The new shape of risk

How insurance CROs are leading in a world defined by speed, volatility and interconnection

Third annual EY/IIF global insurance risk management survey

The better the question. The better the answer.
The better the world works.

EY
Shape the future with confidence

IIF Institute of International Finance

Executive summary

The world of risk has fundamentally changed. The patterns that once guided risk management no longer hold. Insurance chief risk officers (CROs) are navigating a NAVI environment where shocks arrive faster, spread further and compound more often:

- **Nonlinear:** risks do not build gradually; they erupt and trigger tipping points
- **Accelerated:** decision windows are shorter and response times matter more
- **Volatile:** direction shifts quickly, testing organizational agility
- **Interconnected:** a single disruption can cascade across technology, third parties, operations and markets

Those dynamics were on full display in 2025. Inflation eased but stayed elevated; geopolitical fragmentation persisted; and macroeconomic volatility continued to shape decision-making.

Non-life carriers faced heightened natural catastrophes, climate risks and social inflation. Life insurers benefited from improved investment yields but contended with lapses, guarantees and aging populations. Across the sector, strong capitalization and liquidity, alongside the expanding use of AI and advanced analytics, reflect the industry's underlying resilience. At the same time, greater reliance on these technologies introduces new and evolving risks that organizations must proactively manage. Meanwhile, supervisors increased their focus on private credit, climate and cyber as emerging systemic risk channels.

In this environment, the CRO role becomes more central — not only to identify risk, but to drive timely decisions under uncertainty. CROs are expected to embed risk management into business decision-making, draw on more real-time risk insights and establish clear escalation paths to quickly address emerging risks and safeguard the organization.

The third annual EY–IIF (Institute of International Finance) global insurance CRO survey reveals how this shift is reshaping CRO agendas, operating models and investment priorities. This year's findings highlight the ongoing evolution of the CRO role, which is both reinforcing risk discipline and empowering the organization to act with confidence on growth and transformation decisions:

- Cyber remains the top, near-term priority, accelerated by geopolitical risks, with rising expectations for measurable resilience in prevention, containment and recovery
- AI and automation have moved from experimentation to operating model impact, becoming a headline priority in risk technology roadmaps alongside stronger governance and controls
- Operating models are shifting from capacity to capability, as risk teams redesign workflows and skill mix to focus on insight, judgment and partnership with the business

This report brings together insights from insurance CROs across geographies, business models and organizational sizes, comparing current and prior-year results, to highlight what is changing and what is proving durable. It also examines how CROs are strengthening foundations, modernizing capabilities and repositioning risk management to operate at the pace today's environment demands.

CROs who embrace NAVI principles will position their organizations for readiness, resilience and sustained confidence amid an evolving risk landscape.

Contents

Key takeaways

1 Cyber risk is expanding across multiple dimensions of enterprise exposure

Cyber is no longer a standalone technology issue; it is a complex, integrated risk with strategic, operational, geopolitical and reputational implications.

Eighty percent of insurance CROs rank cyber among their top-five risks, driven by escalating threats from geopolitics, third-party exposure and AI. Nearly four out of five CROs (78%) cite cybersecurity threats and digital hostilities as the most significant geopolitical impact on their organizations.

As one CRO reflected on this evolving risk landscape, "Our risk priorities have fundamentally shifted in the past five years; we now approach geopolitical risks with more structured scenario analysis and involve senior management in these discussions."

Insurers are responding by proactively strengthening cyber defenses and resilience plans, with heightened attention on third-party cyber risk, phishing and business email compromise, data protection and cyber resiliency. Board engagement continues to rise, with greater scrutiny on key risk indicators (KRIs), testing results, incident insights and service continuity. The industry standard is evolving: the ability to prevent, contain and recover from cyber incidents is now seen as a core measure of enterprise trust and stability, not just a regulatory requirement.

CROs must continue to treat cyber as a multidimensional enterprise risk, ensuring clear ownership, governance and monitoring across third-party exposure, data protection, fraud, social engineering and resiliency. The focus must move beyond risk identification to demonstrating robust prevention, impact resistance and rapid recovery, while preparing for new disruptions from emerging technologies, nation-state actors and weaknesses in traditional infrastructure.

> "What CROs say:
>
> The growing complexity of IT security and third-party risk is demanding more of our attention and resources than ever before.

78%

of CROs cite cybersecurity threats and digital hostilities as the **most significant geopolitical impact** on their organizations.

Jump to contents

2 Advanced technologies are shifting from experimentation to full incorporation within the operating model

Organizations are rapidly shifting advanced technologies from pilot projects to core operations. To keep pace, they are developing robust governance and risk frameworks focused on oversight, accountability and adaptability. As these frameworks mature, firms are deploying AI-driven tools such as chatbots, large language models, document and legal review solutions, and cyber analytics to enhance risk management. Beyond current applications, expansion is anticipated across fraud detection, underwriting and pricing. Many insurers are also evaluating whether and how digital assets may affect products and claims payments, making dynamic governance structures and flexible risk management approaches increasingly critical.

As adoption of advanced technologies accelerates, organizations are adapting their governance and risk frameworks. Currently, 62% of firms have enterprise AI governance frameworks in place and 55% have formal generative AI (GenAI) policies, reflecting increased attention on model risk, data quality and accountability.

Despite progress, barriers remain — skill gaps, data limitations, budget constraints, regulatory complexity and evolving supervisory expectations — reinforcing the need for clear ownership, cross-functional coordination and scalable controls.

The trend is clear: digital transformation is fundamentally reshaping both risk management and broader business operations. As adoption expands, CROs and business leaders face a dual challenge: leveraging AI to strengthen oversight and risk management, while also navigating AI-driven risks that can amplify cyber, data, technology and talent pressures across the enterprise. Addressing these challenges requires both innovation and disciplined governance, ensuring controls and explainability scale effectively with each new use case.

CROs should work to integrate advanced technologies into existing risk and governance models, rather than treating them as standalone initiatives. Governance frameworks should address model risk, data quality, accountability and third-party dependencies, while remaining flexible enough to evolve with expanding use cases and regulations. CROs should invest in skills, data foundations and cross-functional coordination so transformation is controlled, explainable and aligned with enterprise strategy — building trust and resilience as adoption scales.

> “
> What CROs say:
>
> The main challenge in adopting AI is not the technology itself, but ensuring the first line develops effective governance and the board sets a strategy for managing new risks.

Jump to contents

3 The risk operating model is changing as workforce demands intensify

Risk operating models are transforming — less through headcount growth and more through redesign of workflows, skill mix and decision cadence. AI and automation are driving this shift (62%), alongside regulatory demands (39%) and business growth (34%). As routine tasks are automated, adaptability, digital acumen and communication become more critical for risk professionals.

CROs recognize that AI will enable teams to accomplish more without expanding headcount. As one CRO noted, "When technology is no longer a barrier, qualities like curiosity and creativity become even more essential for our teams."

This shift is also reshaping decision-making. Many organizations are moving from calendar-based reviews to more data-driven, trigger-based models, helping risk teams respond faster and more efficiently. Risk's role in enterprise initiatives is expanding, with less focus on volume and more on insight, judgment and partnership with the business. Embedding risk management into business processes, with clear decision rights, supports agility while maintaining control as complexity increases.

