top five, cited by **39%** of respondents.
- **Business Impact Analysis and Business Plan scenarios** remain broadly stable in the ranking.
- **Digital transformation** of the organisation is now cited by **20%** of respondents, as **the impact of Artificial Intelligence on the business**.
- **Carbon-neutrality transition** remains the least cited area of focus, at **10%**.

Key focus areas within corporate strategy



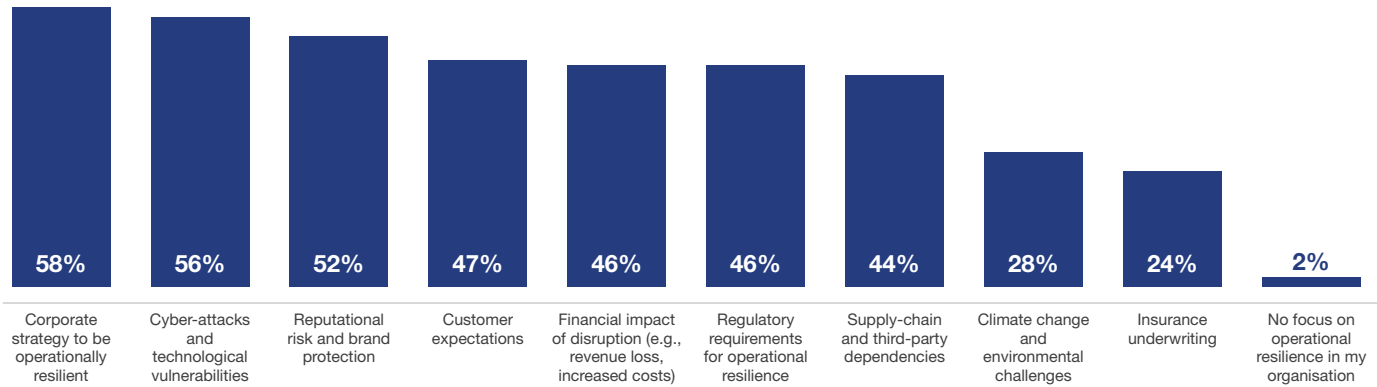
- This ranking can vary significantly depending on the respondents’ continents:
- In South America opportunities related to strategic risks rank first
 - Operational resilience is ranked first in Asia and Africa
 - The third-place ranking of sustainability risks and impacts is driven by Europe, as other continents rank this risk fourth or lower

Operational resilience has become a near-universal strategic priority, addressed by 98% of respondents’ organisations.

Ranked second among corporate strategy priorities, operational resilience is no longer viewed as a purely technical, business continuity or compliance-driven topic. It is increasingly understood as a multi-dimensional imperative, linking strategy, cyber and technology resilience, reputation, customer trust, financial performance, regulatory expectations and third-party dependencies.

This shift reflects the fact that disruption can now affect several critical dimensions of the organisation simultaneously, from operations and supply chains to market conditions and stakeholder confidence. In this context, resilience goes beyond crisis response: it is about preserving the ability to deliver strategic objectives despite cyber threats, geopolitical shocks, climate events or sudden changes in the external environment. This explains why organisations increasingly embed operational resilience into strategic planning, investment decisions and transformation programmes.

Main drivers of operational resilience



The main drivers of operational resilience are broadly distributed, with no single factor dominating. The top three — corporate strategy to become operationally resilient (58%), cyber-attacks and technological vulnerabilities (56%), and reputational risk and brand protection (52%) — are each cited by more than half of respondents.

A second group of drivers is closely clustered: customer expectations (47%), financial impact of disruptions (46%), regulatory requirements (46%), and supply-chain and third-party dependencies (44%). Their proximity highlights the interconnected nature of resilience pressures, which organisations must address simultaneously across operational, commercial and regulatory dimensions.

By contrast, climate change and environmental challenges (28%) and insurance underwriting (24%) rank lower. While these factors are recognised, they are not yet viewed by most organisations as primary drivers of operational resilience — a point to monitor given the prominence of climate risk and insurance market evolution in the broader survey findings.



“Enterprise resilience goes beyond operational continuity and operational resilience alone. It encompasses a strategic, operational and financial triptych, designed to help organisations absorb shocks, respond with agility and adapt their business, strategic and operating models when confronted with multiple external pressures. This is particularly critical in a tense geopolitical environment, where uncertainty, supply-chain disruption, cyber threats, regulatory changes and market volatility are putting organisations under pressure, regardless of sector. Building resilience therefore requires more than crisis management and business continuity plans: it relies on strong governance, robust risk analysis, anticipation capabilities and scenario planning to identify the right levers to activate when needed. Business Impact Analysis also plays a central role by modelling the value chain, understanding critical dependencies and assessing the potential consequences of disruption. Because resilience is inherently transversal, it must involve many functions across the organisation, with Risk Management acting as an orchestrator closely connected to strategy. Ultimately, the objective is to secure, protect and, where necessary, evolve the company’s business model, strategic model and related operating model.”

Laure Laheurte, Partner, PwC France

Risk Managers’ investment priorities continue to vary by time horizon

Risk Managers’ investment priorities reflect a shift from immediate risk identification and response towards longer-term integration, resilience and framework maturity. In the short term, organisations continue to focus on strengthening risk assessment, mitigation and preparedness; over the medium term, the emphasis moves towards embedding risk management more deeply across functions and reinforcing the governance, culture and capabilities needed to support mature and resilient organisations.

Main areas of investment in short and medium term for Risk Management



Over the next 1 to 2 years, organisations are primarily focused on risk mitigation and resilience and risk assessment, both cited by 37% of respondents, followed by risk culture at 32%. This reflects a near-term priority to strengthen preparedness, response capabilities and understanding of current and emerging risks. Most activities remain relevant over this horizon, with responses ranging from 24% to 37%. By contrast, risk-based planning to identify resource requirements and a risk-based approach to internal audit are the lowest priorities.

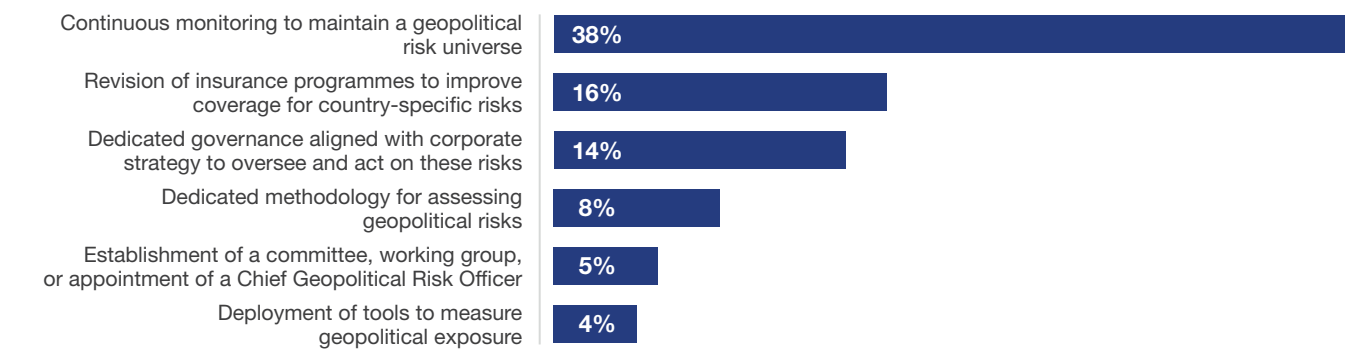
Integration between Risk Management and other functions declined from first position at 46% to fifth at 29%, risk management tools have declined significantly, falling from second position and 45% in 2024 to eighth position and 26% in 2026, while risk culture remains third and risk governance remains fourth, despite both decreasing compared with 2024.

Over the next 3 to 5 years, the main priority remains the integration of Risk Management with other functions, cited by 32% of respondents, compared with 36% in 2024. This is followed by risk mitigation and resilience and risk culture, both at 26%, confirming that resilience remains a priority across both time horizons. By contrast, risk appetite and risk assessment, which rank sixth and second respectively in the short term, fall to the lower end of the 3-to-5-year agenda, at 15% and 14%. A risk-based approach to internal audit remains the lowest priority, at 9%.

This contrast between time horizons suggests that risk assessment is viewed primarily as a near-term priority, while longer-term investment is expected to focus more on integration, resilience, governance and the continued embedding of risk culture across the organisation.

Geopolitical risk is a key concern, most commonly addressed through monitoring activities

Measures implemented to manage geopolitical and geostrategic risks



The measures implemented to manage geopolitical and geostrategic risks reveal a focus on awareness and monitoring while structured governance, formal methodologies or dedicated decision-making instances are emerging.

- 1. **Continuous monitoring** is by far the most common measure, cited by **38%** of respondents. This confirms that organisations prioritise situational awareness, but also suggests that many remain in a reactive mode, relying on information gathering rather than embedding geopolitical risk into formal management processes.
- 2. **Revision of insurance programmes** is cited by **16%** of respondents, reflecting the direct impact of geopolitical instability on risk transfer strategies and the need to reassess coverage, exclusions and limits in a more volatile environment.
- 3. **Dedicated governance aligned with corporate strategy** is mentioned by only **14%** of respondents, despite geopolitical uncertainty ranking as the leading short-term risk in 2026. This points to a disconnect between the perceived importance of the risk and its integration into strategic governance.
- 4. **Dedicated methodologies** for assessing geopolitical risks remain limited, at **8%**, indicating that few organisations have yet formalised consistent approaches to evaluate exposure, scenarios, impacts and response options.
- 5. **Dedicated committees or working groups** are reported by only **5%** of respondents, suggesting that geopolitical risk is rarely managed through institutionalised, cross-functional structures.
- 6. **Specific measurement tools** are the least adopted measure, at **4%**, highlighting a significant gap in analytical and technological support for geopolitical risk assessment and monitoring.

Overall, the data show that geopolitical risk management remains at an early stage of maturity. Most organisations have started by strengthening monitoring, but far fewer have translated this awareness into governance, methodologies, tools or cross-functional structures. This creates a gap between the strategic importance of geopolitical uncertainty and the robustness of the mechanisms in place to anticipate, assess and respond to it.



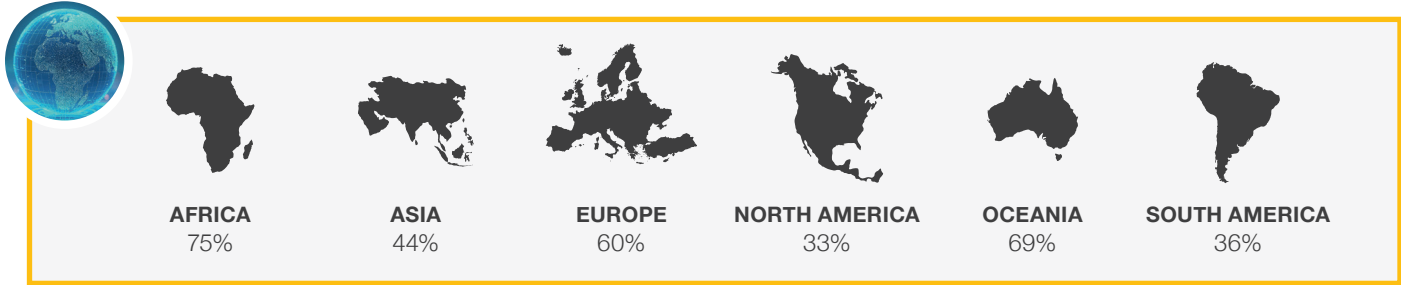
In Oceania and South America, the main measure implemented is a dedicated governance aligned with corporate strategy to oversee and act on these risks, at 41% and 43% respectively.