CROs should leverage AI and automation to reduce routine tasks, enabling teams to focus on deeper insights and strategic collaboration. Prioritizing adaptability, digital fluency and soft skills will help teams add greater value in today's fast-paced environment. Embedding the second line into strategic decision-making reinforces risk's value as a trusted advisor, rather than a volume-driven control function.

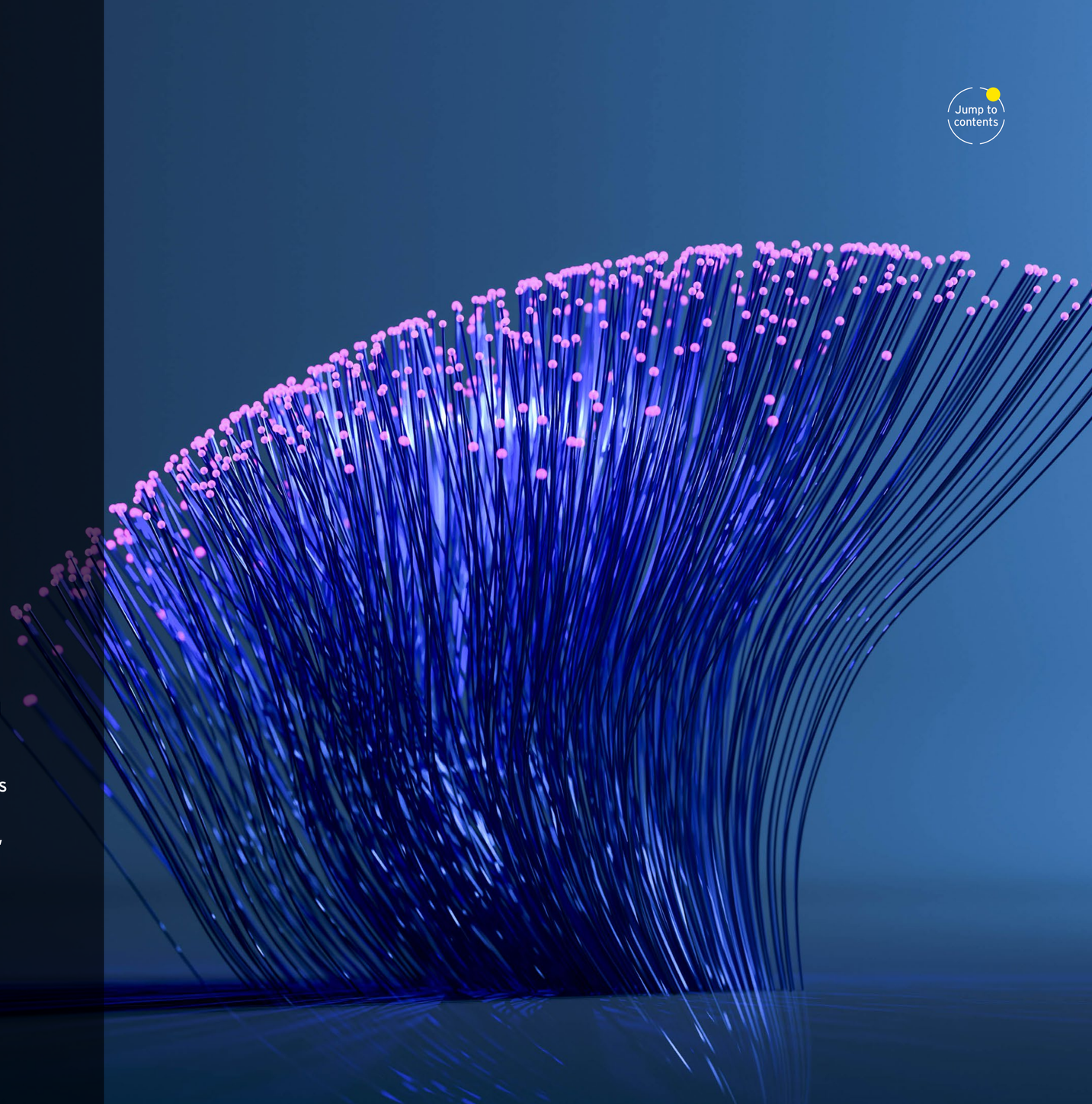
> "What CROs say:
>
> When technology is no longer a barrier, qualities like curiosity and creativity become even more essential for our teams.

Jump to contents

CHAPTER 1

The CRO agenda: risk priorities and planned enhancements

Cybersecurity remains the defining near-term priority for insurance CROs, consistently ranking as the top risk across the past three survey cycles (2023-2025). This sustained prominence reflects both the persistence of the threat environment and rising expectations from boards and regulators for resilience, defensibility and operational stability. Meanwhile, the sharp rise in strategic risk highlights CROs' growing awareness of the critical need to navigate long-term uncertainties and market shifts, requiring heightened attention going forward.



Near-term risk priorities — cyber leads, while strategic and interconnected risks rise

Figure 1: Over the next 12 months, what are the top five risks that will require the most attention from the CRO?

Beyond cyber, the broader CRO agenda has remained largely stable across third-party risk, regulatory- and compliance-related risks risk and core financial exposures (credit, market and interest rate risk). This pattern suggests CROs are managing technology-driven threats alongside more traditional balance sheet and market risks — often in combination rather than isolation.

Comparing risk priorities: Insurance vs. banking

Insurance markets are evolving with complex product innovation, sidecars and increased private-equity involvement, driving more sophisticated, capital-efficient and interconnected operating models. In contrast, banking — especially among global systemically important banks (G-SIBs) and the largest institutions — is accelerating strategic planning around digital assets like tokenization, smart contracts and digital currencies.

While cybersecurity tops the risk list for both sectors, it remains a greater concern in banking (86% vs. 80%). Digital fraud (59% vs. 25%) and data risks (41% vs. 25%) also weigh more heavily on banking CROs. Meanwhile, insurers prioritize strategic risk more highly (44%, second place) compared to banking (33%, eighth place), with market risk ranking in insurers' top five but falling outside banking's top 10.