02

Risk Managers strengthen ESG governance amid uneven progress on climate change and social practices

ESG involvement remains steady, while governance responsibilities gain traction

More than half, **56%** (57% in 2024), of Risk Managers are involved in assessing ESG-related risks.



Risk Managers are strengthening ESG risk governance through analysis, framework definition, reporting and committee participation

Role played by Risk Managers with regards to ESG



Risk Managers are playing an increasingly important role in ESG-related activities. Since 2024, their level of responsibility has increased across all ESG activities covered by the survey. The three areas where Risk Managers most frequently have full responsibility are:

- analysing and mapping ESG risks, cited by 28% of respondents, compared with 22% in 2024
- defining the ESG risk framework, increasing from 19% to 25%
- reporting ESG risks to the Board or its Committees, increasing from 19% to 23%

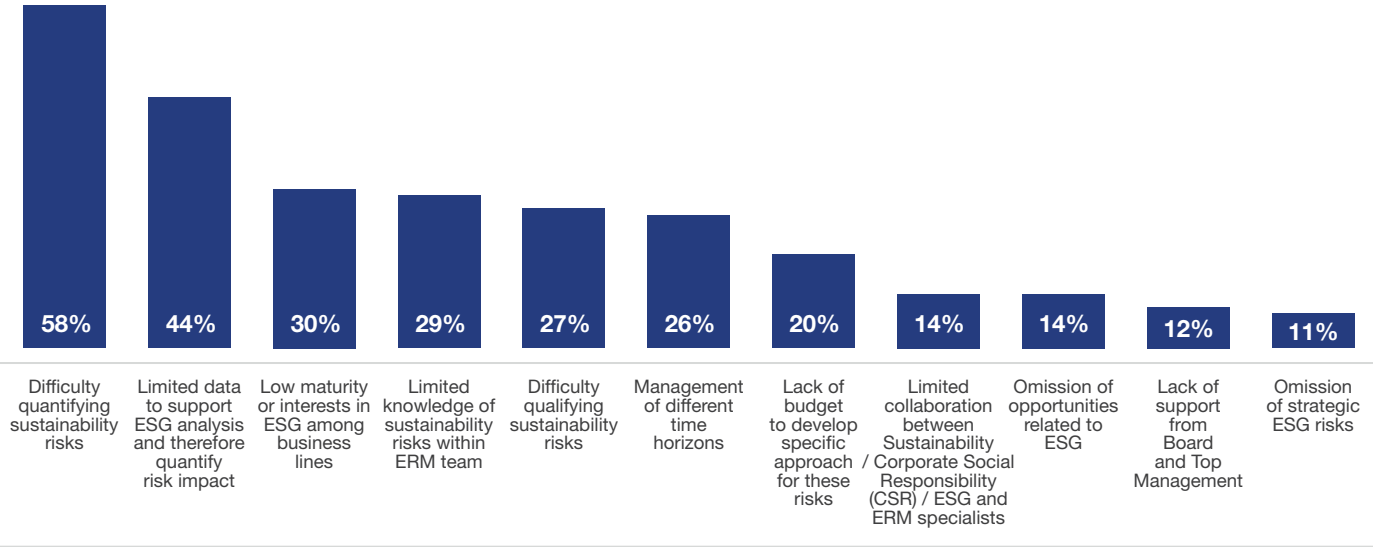
These findings underline the importance of Risk Managers in providing the methodology, framework and consistency needed to analyse, map and report ESG risks effectively.

In addition, more than half of respondents either are responsible for or contribute to other ESG-related activities, including climate-change mitigation and adaptation measures, the integration of ESG risks into corporate strategy, double materiality assessments, corporate sustainability reporting, and scenario

definition and analysis. This role is also reflected in their involvement in ESG committees: 15% are either chairs or permanent members, while a further 17% are invited to and participate in the meeting. In parallel, 13% are responsible for the ESG risk map and 38% contribute to it. Finally, collaboration between Risk Managers and Corporate Social Responsibility, Sustainability or Sustainable Development functions remains strong, although a shift from regular to occasional collaboration is visible. In 2026, 14% of respondents reported no relationship, stable compared with 2024; 7% reported that ESG falls under their responsibility, compared with 10% in 2024; 36% reported regular, close collaboration based on a clear mandate, compared with 44% in 2024; and 42% reported occasional collaboration, compared with 32% in 2024. This is consistent with the continued challenge of limited collaboration between Sustainability and ERM teams, reported by 14% of respondents, stable compared with 2024.

Persistent ESG integration challenges remain, with the maturity across business lines emerging as a key issue

Challenges in integrating ESG into the ERM process



- 1st Difficulty quantifying sustainability risks** remains by far the main challenge in 2026, cited by **58%** of respondents, unchanged from 2024. This challenge is closely linked to the other most frequently cited obstacles
- 2nd Limited data to support ESG analysis and quantify risk impacts**, cited by **44%** of respondents, compared with **49%** in 2024. It remains the second most frequently cited challenge, although the decrease may suggest a modest improvement in data availability, potentially driven in some regions by growing ESG reporting requirements
- 3rd Low maturity of ESG awareness across business lines**, newly introduced in the 2026 survey and cited by **30%** of respondents, entering directly in third position
- 4th Limited knowledge of sustainability risks within ERM teams**, cited by **29%** of respondents, compared with **31%** in 2024, moving from third to fourth position
- 5th Difficulty qualifying risks**, cited by **27%** of respondents, stable compared with 2024 but moving from fourth to fifth position

These results show that integrating ESG into ERM remains a complex exercise, requiring higher-quality data, more robust methodologies and stronger internal capabilities to assess sustainability-related risks effectively.

The lower-ranked challenges remain broadly stable compared with 2024, suggesting that coordination and sponsorship remain relevant for some organisations but that the main obstacles in 2026 are still methodological and capability-related, particularly around quantification and data availability.



In Africa, the top three challenges are **limited knowledge of sustainability risks within ERM teams**, cited by **78%** of respondents, **limited data to support ESG analysis**, cited by **67%**, and **difficulty qualifying ESG risks**, cited by **44%**.

In Asia, the main challenge is **limited data to support ESG analysis**, cited by **75%** of respondents, followed by **difficulty qualifying ESG risks** and **difficulty quantifying sustainability risks**, each cited by **50%**.

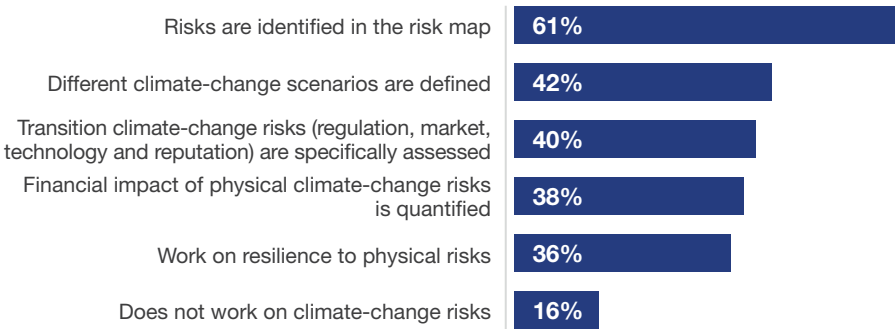
In North America, the top three challenges are broadly aligned with the global results, although the **low maturity of ESG awareness across business lines** stands out as the leading issue.

In South America, the main challenges are the **lack of budget to develop a dedicated approach to ESG risks** and the **limited consideration of ESG-related opportunities**, each cited by **50%** of respondents.

Climate-change practices show modest progress, with greater focus on transition impacts

Climate-change risks remain a key area of focus for respondents' organisations, with **84%** addressing them in 2026, compared with **89%** in 2024. While the decrease may seem counterintuitive in the context of broader global developments around sustainability and climate-change adaptation, it should be monitored over a longer period to determine whether it reflects a lasting trend or a short-term fluctuation.

Climate-change practices in organisations



Among the main practices, **61%** of respondents' organisations **identify climate change risks in their risk maps**, broadly stable compared with 2024. As noted earlier in the report, another 61% report performing a dedicated carbon-neutrality transition risk map. The use of **climate-change scenarios** has increased from **38%** to **42%**, indicating that organisations are gradually moving beyond risk identification towards more forward-looking approaches. This trend may reflect the growing need to test the resilience of strategies, assets and operating models under different climate pathways. The **assessment of transition climate risks** has recorded the strongest increase, gaining two places in the ranking and rising by 7 percentage points, which suggests stronger attention to the business implications of decarbonisation, regulatory change, market shifts and evolving stakeholder expectations. Meanwhile, **quantifying the financial impact of physical climate risks**, which ranked third in 2024, has moved down one position but increased in absolute terms, from **35%** to **38%**. In addition, **36%** of respondents report that their organisations **work on resilience to physical risk**, compared with **34%** in 2024.

These trends point to a gradual broadening of climate-risk practices. Organisations continue to rely on risk mapping as the foundation of their approach, but are increasingly complementing it with scenario analysis, transition-risk assessment and resilience measures. This suggests a more holistic integration of climate change into Enterprise Risk Management frameworks, with climate risks increasingly considered not only as sustainability issues, but also as strategic, operational and financial risks that need to be embedded in governance, planning and decision-making.