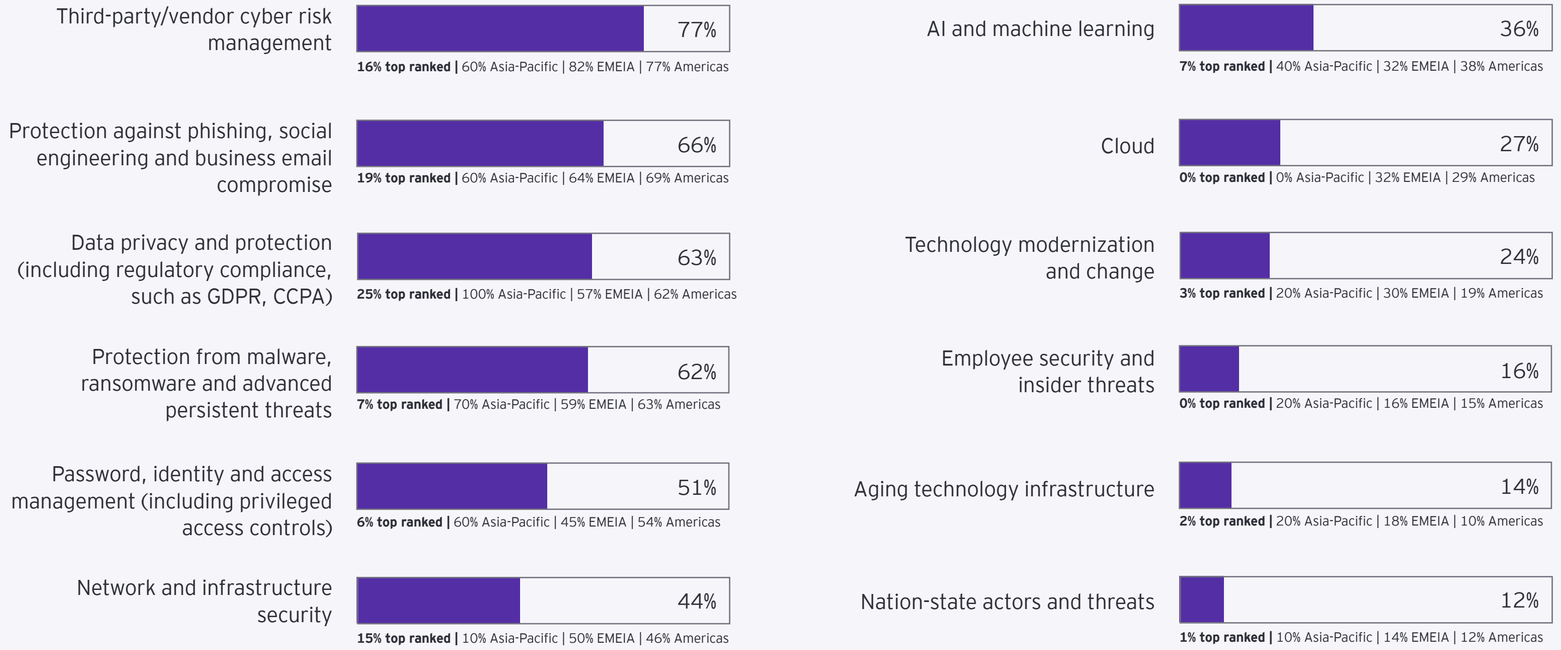
Cyber – risk priorities are shifting toward data, social engineering and third-party exposure

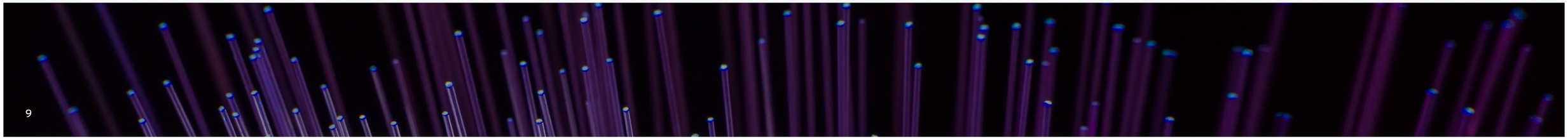
Jump to contents

CROs continue to describe cyber risk as multidimensional, with emphasis on different aspects of exposure and control depending on the region. This year's results indicate that data privacy and protection (including regulatory compliance) is the most frequently top-ranked cyber dimension, followed by protection against phishing and third-party/vendor cyber risk management.

Regional differences also stand out. In the Americas and APAC, cyber risk is more frequently framed through technology resilience, control effectiveness and data protection, while in EMEIA, it is more closely linked to regulatory oversight and third-party obligations.

Figure 2: Which aspects of cyber risk are most important to your organization?





What is shifting most – third-party dependency risk

The most notable shift in the CRO agenda over time is the rise of third-party risk as a persistent top-tier concern. This highlights growing recognition of dependency risk across extended value chains – particularly as operational resilience requirements, outsourcing oversight and vendor concentration concerns increase. Regional patterns suggest EMEIA and APAC place heightened focus on outsourcing, operational resilience and vendor concentration, while in the Americas, third-party risk is increasingly viewed through a technology and cyber lens tied to data access, control automation and vendor governance.

> “
> What CROs say:
>
> The CRO’s evolving role as a strategic advisor depends on balancing true independence with deeper engagement across the business and senior leadership.

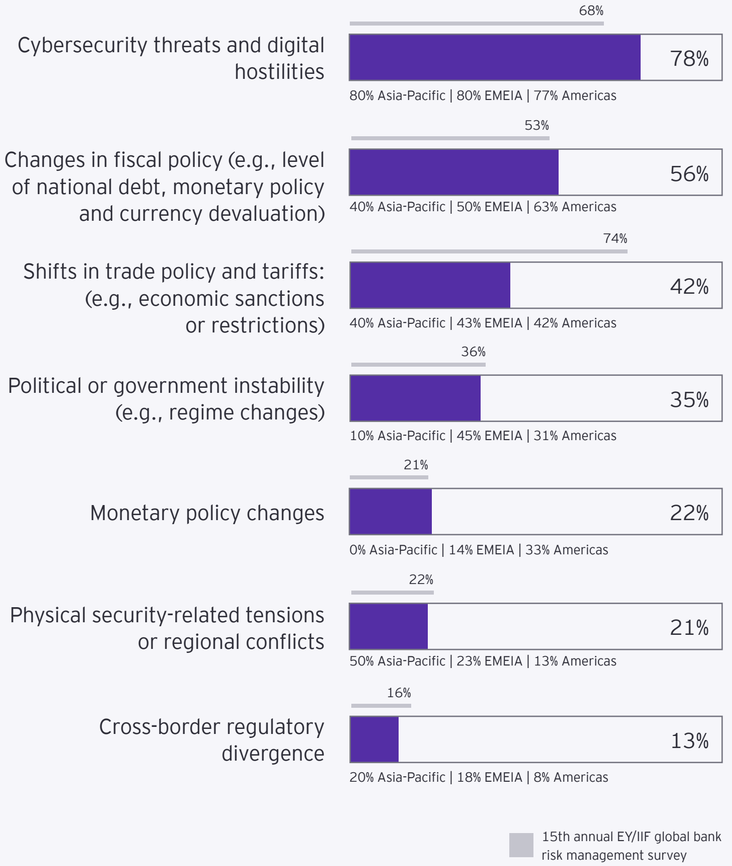
Geopolitical risk – cyber hostilities lead, followed by fiscal and trade policy channels

Jump to contents

Geopolitical and macroeconomic concerns remain prominent, with cybersecurity threats and digital hostilities far outpacing other factors (78% overall). The next tier of concerns centers on fiscal policy changes (56%) and trade policy and tariffs (42%), with notable regional variation across political instability, monetary policy and physical security tensions.

The current macroeconomic and geopolitical environment is putting significant pressure on the insurance industry by amplifying both financial and operational risks. Slower and uneven global growth, persistent inflation and tariff-driven disruptions are increasing market volatility, raising capital costs and adding uncertainty to claims patterns – especially in trade-exposed and globally connected lines. At the same time, geopolitical fragmentation, including sanctions, protectionist policies and diverging regulations, is complicating cross-border underwriting, raising compliance costs and reducing the diversification benefits insurers traditionally rely on. These forces, combined with escalating state-driven cyber activity, are reshaping risk profiles across underwriting, investments and operational resilience, aligning closely with why CROs view fiscal policy shifts, trade tensions and cyber hostilities as the most significant cross-border risks.

Figure 3: What are the top impacts from potential geopolitical risks that your organization anticipates will pose the greatest risk in the next 12 months?



Planned enhancements to risk management

Financial risk management enhancements remain anchored in **core quantitative disciplines**, including risk appetite/limits and stress testing/scenario analysis.

Jump to contents

Planned enhancements over the next 12 months reinforce a shift toward stronger infrastructure and integration across both financial and nonfinancial risk management. Financial risk management enhancements remain anchored in core quantitative disciplines, including risk appetite/limits and stress testing/scenario analysis. In nonfinancial risk management, risk technology continues to grow as the leading priority, alongside controls, governance, operating model and, importantly, talent-related enhancements. Overall, the data points to greater focus on infrastructure, integration and the critical role of human capital, rather than incremental, siloed improvements.

Figure 4: What key enhancements is your organization planning to make to its financial risk management capabilities over the next 12 months as part of business-as-usual (BAU) risk management?

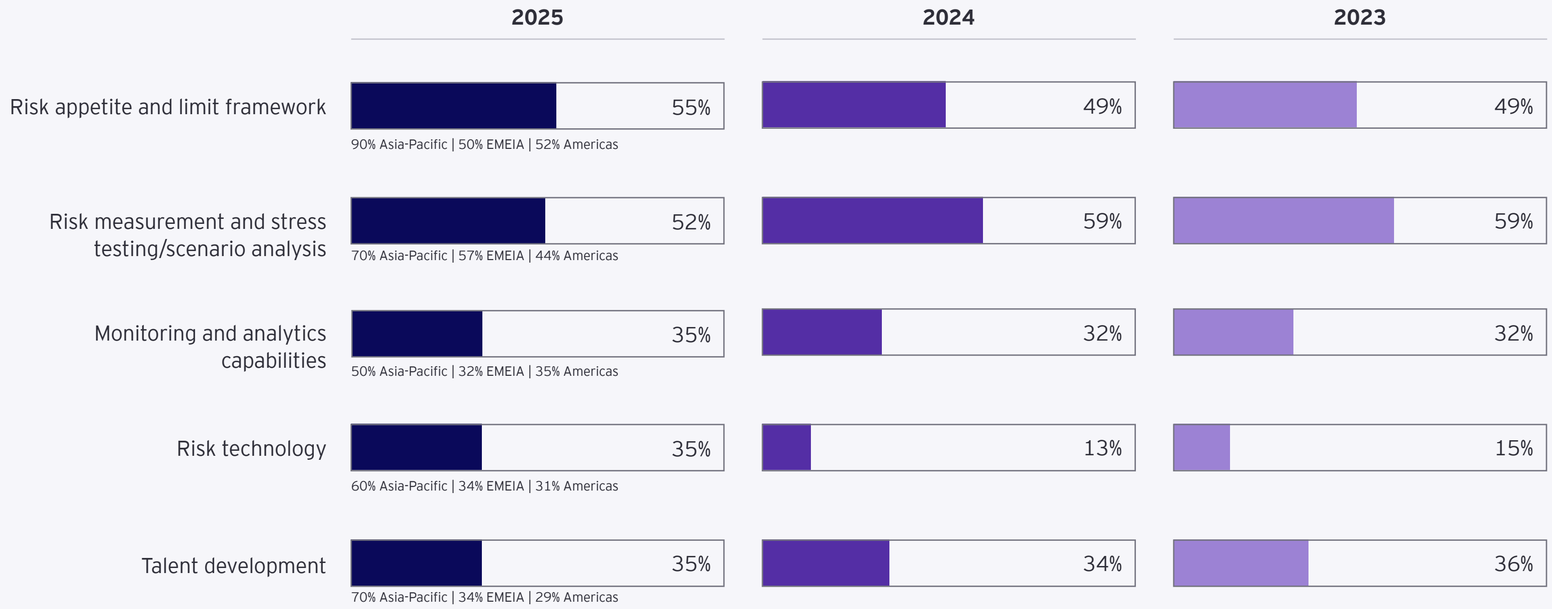
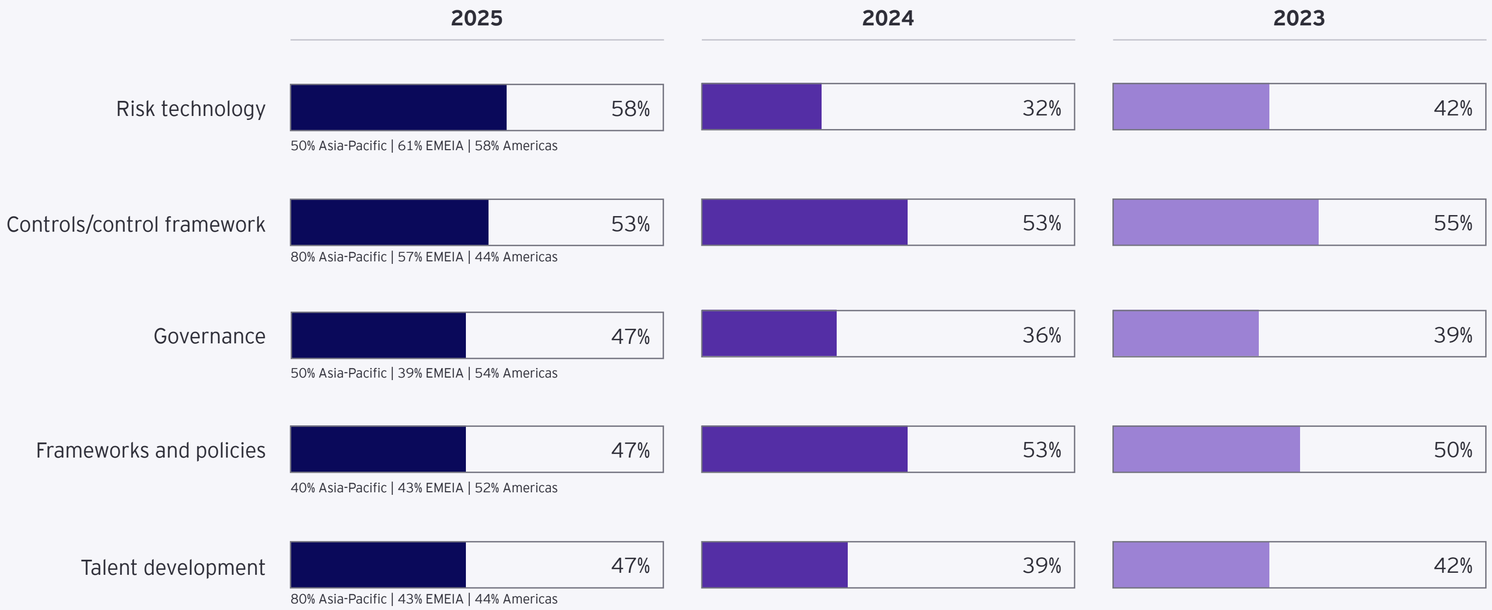
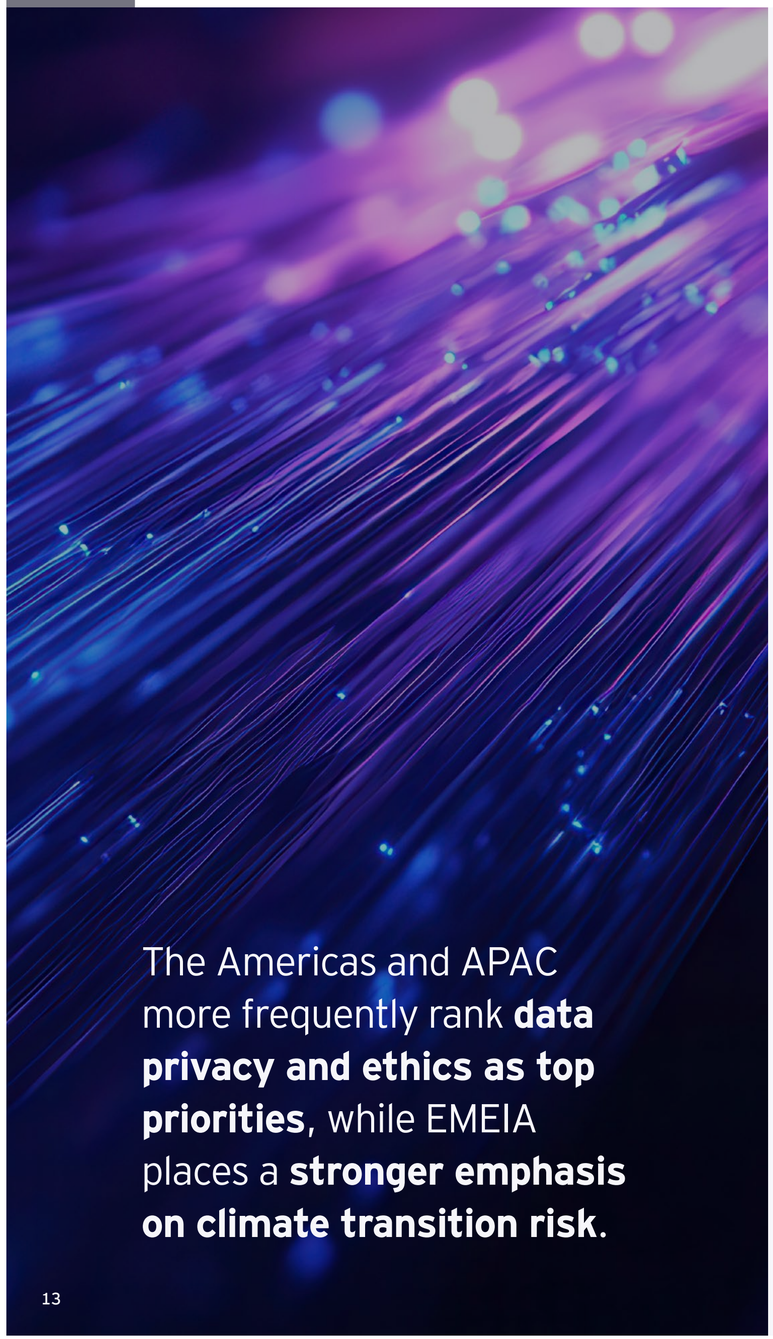