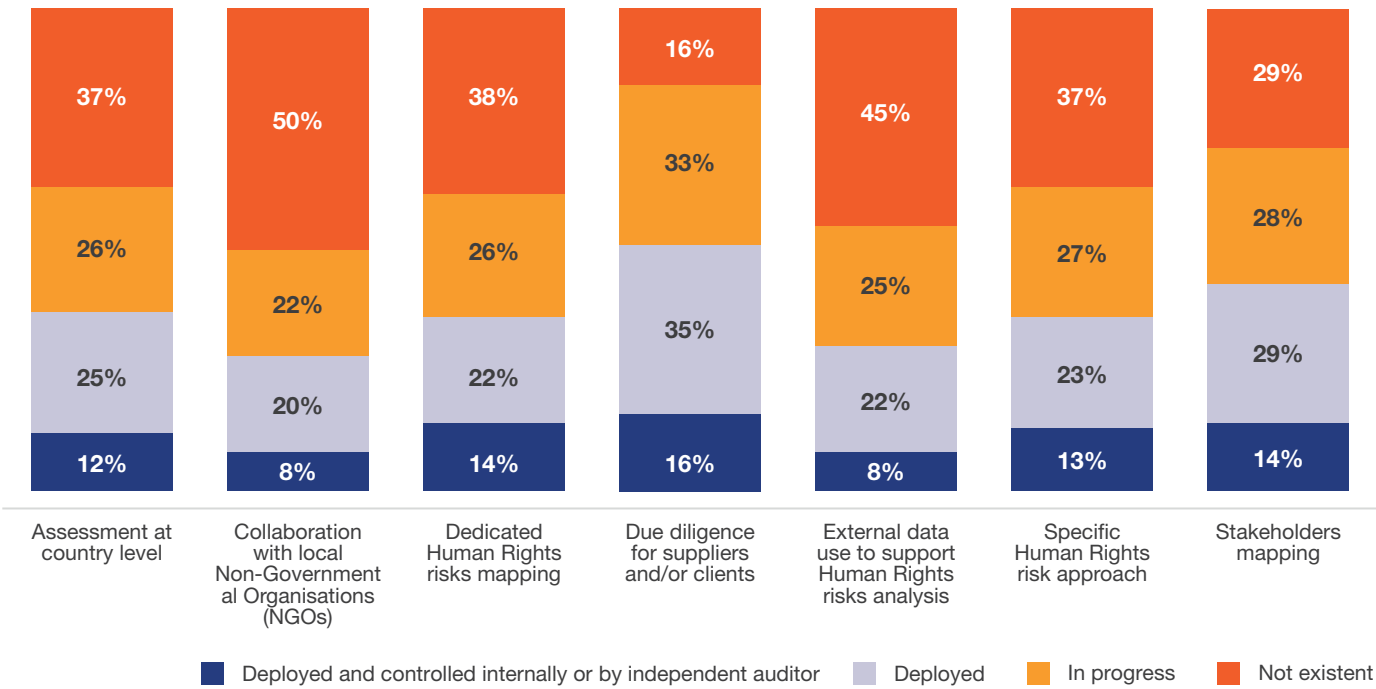
Regional differences remain significant: 50% of respondents in Africa report that their organisations do not work on climate-change-related risks, compared with 33% in Asia, 29% in North America, 27% in South America, 19% in Oceania and 12% in Europe.

Identifying climate-change-related risks in risk maps is the leading practice in several regions, including Africa (50%), Oceania (63%) and both North and South America (45%). Asia stands out, with only 11% of respondents reporting this practice; instead, the quantification of the financial impact of physical climate-change risks is the most frequently cited action, mentioned by 44% of respondents.

The assessment of transition-related climate-change risks is the least frequently reported activity in South America and Africa, performed by only 9% and 8% of respondents respectively.

Social ESG practices gain ground, but maturity varies

Approaches to identifying and assessing social and Human Rights risks



The results suggest that Risk Managers are less advanced on the social dimensions of ESG than on climate-change-related practices. However, the picture is nuanced: while fully deployed social-risk activities have increased compared with 2024, the share of activities reported as not existing has also risen, suggesting that some initiatives previously described as “in progress” have either been completed or have lost momentum. Overall, between one quarter and one half of respondents report that these activities are deployed in their organisations, with deployment levels increasing across all activities compared with 2024.

The most established practices are **third-party due diligence** (increased from **44%** to **51%**), and **stakeholder mapping** (from **40%** to **43%**). By contrast, **collaboration with NGOs** and the **use of external data to support Human Rights risk analysis** remain the least developed, indicating that organisations still tend to prioritise more operational and compliance-driven activities over broader engagement or advanced analytical approaches.

Dedicated Human Rights risk maps and specific **Human Rights risk approaches** remain broadly stable, with **36%** of respondents reporting that each is already deployed in their organisation. At the same time, **37%** report performing **Human Rights risk assessments at country level**, up from **33%** in 2024.

The financial services sector shows the greatest room for improvement on social matters, with only around one quarter of activities deployed on average. By contrast, Industry appears to be the most advanced sector overall.



Europe leads with the most mature profile, potentially driven by regulatory compliance. Due diligence is the most deployed activity across the world, and Africa remains the least engaged, with “not existent” exceeding 2/3 of responses across activities.



In recent years, ESG investments have experienced global growth, driven by increasing regulatory demands for transparency and robust sustainability reporting. However, Europe's introduction in 2025 of the EU Commission's Omnibus package, which softens the Corporate Sustainability Reporting Directive (CSRD) by reducing reporting requirements and postponing deadlines, may impact this trend. This regulatory adjustment, aimed at easing administrative burdens, has sparked concerns about decreased transparency and its potential consequences on ESG investments in Europe. Similar debates are emerging in other regions, such as the United States, where evolving ESG guidelines and regulatory uncertainty continue to influence investor behaviour worldwide.

The softening of CSRD reporting requirements may inadvertently signal a reduction in risk management activities related to sustainability. With less comprehensive and consistent ESG disclosures, investors face greater uncertainty in identifying, evaluating, and mitigating long-term environmental and social risks. Maintaining rigorous sustainability reporting is deemed to remain critical for Europe and globally, as risk transparency and investor confidence underpin the continued growth of ESG investments in an interconnected market.

At the same time, the regulatory shift may provide an opportunity to distinguish more clearly between sustainability activities undertaken primarily for compliance and reporting purposes and those genuinely embedded in organisations' risk management and strategic decision-making. This is a development the risk management community should welcome and promote, but also scrutinise closely in the years ahead.

03

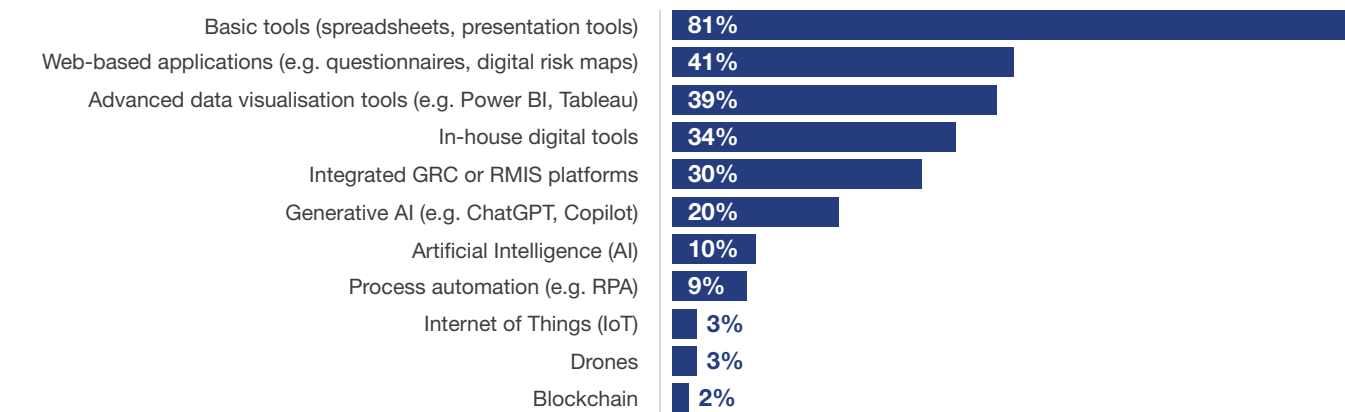
Risk Managers' evolving role in digital and technological transformation

Technology adoption is expanding across all risk management activities

In an era shaped by Artificial Intelligence and accelerating technological change, digitalising risk management activities has become essential to keep pace with evolving risks and decision-making needs. Despite the clear benefits of digital solutions, persistent barriers continue to limit broader adoption and further investment.

Traditional tools remain dominant, while web-based applications and AI usage gain traction

Digital technologies used in risk management activities



Basic tools, including spreadsheets and slide presentations, remain by far the most widely used applications for Risk Management activities, cited by **81%** of respondents, down from **88%** in 2024. **Web-based applications**, such as questionnaires and digital risk maps, now rank second, with usage increasing significantly from **22%** in 2024 to **41%** in 2026. The use of **advanced data-visualisation tools** remain broadly stable, rising slightly from **38%** to **39%**, while **in-house digital tools** have decreased from **39%** to **34%**. **Integrated Risk Management Information System (RMIS) or Governance**,

Risk and Compliance (GRC) platforms have also declined, from **40%** in 2024 to **30%** in 2026.

The results also show a gradual increase in the use of **AI** for Risk Management activities. In 2026, **10%** of respondents report using AI and **20%** report using generative AI, bringing combined AI-related usage to **30%**, compared with **26%** in 2024.

The 64% of respondents who reported having either an in-house or RMIS/GRC tool deployed, described using this tool for the following activities:

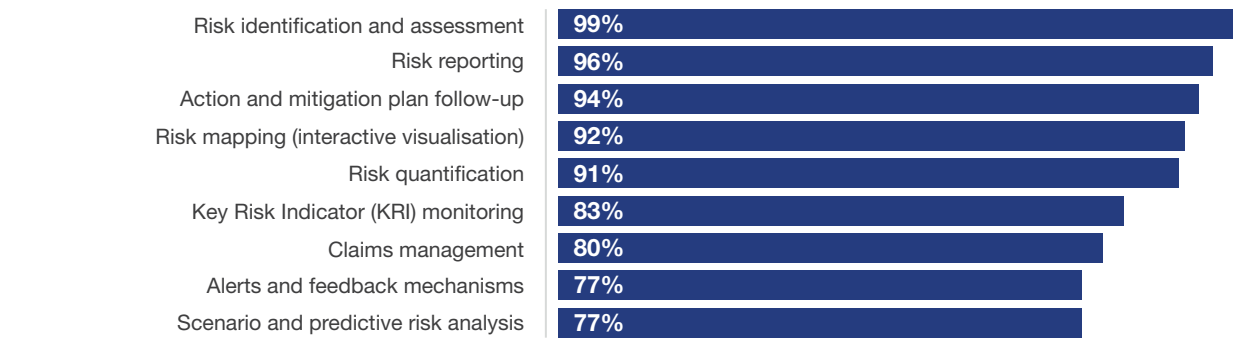
Type of RMIS / GRC module deployed



Technology adoption accelerates across risk management activities, strengthening data-driven decision-making

The technologies presented on the prior page are applied across the risk management activities outlined below.

Technology-backed risk management activities



The 2026 results show a marked increase in the use of technology across risk management activities. Adoption levels now range from **99%** for the highest-ranked activity to **77%** for the lowest-ranked activity, compared with a range of **77%** to **36%** in 2024.