Figure 5: What key enhancements is your organization planning to make to its nonfinancial risk management capabilities over the next 12 months as part of BAU risk management?



Jump to contents

In nonfinancial risk management, **risk technology** continues to rise as the leading priority, alongside **controls, governance, operating model** and importantly, **talent** related enhancements.

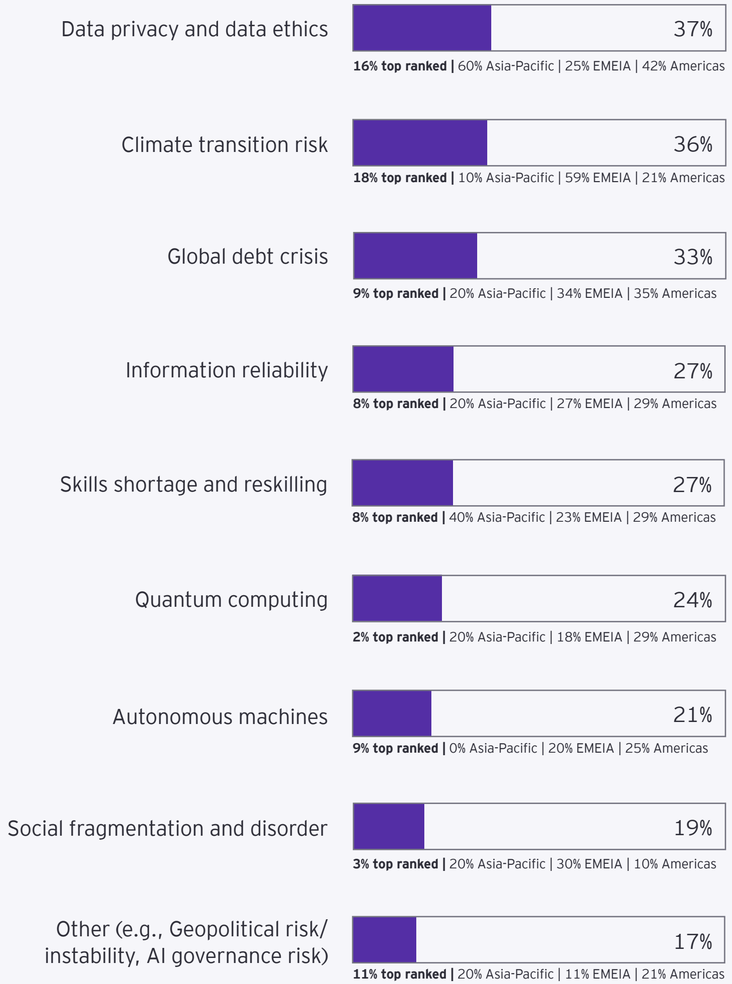


Emerging risks – longer horizon forces rise in importance

Looking five to 10 years ahead, CROs continue to prioritize a durable cluster of emerging risks, including climate transition risk, data privacy and ethics, and global financial stability. However, regional distinctions persist, as the Americas and APAC more frequently rank data privacy and ethics as top priorities, while EMEIA places a stronger emphasis on climate transition risk. These patterns suggest increasing attention to longer-horizon structural forces – transition, ethics and trust, and disruptive technologies – that are likely to reshape the CRO agenda over time.

Jump to contents

Figure 6: What emerging risks do you anticipate will significantly shape and influence the strategic agenda of the CRO over the next five to 10 years?