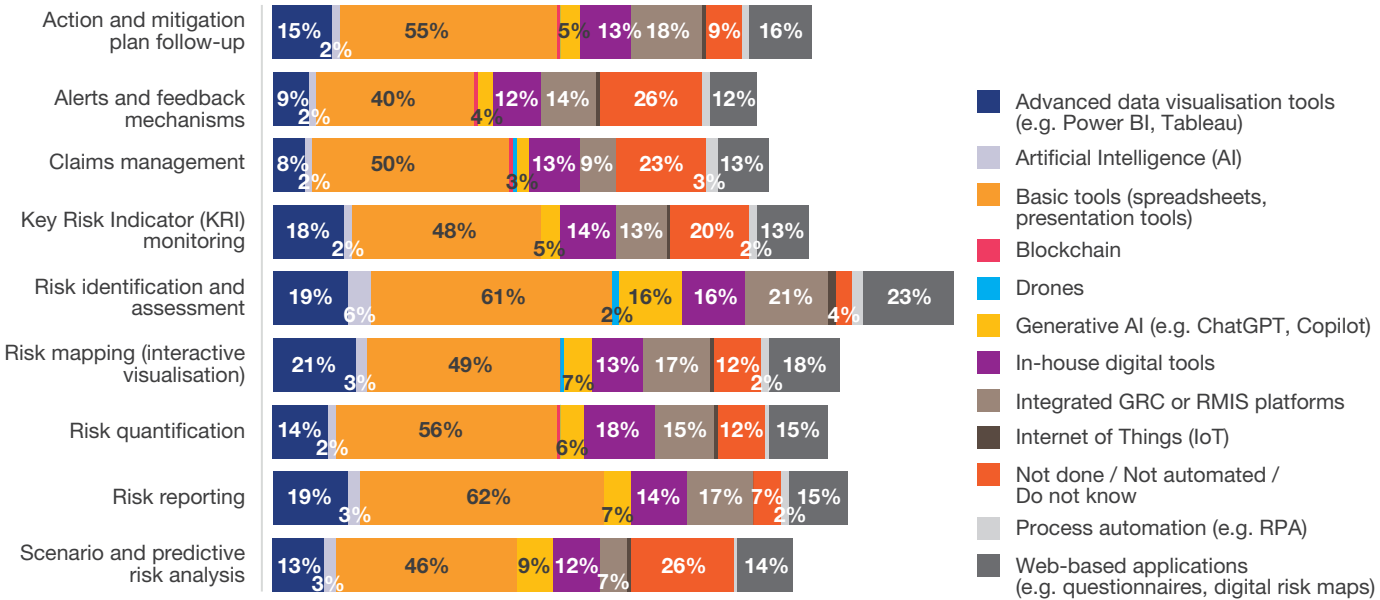
Risk identification and assessment remain the leading technology-enabled activity, cited by **99%** of Risk Managers, compared with **77%** in 2024. **Risk reporting** now ranks second, at **96%**, whereas it was ranked joint third in 2024 at **70%**. It is closely followed by **action and mitigation plan follow-up**, cited by **94%** of respondents, also up from joint third position at **70%** in 2024. **Interactive risk mapping visualisation** has moved from second to fourth position, but its use has increased substantially in absolute terms, from **71%** to **92%**. **Risk**

quantification remains in fifth place, rising from **67%** to **91%**.

These findings suggest that Risk Managers are increasingly leveraging technology to generate more dynamic, real-time insights and strengthen decision making. The strong growth in technology-enabled risk quantification also points to a shift towards more precise, data-driven approaches.

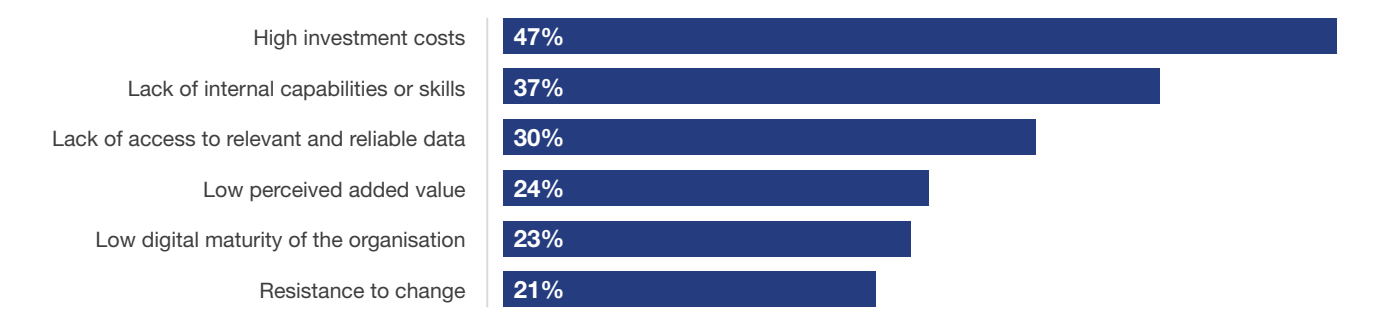
Scenario and predictive risk analysis is now supported by technology for **77%** of respondents, compared with **50%** in 2024. This increase may reflect both the growing need to address complex and interconnected risks, and the expanding ability of new technologies, including AI, to support more forward-looking risk analysis.

Technology adoption is accelerating across all risk management activities, although basic tools remain dominant



► **Barriers persist as Risk Managers seek to scale data and technology use.**

Barriers to the adoption of digital technologies in risk management



Despite the clear benefits of technology in improving efficiency, enabling automation and strengthening the ability to anticipate risks, Risk Managers continue to face several barriers to broader adoption.

- 1st** | **The level of investment required** remains the leading obstacle, cited by **47%** of respondents in 2026, compared with **50%** in 2024, **45%** in 2022 and **50%** in 2020.
- 2nd** | **The lack of internal capabilities or skills** now ranks second, at **37%**, up from fourth position and **27%** in 2024.
- 3rd** | **The lack of access to relevant and reliable data** ranks third, at **30%**, whereas it ranked last in 2024, at **18%**.
- 4th** | **The perceived lack of added value** for the function has declined in relative importance, now ranking fourth, compared with second in 2024 (**24%** in 2026, **36%** in 2024, **39%** in 2022 and **52%** in 2020).
- 5th** | **The low digital maturity of the organisation** remains broadly stable, decreasing from **27%** to **23%**, and moves from third to fifth position.

Technology adoption in risk management is no longer mainly constrained by awareness of its potential value, but by organisations’ ability to operationalise it effectively. While Risk Managers increasingly recognise the benefits of digital tools, automation and AI-enabled analysis, broader adoption still requires significant investment, reliable and accessible data, and specialised capabilities that many functions do not yet fully possess. The rise of skills and data-related barriers suggests that the challenge has shifted from convincing stakeholders of the relevance of technology to building the foundations needed to use it at scale. Digital maturity becomes a determining factor where appropriate governance, data infrastructure and internal expertise are needed to move beyond isolated tools or pilot initiatives towards more integrated, value-generating risk management solutions.

Risk Managers remain closely connected with tech functions to manage technology-related risks across the organisation

► **Close collaboration with IT, Information Security (IS) and AI functions is essential for Risk Management.**

This collaboration participates in understanding emerging technologies, assessing the risks they may create, and defining proactive responses. Such collaboration helps embed technological risk awareness across the organisation and strengthens its resilience in the face of digital disruption.

In this context, Risk Managers continue to report a high level of collaboration with IT teams, stable at 57% in 2026, in line with 2024. Collaboration with IS / AI teams remains significant, at 53%, although this represents an 8 percentage point decrease compared with 2024.

In addition, 42% of Risk Managers are involved in IT security committees where such committees exist, broadly stable compared with 43% in 2024. A further 26% are involved in New Products / Innovation Committees, compared with 31% in 2024.

Risk Managers are more involved in cybersecurity / IT / data / AI risk mapping than in 2024, with 49% reporting involvement, compared with 37% in 2024. This suggests that Risk Managers are moving beyond coordination with technology functions to play a more active role in structuring the identification, assessment and governance of technology-related risks.



At the global level, collaboration remains high with IT teams (91%) and IS / AI teams (89%), a trend reflected across all continents in 2026.

In every region, at least 44% of Risk Managers are involved in cyber / data / AI / IT risk maps.

► **Risk Managers are also increasingly involved in managing risks arising from the use of AI.**

Risk Managers’ main activities are **monitoring regulatory developments**, cited by **54%** of respondents, and **deploying internal policies for the day-to-day use of AI**, cited by **52%**. These two activities have increased significantly since 2024, when they were already the leading AI-related risk management practices, at **34%** and **29%** respectively. In addition, 41% of respondents report **close collaboration between IT and ERM teams to identify AI-related risks and define mitigation actions**, representing an 18 percentage point increase and a one-place rise in the ranking. A further **31%** **analyse risks before any use of AI**, while **27%** have **established a dedicated AI Committee**. By contrast, **25%** indicate that **AI-related risks are monitored only by IT teams**, now ranking sixth, down from third position in 2024. Finally, **19%** **work with Internal Audit on existing AI-related risks** to ensure appropriate review of AI use, up 7 percentage points from 2024.

This ranking is broadly reflected across all sectors of activity.

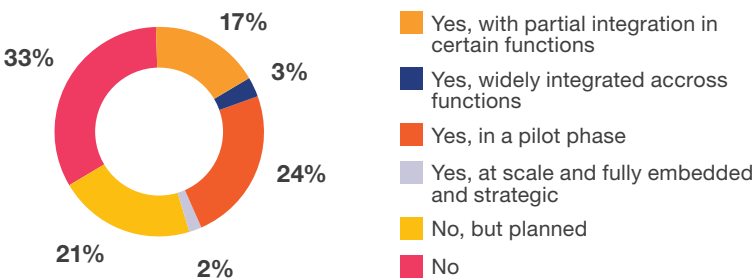


Africa primarily focuses on establishing dedicated AI committees, while Oceania, North America and South America mainly focus on deploying internal policies for the day-to-day use of AI.

Progressive adoption of Artificial Intelligence

Artificial Intelligence is progressively being adopted in Risk Management functions, although its use remains at an early stage in many organisations. While **33%** of respondents report that their organisation does not use AI for risk management, a further **21%** indicate that its use is planned, showing that its use is planned, while 46% are already using AI either at scale, widely, partially or in a pilot phase.

Use of AI for risk management



Among organisations already using AI for risk management, adoption is most often at a developing stage: **24%** use it in a pilot phase, and **17%** report partial integration in certain functions. More mature adoption remains limited, with only **3%** saying AI is widely integrated across functions and **2%** indicating that it is fully embedded at scale and strategic.