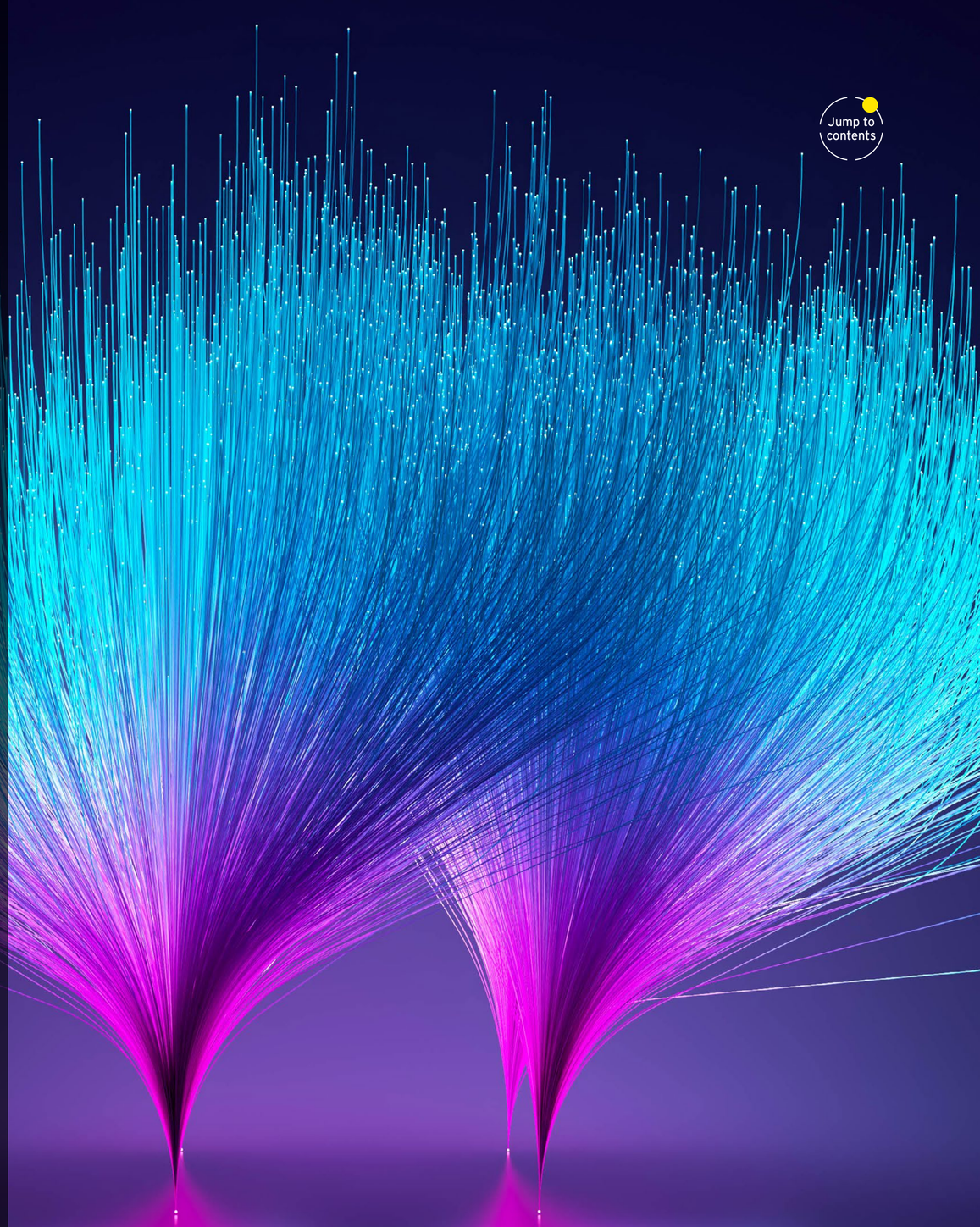


CHAPTER

2

Technology and risk transformation: from foundations to AI at scale

Risk management technology priorities over the next three to five years are increasingly defined by a heightened conviction and quickening pace of execution. Over the past three years, CROs' technology roadmaps have remained focused on a consistent set of investments: enterprise governance, risk and compliance (GRC) platforms, automated controls testing and AI-enabled risk solutions.

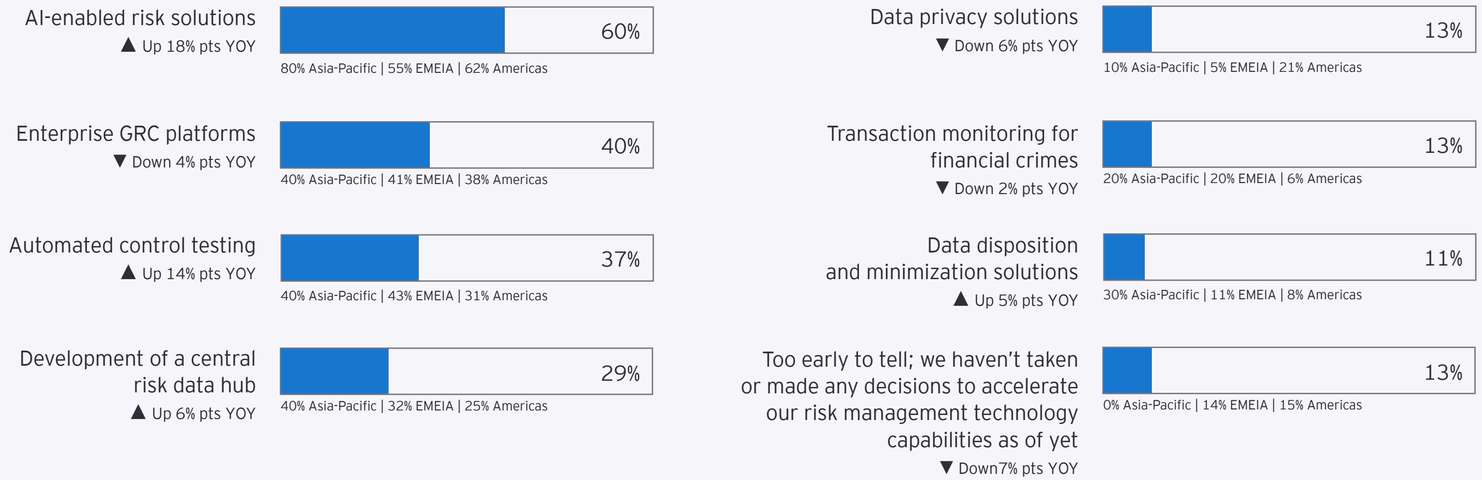


Jump to contents

Jump to contents

AI and automation are increasingly shifting risk oversight from periodic review to continuous, real-time visibility and faster, self-service risk insights for the business. As digital fluency becomes more important, CROs are leveraging technology to strengthen insights, sharpen decision-making and support scalable risk management capabilities.

Figure 7: What are your organization's top priorities in risk management technology solutions and capabilities over the next three to five years?



CROs are leveraging technology to **strengthen** insights, **sharpen** decision-making and **support** scalable risk management capabilities.

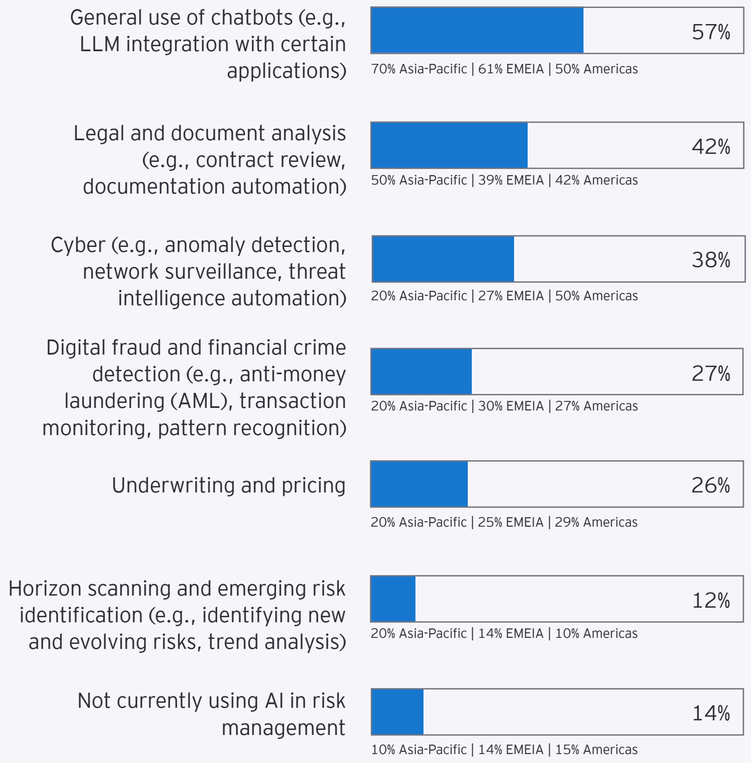
Overall direction is consistent across regions, but adoption and execution constraints vary. APAC respondents are the most assertive on AI adoption, with the strongest prioritization of AI-enabled risk solutions. The Americas follow closely, pairing AI priorities with automated control testing and enterprise GRC. EMEIA adoption is more measured and is often framed around governance, compliance and integration with existing control frameworks.