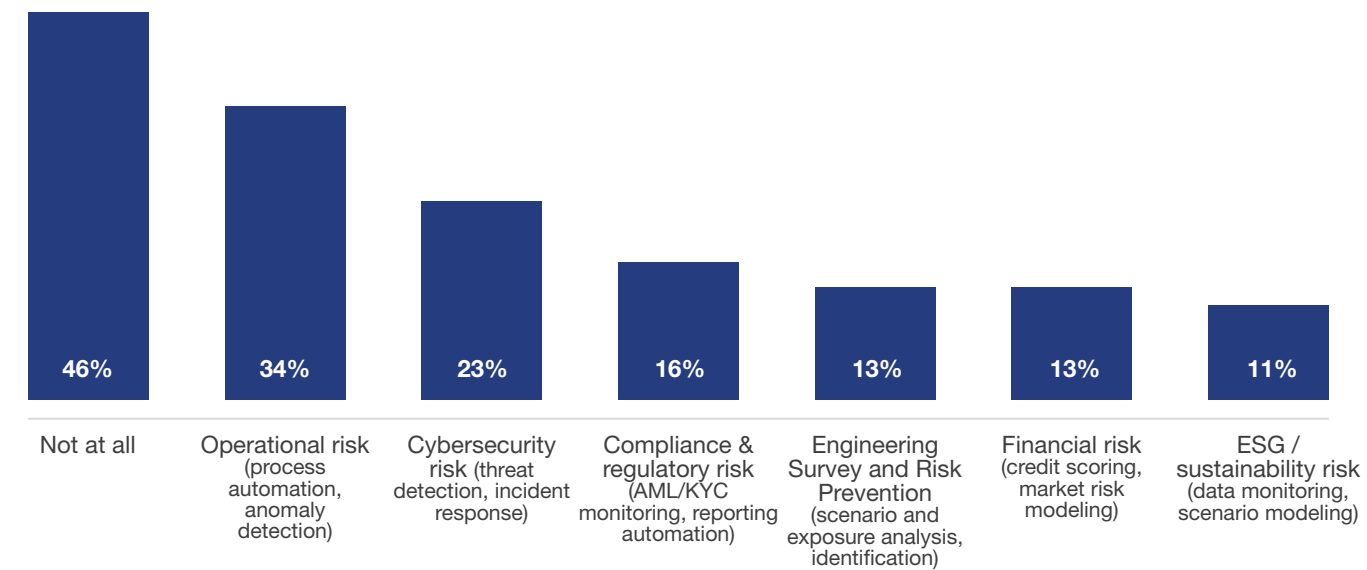
These results suggest that, while AI is clearly gaining traction in Risk Management, most organisations are still in the experimentation or early implementation phase rather than at full deployment.



In Africa, 42% of respondents are either using or planning to use AI. North America appears more advanced, with this figure reaching 68%, including 22% who are planning to adopt it. In Oceania, 38% have already deployed AI and a further 38% are planning to do so. South America and Asia appear to be among the most advanced regions in terms of actual deployment, with 63% and 55% respectively already using AI.

AI adoption for risk management remains targeted

Areas of risk management where AI is currently used



Artificial Intelligence is used within risk management functions in **54%** of respondents' organisations. Where AI has already been adopted, its application is mainly concentrated in operational and data-intensive areas. Operational risk is the leading area of use, cited by 34% of respondents, followed by cybersecurity risk at 23% and compliance and regulatory risk at 16%.

AI use remains more limited in other areas of risk management, with 13% of respondents citing Engineering Survey and Risk Prevention, 13% Financial risk, and 11% ESG / sustainability risk.

These findings reflect the **growing maturity of AI risk governance** within organisations. The rapid expansion of generative AI and the emergence of regulations

such as the **European AI Act** have led organisations to strengthen regulatory monitoring and formalise internal AI usage policies.

The increased collaboration between **IT and ERM teams** shows that AI-related risks are now viewed as **enterprise-wide risks**, rather than purely technology risks, which helps explain the decline in organisations relying solely on IT to oversee AI risks.

The growing use of AI committees, pre-deployment risk assessments and Internal Audit reviews further indicates a shift towards **more structured AI governance**, aimed at addressing compliance, cybersecurity, ethical and reliability concerns.



The findings on AI in Risk Management reflect a broader trend observed among CEOs globally.

According to the [29th PwC Global CEO Survey](#), AI has become a strategic priority, with 42% of CEOs citing the need to transform fast enough to keep pace with technological change and AI as their main concern. However, the survey also highlights that most organisations remain in the early stages of their AI journey: only 12% of CEOs report achieving both cost and revenue benefits from AI, while 56% have not yet seen significant financial returns. These figures do not mean that AI is ineffective. Rather, they suggest that most deployments remain premature, poorly targeted, or insufficiently supported.

Fewer than one in four executives report having widely integrated AI into demand generation or support functions. This limited level of adoption indicates that organisations that are already succeeding in scaling AI are building a significant competitive advantage.

While 67% of executives believe their technology environment is ready for AI, surveyed CTOs and CIOs paint a different picture, highlighting significant risks related to data quality, fragmented systems, and technical debt. This gap creates a major risk: substantial AI investments being built on fragile foundations, potentially leading to costly implementation failures. This aligns with AI adoption in risk management progressing but remaining largely focused on pilot initiatives, partial deployments and targeted use cases in operational, cyber and compliance risk management. Together, the two surveys suggest that organisations are moving from experimentation towards structured adoption, but that large-scale integration and value realisation are still emerging.

Source: PwC, 29th Global CEO Survey: Leading through uncertainty in the age of AI, 2026

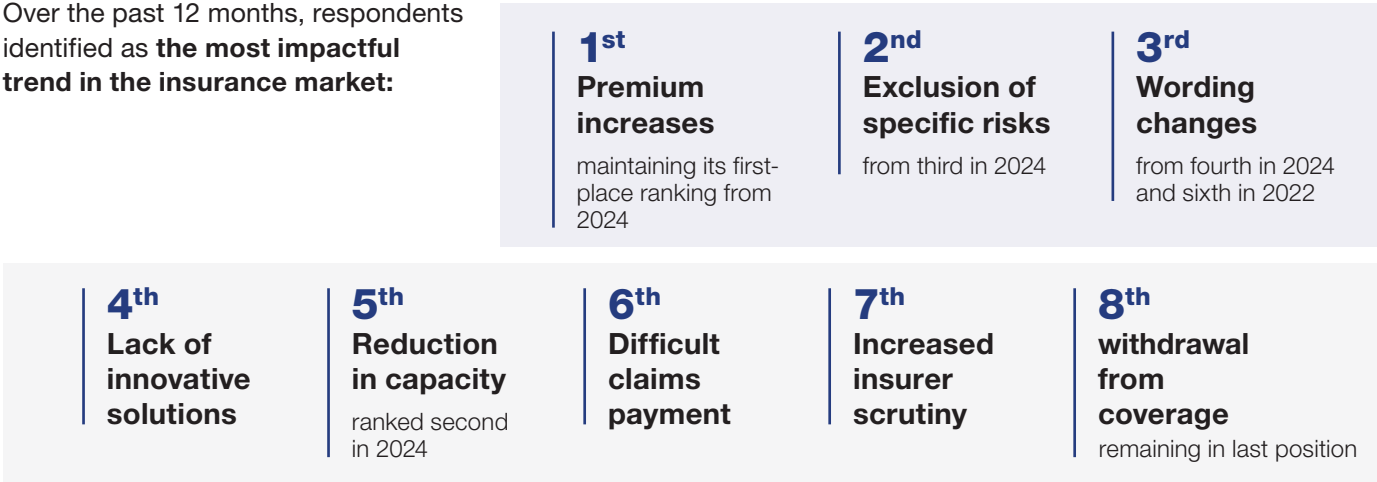
04

**Insurance Managers
maintain established
risk financing strategies**

Over the past 12 months, Insurance Managers have adapted to a changing market

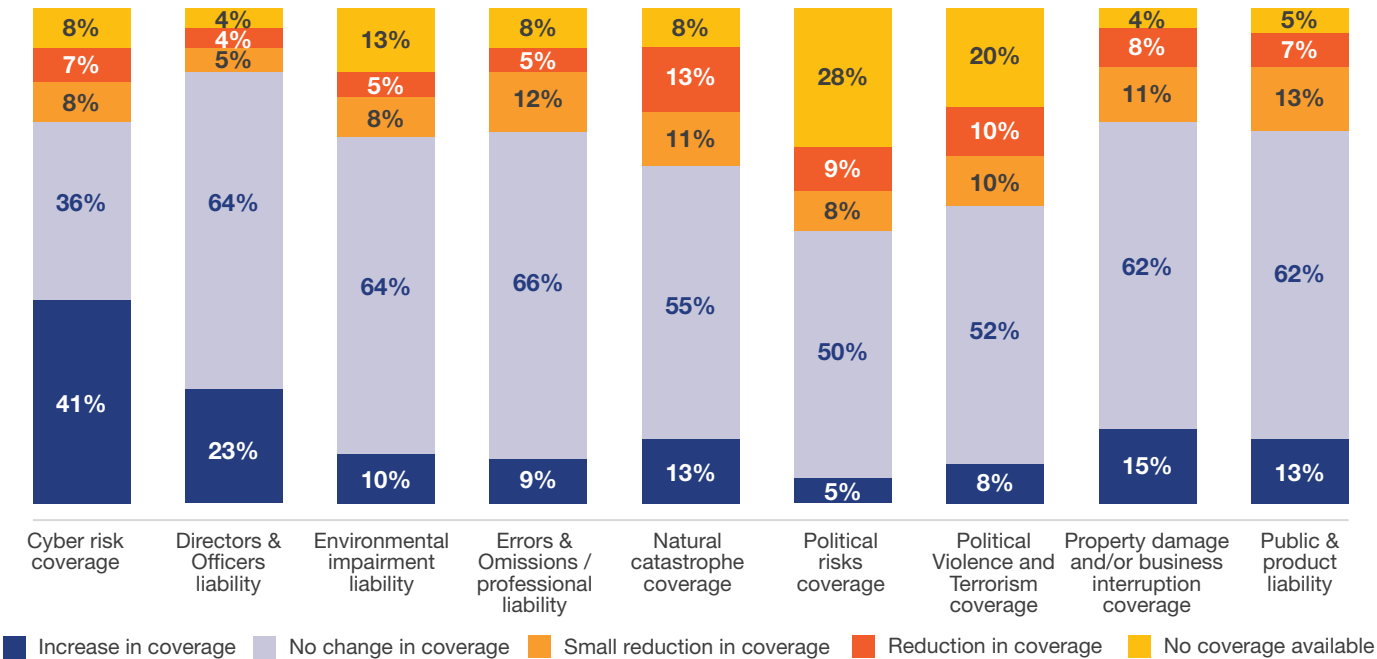
In 2025 and early 2026, the global insurance market was being shaped by a combination of geopolitical pressures, economic volatility, technological acceleration, and increasing regulatory requirements. The hard market of recent years was characterised not only by substantial premium increases across several lines of business, particularly property and casualty and commercial insurance, but also by tighter capacity, stricter underwriting, higher deductibles and more restrictive terms and conditions. The market is gradually entering a phase of normalisation, with increased capacity and competition leading to significant premium reductions in certain lines and for well-managed risks, alongside broader improvements in coverage and terms. However, underwriting discipline remains strong in response to the growing frequency of natural catastrophes, cyber incidents and liability claims. Geopolitical tensions, the fragmentation of global value chains and macroeconomic uncertainty are also driving demand for cyber, political risk, credit and business interruption coverage. More broadly, major megatrends such as digitalisation, climate transition, demographic shifts and the rise of systemic risks are reshaping insurance strategies, with greater emphasis on prevention, resilience and economic transformation.

Over the past 12 months, respondents identified as **the most impactful trend in the insurance market:**



Notable changes in insurance coverage over the past 12 months

Changes in coverage for various business lines over the past 12 months



In 2025, **41%** of respondents reported an increase in **cyber risk coverage**, compared with **25%** in 2024. At the same time, only **15%** reported a reduction in cyber coverage, whether significant or limited, representing a 20 percentage point decrease compared with 2024. A further **8%** indicated that no coverage was available, a level unchanged from 2024. Overall, these results suggest a relative strengthening, or at least a reassessment, of cyber risk insurance strategies, with only a limited proportion of companies experiencing a reduction in coverage.

Property damage and business interruption coverage also evolved positively compared with our previous survey. The share of respondents reporting an increase in coverage remained broadly similar to 2024, while those reporting a reduction fell from 37% in 2024 to 19% in 2026. At the same time, 62% reported no change in coverage, compared with 48% in 2024.

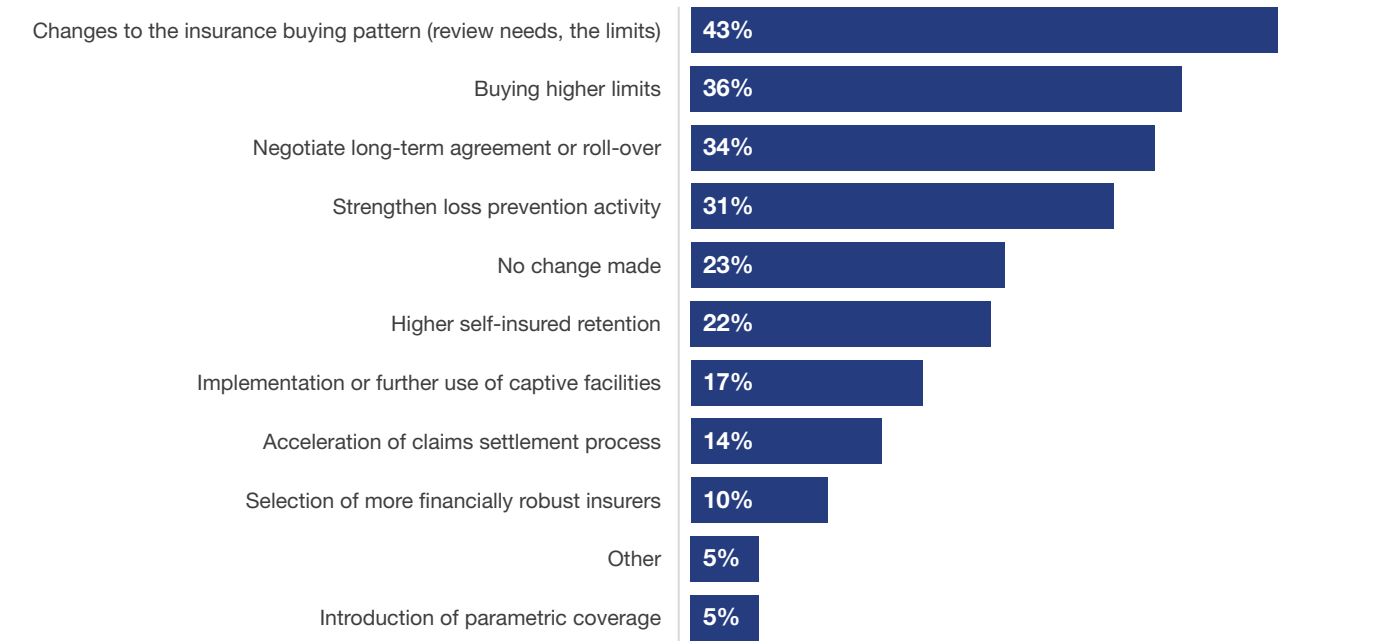
Natural catastrophe coverage and environmental impairment liability remain challenging, although the pressure appears to have eased compared with 2024.

In 2026, 24% and 13% of respondents respectively reported a reduction in coverage, compared with 43% and 19% in 2024. For natural catastrophe coverage, the main difference is reflected in the higher proportion of respondents reporting unchanged coverage, which increased by 12 percentage points. Increases in coverage remained broadly stable, with both business lines recording a modest 3 percentage point rise between 2024 and 2026. However, a slight increase of 3 to 4 percentage points was also observed in the unavailability of coverage for both lines.

Violence and terrorism as well as **political risks**, were introduced as new business lines in this year’s survey, to assess how the insurance market is responding to a more complex geopolitical environment. Comparison with other business lines suggests that these two lines show both the lowest levels of status quo and the lowest reported increases in coverage. They also record the highest levels of unavailable coverage, reported by 20% and 27% of respondents respectively.

Around one quarter of respondents did not change their insurance strategy in 2025

Changes in insurance strategy over the past 12 months



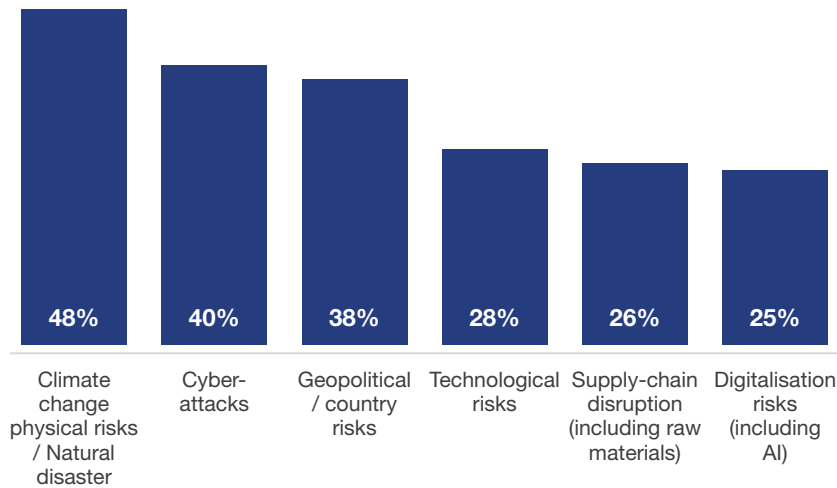
- **Changes to insurance buying patterns** remained the leading action, as organisations sought to reduce premium costs in a fluctuating insurance market while reassessing their coverage considering the evolving risk landscape.
- **Buying higher limits** entered the proposed options and ranked among the top strategies in 2026. This suggests that organisations are seeking additional protection against larger and more complex losses in an increasingly interconnected risk environment.

- **Negotiating long-term agreements or roll-overs** gained one position among the top strategies, as Insurance Managers look to stabilise costs and coverage and secure favourable terms and conditions in a market still shaped by repeated crises. This also reflects the need to reconcile long-term risk assessments with insurance contracts that often remain short-term in scope.
- **Strengthening loss prevention activities** moved down from second place in 2024 to fourth place in 2026, decreasing by 13 percentage points. It nevertheless remains an important lever to anticipate potential market hardening and maintain attractiveness to insurers.
- **Higher self-insured retention** was also introduced as a proposed strategy and was selected by 22% of respondents. This suggests that organisations are increasingly willing to retain a greater share of losses before insurance coverage applies, reflecting a more deliberate approach to risk financing that aims to optimise premium costs, preserve access to coverage and rely more on the balance sheet for predictable or manageable losses.
- **Implementation or further use of captive facilities** decreased by 11 percentage points, suggesting a more selective use of captive solutions compared with previous survey editions.

Over the next 2 years, risk retention remains dominant as Insurance Managers explore targeted alternative solutions

More than 1/3 of respondents think some of their business activities or locations will become uninsurable in the future, down 16 percentage points from 2024

Risks cited as potentially uninsurable in the future



Of the respondents who believe uninsurability is possible in the future, 48% of Insurance Managers identify **physical risks related to climate change** as the area most likely to face a withdrawal of insurance capacity, a sharp decrease from 73% in 2024.

Cyber-attacks remain the second most frequently cited area at risk of becoming uninsurable, mentioned by 40% of respondents compared with 55% in 2024.

Geopolitical and country risks, introduced as a new response option in this year’s survey, are cited by 38% of respondents.

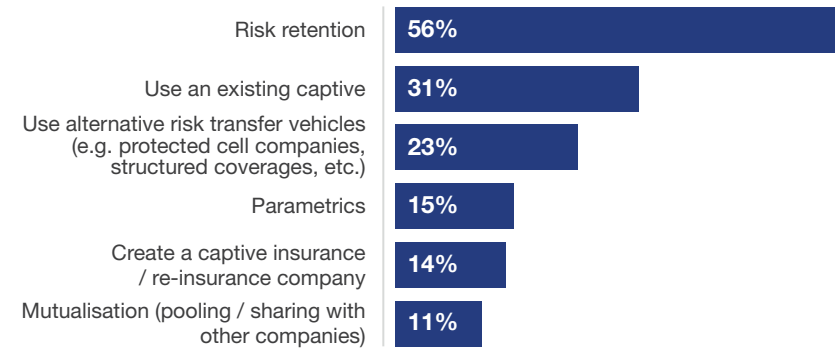
Technological risks are mentioned by 28%, broadly stable compared with 2024.

By contrast, **supply-chain disruptions** and **digitalisation risks, including AI**, both declined in the ranking and decreased by 8 percentage points.

Risk retention remains by far the top strategy for the next two years, across all geographies

The 2026 financing strategy rankings remain broadly consistent with 2024, confirming that **risk retention** continues to be the preferred risk financing strategy. However, its share has continued to decline, from **73%** in 2022 to **62%** in 2024 and **56%** in 2026. This gradual decrease does not suggest a move away from retention altogether, but rather a more selective and structured approach to retained risk. Organisations appear to be reassessing which risks can be kept on the balance sheet and which require complementary financing solutions, particularly in a context of evolving insurance capacity, changing policy wordings and persistent uncertainty around complex or emerging risks.

Strategy in regards to the financing of risks over the next 2 years

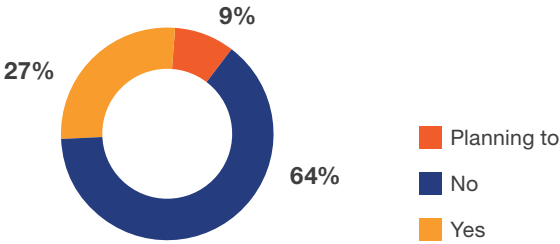


The continued prominence of **existing captives** and **alternative risk-transfer vehicles**, despite a slight decrease of 4 to 5 percentage points each, illustrates the search for more flexible and tailored risk financing mechanisms. These solutions allow organisations to manage volatility, access capacity for difficult-to-place risks and better align risk financing with their own risk appetite.

Parametric insurance, cited by 15% of respondents compared with 19% in 2024, remains a targeted solution, particularly relevant for natural catastrophe exposures where rapid pay-outs and predefined triggers can support recovery. Finally, the **creation of new captive insurance or reinsurance companies** stands at 14%, down from 17% in 2024, suggesting that while captives remain strategically important, organisations may be prioritising the optimisation of existing vehicles over the establishment of new structures.