In this year's survey, AI-enabled risk solutions emerge as the clear headline priority across regions. Enterprise GRC platforms remain a major focus, automated controls testing remains prominent, and investment in centralized risk data hubs continues to grow — reinforcing the importance of data and controls alongside AI.

Commitment to improving risk technology is also strengthening. The share of respondents indicating it is "too early to tell" declined from 20% in 2024 to 13% in 2025, signaling a shift from experimentation toward clearer roadmaps and investment decisions.

Current patterns of AI use reinforce this shift. Early adoption is focused on fraud detection and monitoring. By 2025, AI-style enablement — chatbots and document/legal analysis — dominates across regions. APAC shows particularly high adoption in chatbots and operational risk monitoring, while the Americas and EMEIA show broader use across cyber analytics, underwriting and controls.

Figure 8: What are the most significant areas in which your organization is currently using artificial intelligence (AI) in risk management?

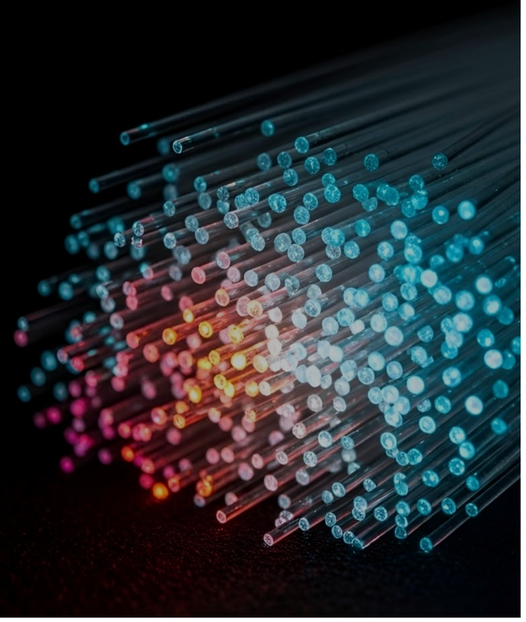


Jump to contents

"

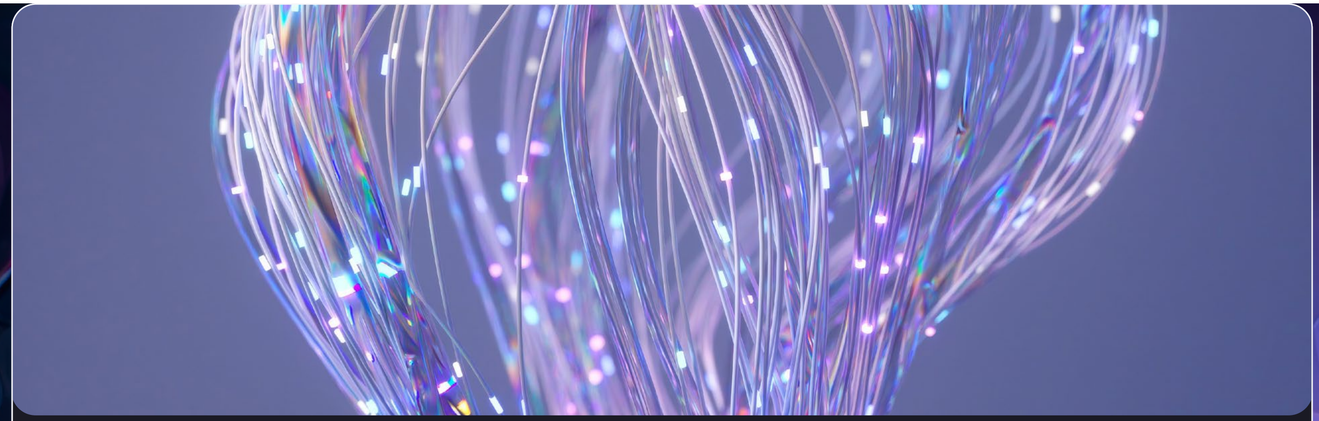
What CROs say:

While AI has marginally improved efficiency, it has not yet transformed how we work. Its main contribution is automating routine tasks, not fundamentally changing our operations.



Other research related to AI usage in financial services – including the annual study conducted by IIF-EY (see sidebar) – confirms that the business has so far realized greater value than the risk management function has in initial AI deployments. However, through our engagement with risk leaders across the financial services industry, and particularly in insurance, firms are continuing to identify new use cases to drive efficiency and shift the way traditional work has been performed.

> "What CROs say:
>
> We see AI as efficiency in the near term, with strong capabilities coming later. AI is everywhere except for the P&L right now. It provides a huge uplift in productivity and the operational side.



IIF-EY research on AI:

To put these findings in context, the latest IIF-EY Annual Survey Report on AI Use in Financial Services shows how insurers are adopting this revolutionary technology across all parts of the business, complementing our annual risk management survey. It's clear that deployments in different functions are outpacing those in risk management.

Among this year's highlights:

100%
of institutions planning changes in their AI investments are looking to increase their spending.

83%
of financial institutions (FIs) reported some level of work on agentic AI – 23% are in production, 34% are piloting and 26% are still planning.

79%
of all institutions and 100% of insurance firms said data quality was the top challenge for AI development, with data availability a very close second.

77%
of FIs use third-party platforms to address challenges (e.g., data preparation, access to training data and AI talent) and bring AI into production.

Read the full report here.