Captives remain relevant despite lower reported usage

Use of captives and similar risk transfer solutions



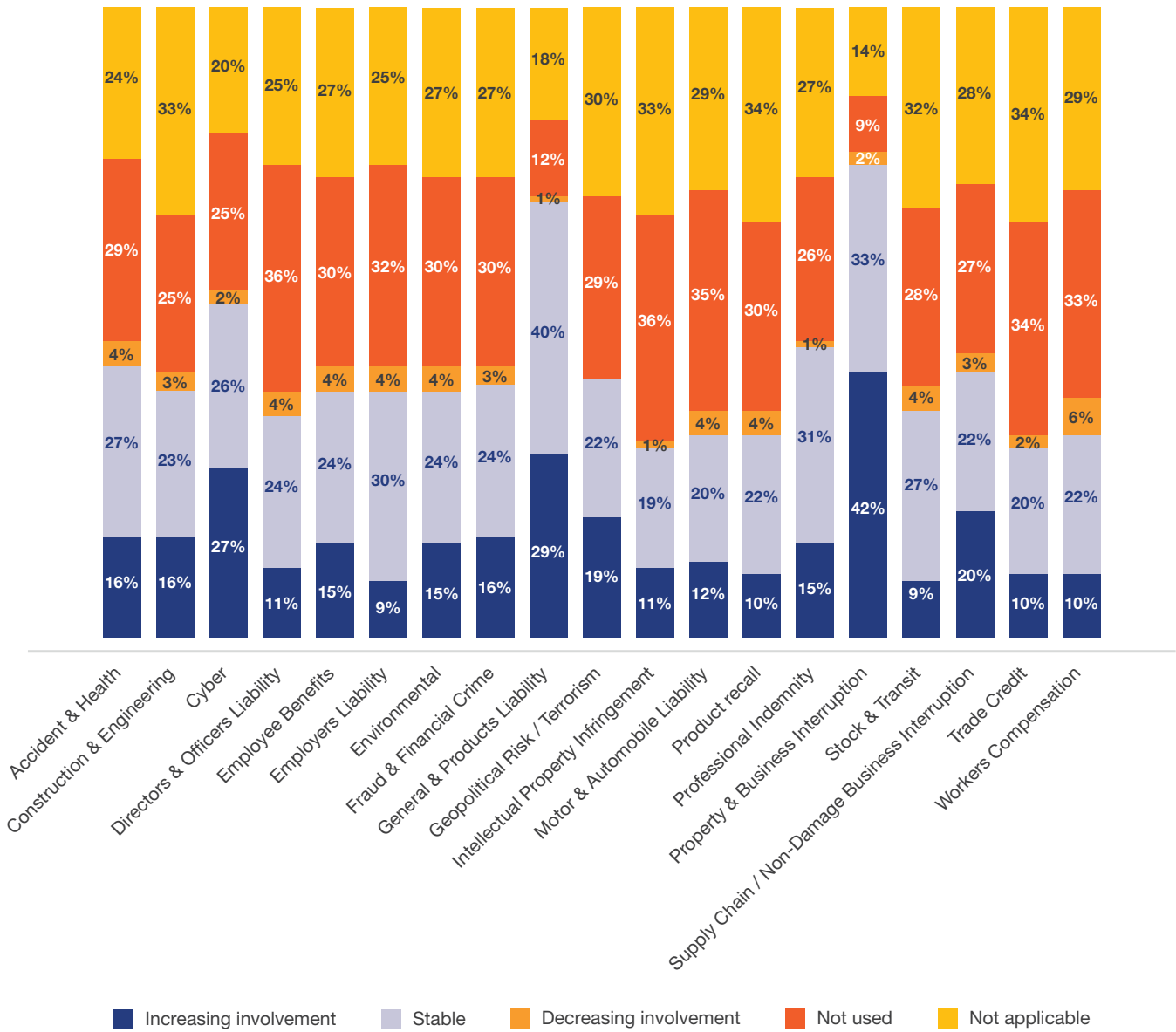
The use of captives has decreased by 10 percentage points compared with 2024, while the proportion of respondents planning to use a captive or similar vehicle remains broadly stable. This suggests that captives continue to be considered a relevant risk transfer solution, but that organisations may be adopting a more selective approach, focusing on existing structures or specific risk financing needs rather than expanding captive use systematically.



Regional differences remain significant. Captive use is highest in Africa, where 33% of respondents’ organisations already use one, followed by Oceania (31%), North America (26%) and Asia (22%). No respondents in South America currently report using a captive, although 9% indicate plans to do so. Planned adoption is also reported in North America (13%) and Africa (8%), while no respondents in Oceania or Asia indicate plans to implement one. These results suggest that future captive development remains concentrated in a limited number of regions and may depend on market maturity, organisational size, regulatory context and the ability to justify the cost and governance requirements associated with captive structures.

Respondents currently using a captive structure were asked how they expect their captive’s involvement to evolve across different lines of cover over the next two years.

Expected captive involvement by line of coverage over the next two years



The results indicate that captives are expected to continue playing a role in the same four main lines of cover as in 2024: **Property and business interruption**, cited by 42% of respondents; **General and products liability**, cited by 29%; **Cyber**, cited by 27%; and **Supply chain / non-damage business interruption**, cited by 20%. This suggests that captives are increasingly being considered not only for traditional property and liability exposures, but also for more complex and potentially constrained lines, such as cyber and supply-chain-related business interruption.

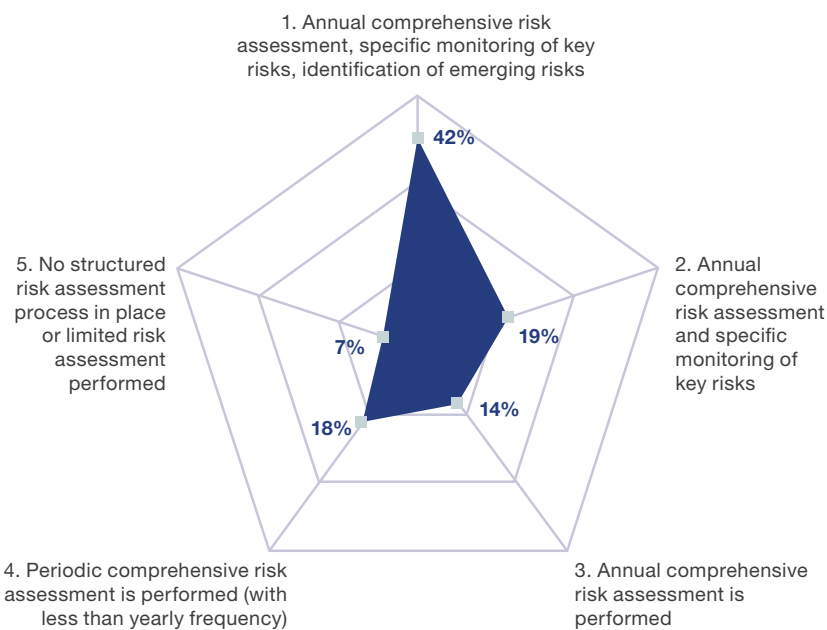
Sectoral differences are visible. **Financial Services** and **Industry** show broadly comparable patterns, whereas the **Services** sector displays a different profile: supply-chain cover is replaced in the leading lines by **Employee Benefits**, cited by 29% of respondents, and **Motor and automobile liability**, cited by 24%. In the **Public sector**, **Directors & Officers** and **Construction & Engineering** follow Property and business interruption, both cited by 29% of respondents, while **Geopolitical risk** and **Professional indemnity** complete the top five at 24%. These differences suggest that captive strategies are closely shaped by sector-specific exposure profiles, with organisations using captives to address the risks most material to their operating model and coverage needs.

05

The maturity of the Enterprise Risk Management model

Maturity varies across organisations and ERM responsibilities

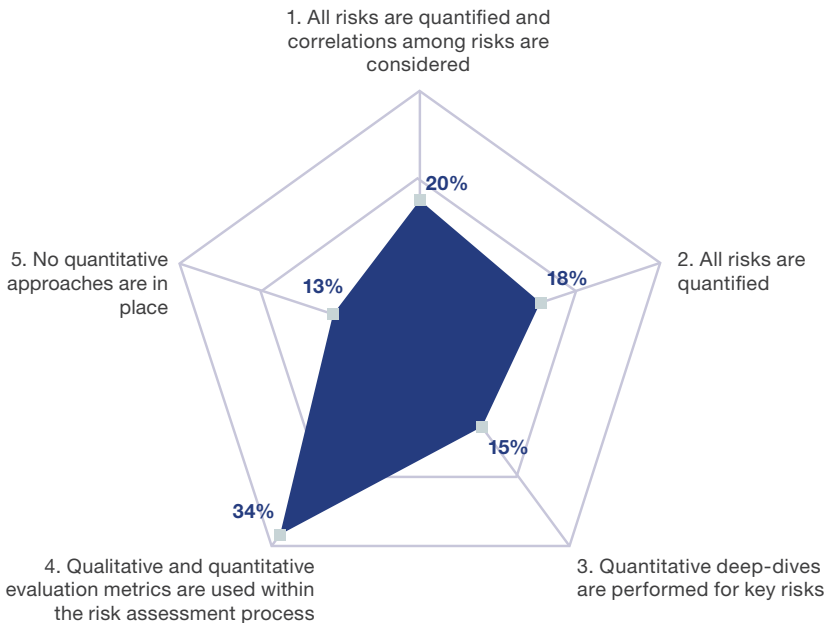
► Uneven maturity in risk assessment approach



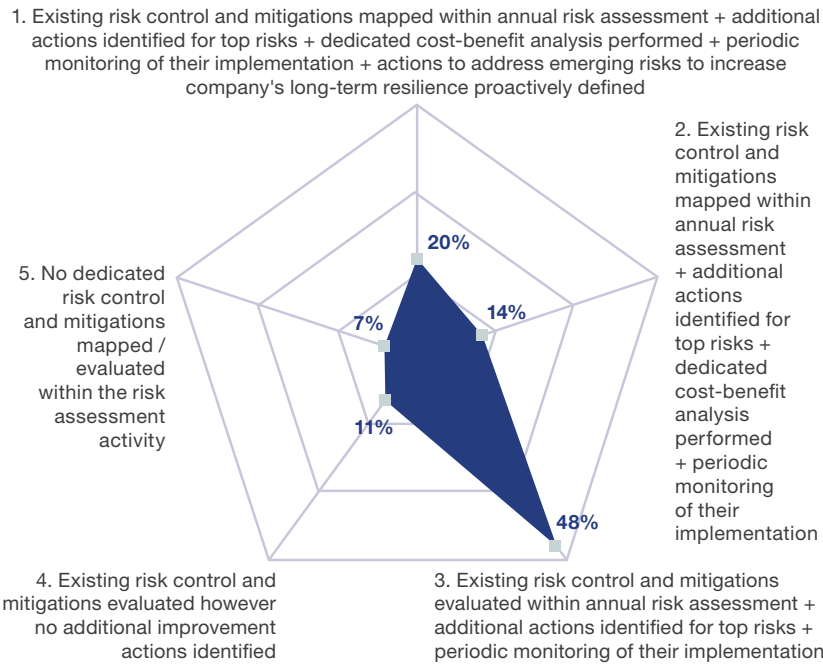
The results suggest that most organisations have established a structured basis for risk assessment, but the level of maturity remains uneven. While 61% of respondents combine regular comprehensive assessments with some form of key-risk monitoring, a significant minority still rely on less frequent or less developed approaches. In particular, 7% report no or limited structured risk assessment (stable since 2024), 18% conduct comprehensive assessments less than once a year, and 14% limit their approach to an annual assessment. This indicates that further progress is needed to embed more continuous monitoring and emerging-risk identification into risk assessment practices.

► Little change in risk evaluation and quantification maturity

In 2026, maturity levels for risk evaluation and quantification remain broadly comparable to 2024. Level 4 out of 5 is still the most frequently reported maturity level, although its share has decreased from 40% in 2024 to 34% in 2026. While this indicates that many organisations have developed relatively advanced quantification practices, the overall picture remains mixed. A stable 20% of respondents report that all risks are quantified and that correlations between risks are taken into account, suggesting that only one organisation in five has reached the highest level of maturity. At the other end of the scale, 13% of respondents indicate that no quantitative approach is in place, highlighting continued room for improvement in embedding structured, data-driven risk evaluation practices.



► Risk mitigation actions still need improvement

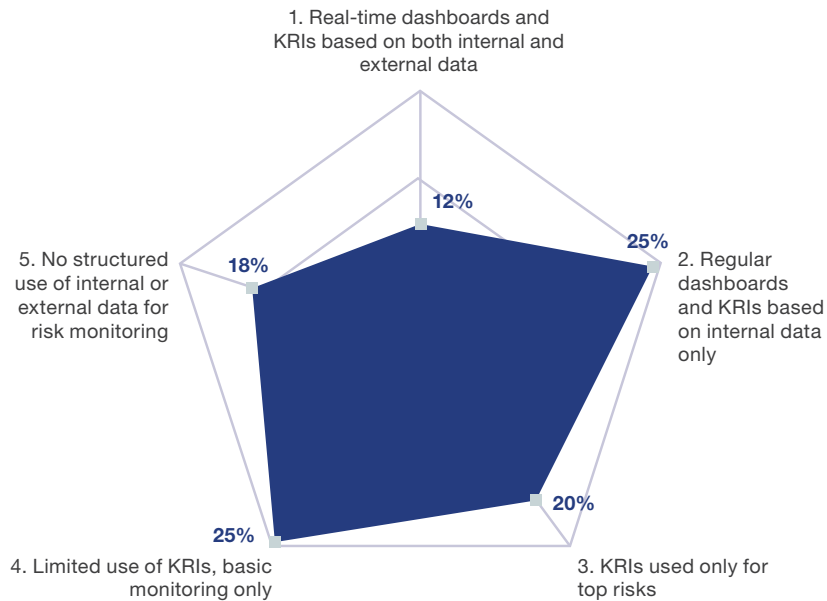


82% of respondents report that risk controls and mitigation measures are mapped and assessed as part of the annual risk mapping process, with improvement actions identified and periodically monitored for top risks. This corresponds to the three highest maturity levels and suggests that most organisations have established a relatively structured approach to risk mitigation.

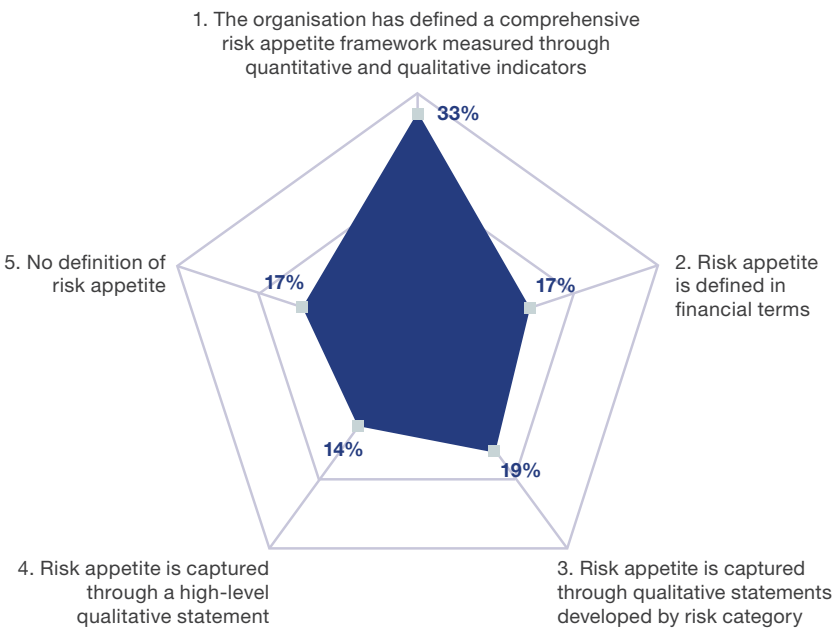
Conversely, 18% of respondents either do not define actions to better address identified risks or do not assess and map the existing controls and mitigation measures in place. This highlights continued room for improvement in translating risk assessment into actionable and monitored mitigation plans.

► Risk monitoring using data remains uneven

The assessment of companies' maturity in leveraging data to monitor risks reveals a broad spread of practices. Only 12% of respondents have reached the highest level of maturity, using real-time dashboards and key risk indicators based on both internal and external data (compared with 21% in 2024). Most respondents, 70%, report an intermediate level of maturity, with limited use of KRIs, mainly focused on top risks and, in some cases, supported by regular dashboards (65% in 2024). By contrast, 18% of respondents do not rely on data to monitor risks, highlighting continued room for improvement in developing more data-driven and dynamic risk monitoring practices.



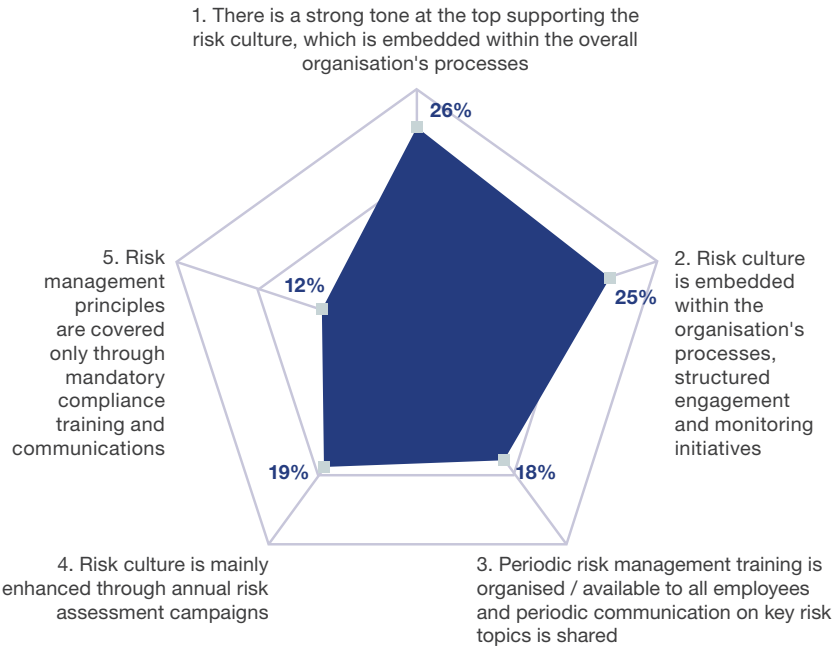
► Risk appetite framework appear to be relatively mature



Results are broadly aligned with 2024, suggesting limited progress in the formalisation of risk appetite frameworks. Around one third of Risk Managers report that their organisation has a comprehensive risk appetite framework in place, broadly stable compared with 35% in 2024. However, 17% of respondents indicate that no risk appetite has been defined, up from 13% in 2024. This slight increase highlights that risk appetite remains an area of uneven maturity, with many organisations still needing to better articulate the level and type of risk they are willing to accept to support decision-making, strategic alignment and risk governance.

► Risk culture enhancement initiatives are well established

The results show a modest improvement in the highest level of maturity for risk culture. The proportion of Risk Managers reporting a strong tone at the top, with risk culture fully embedded in the organisation’s overall processes, increased from 22% in 2024 to 26% in 2026. This suggests that some organisations are progressing towards a more mature and integrated risk culture. A further 25% of respondents report that risk culture is embedded through structured engagement and monitoring initiatives, broadly stable compared with 26% in 2024. However, around half of respondents remain at lower levels of maturity, indicating that risk culture is still unevenly embedded across organisations and that further efforts are needed to move from awareness and initiatives to sustained behaviours and decision-making practices.



Key takeaways

Key takeaways

The 2026 Global Risk Manager Survey highlights an increasingly interconnected and complex risk landscape. Macro trends such as geopolitical instability, cyber threats, AI transformation, regulatory complexity and climate change are multi-layered, driving the need for more sophisticated and tech-enabled risk management approaches as well as more agile corporate responses.

It has also highlighted a profession in transformation, with new opportunities to contribute to organisational resilience and value creation. Boards and Risk leaders that are able to navigate the risk landscape effectively can support stronger outcomes through better decision making, responsible AI and tech adoption, more effective cost control, and greater stakeholder trust.

Four key actions can help Risk Managers and their organisations strengthen preparedness and resilience:



1. Mind the gap – understand what risk data is available in your organisation’s ecosystem, including how this is collated, who validates it, who receives it and what decisions it drives. As organisations become increasingly connected, consistent, transparent risk data is important in helping to avoid blind spots.



2. Strengthen collaboration – assess how the lines of your organisation are working together, including risk, control, compliance, investor relations, insurance, and internal control functions. Are they all pulling in the same direction? Can Risk Managers take the lead in developing a plan for better cross-functional engagement and coordination?



3. Connect strategy and resilience – strategic risk and operational resilience are sometimes considered separately but are two sides of the same coin : operational resilience is a key strategic priority. Ensure that resilience is built into strategy, with processes to stress-test it and mechanisms for crisis management, including ‘what if’ simulations to assess the organisation’s ability to absorb shocks or deal with unintended outcomes arising from new technologies such as AI, which is both a strategic priority and an operational risk.



4. Encourage innovation – review your risk appetite and innovation culture, particularly around AI and tech adoption. Are there opportunities to pilot new ways of analysing, quantifying or reporting risk data with AI, or to remove manual steps? A culture that supports controlled experimentation and learning is important for Risk Managers to transform. Each pilot should be linked to a measurable value outcome, such as cost reduction, greater transparency, more insightful reporting or better decision-making.



in partnership
with



Contact us for further information

enquiries@ferma.eu

www.ferma.eu

The findings presented in this report are based on survey responses and do not constitute professional advice. Readers should not act on this information without obtaining specific professional guidance tailored to their circumstances.

Copyright © 2026 FERMA, in partnership with PwC
PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only and should not be used as a substitute for consultation with professional advisors.