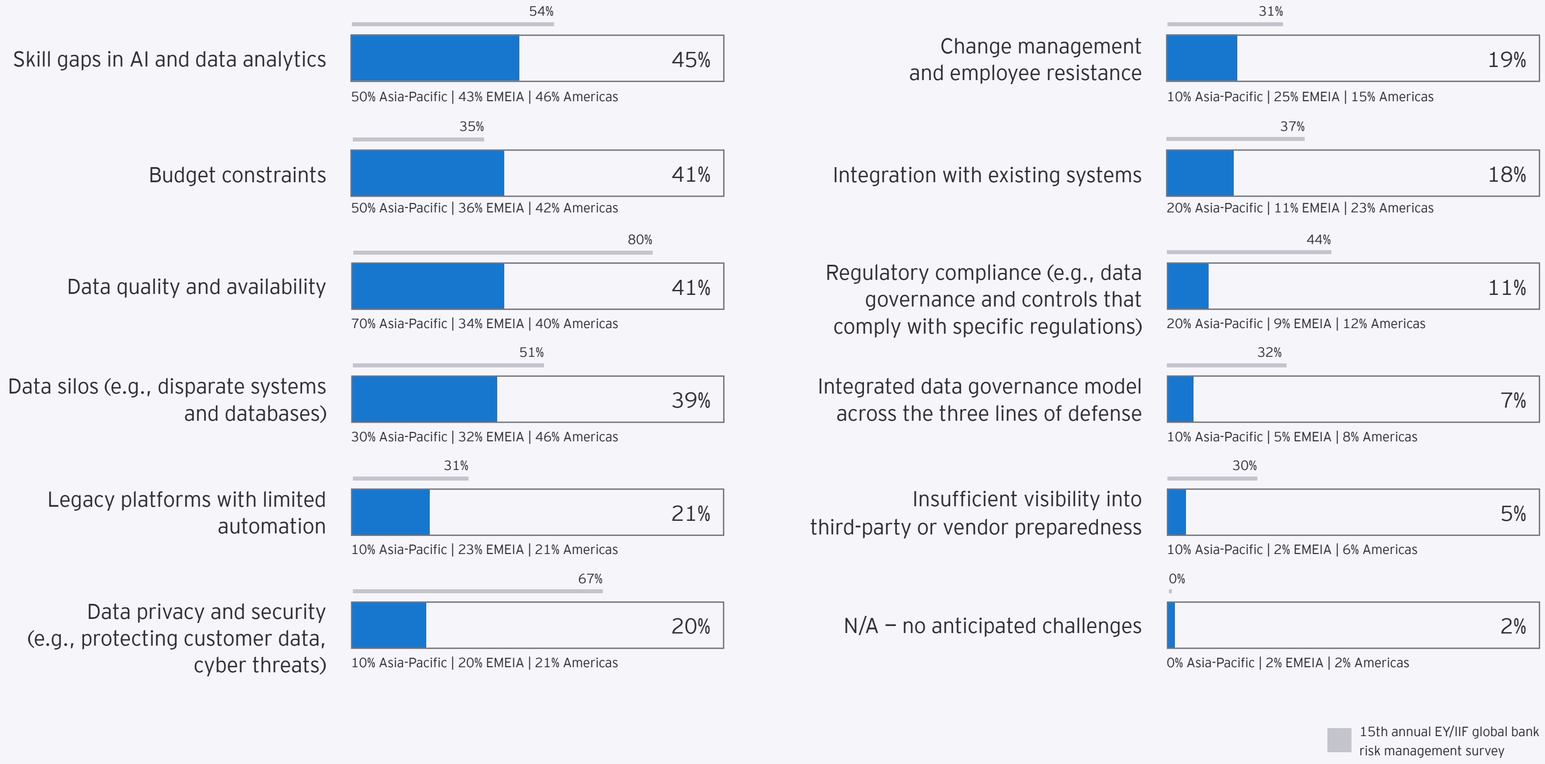
Jump to contents

Jump to contents

Barriers to scale are consistent globally. Skill gaps and data quality remain the most common constraints, while integration with legacy systems and budget limitations continue to slow adoption. These results suggest that risk technology transformation is entering a new phase. The focus is no longer solely on building foundational platforms or automating individual processes but on embedding AI as a core productivity layer supported by robust data, controls and governance. For CROs, the challenge is to ensure that this acceleration enhances insight, consistency and resilience — rather than introducing new fragmentation or unmanaged risk — as risk management capabilities scale into the next generation.

> What CROs say:
>
> AI and automation offer tremendous potential, but legacy systems and insufficient first-line governance continue to limit their impact on risk management.

Figure 9: What are the top constraints your organization faces in adopting or accelerating digital transformation (e.g., use of automation, AI/GenAI and machine learning (ML)) to support risk management practices?

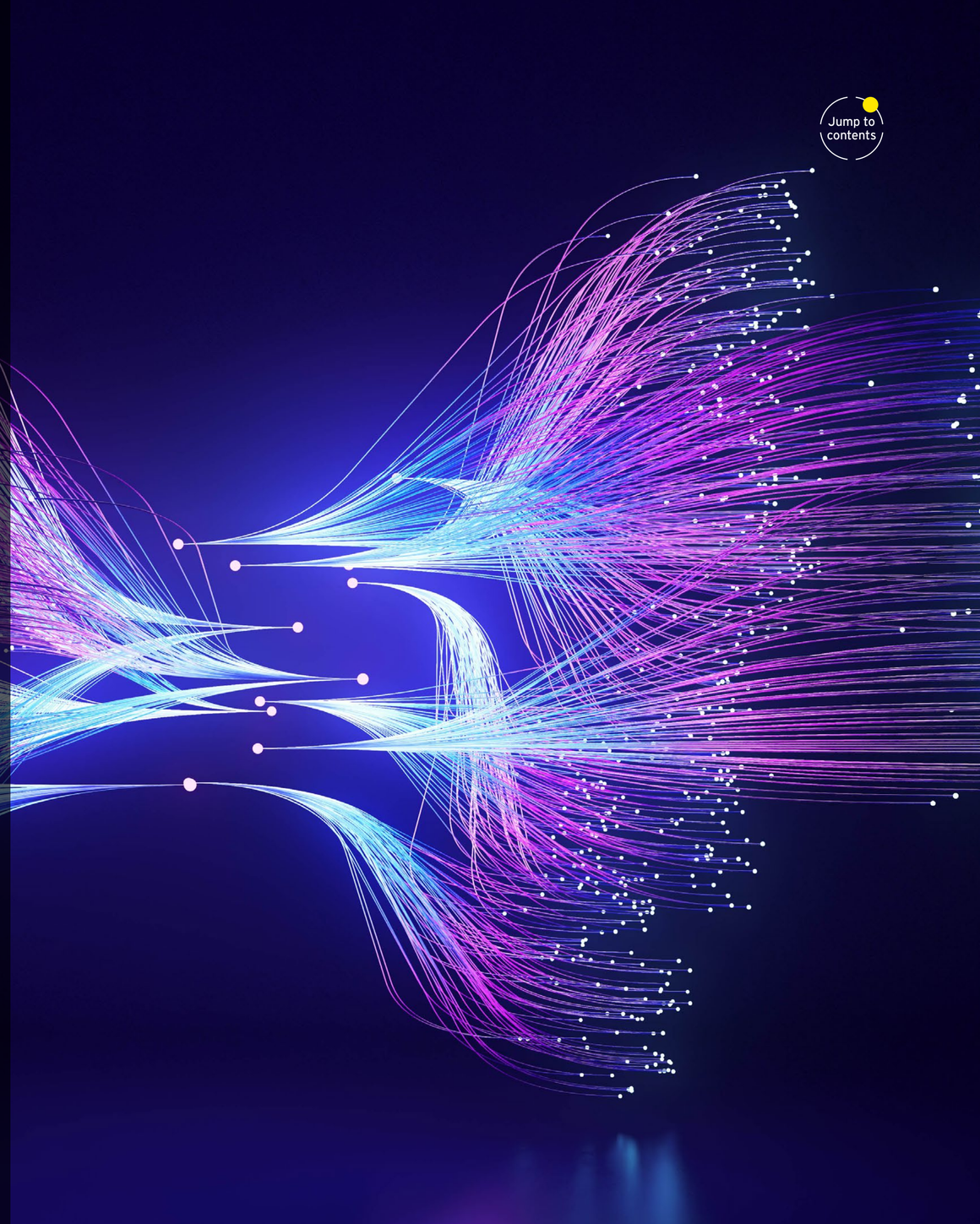


CHAPTER

3

Operational resilience: moving from capabilities to control

Operational resilience continues to rise on the CRO agenda, with a clear shift from standalone preparedness activities toward more integrated, governed resilience. Across the past three survey cycles, organizations have prioritized strengthening resilience through technology readiness, third-party dependency management and formal oversight — while changing how they structure and execute those priorities year over year.



Jump to contents

Figure 10: What level of priority would you assign to each of the following areas of operational resilience for enhancements over the next five years?

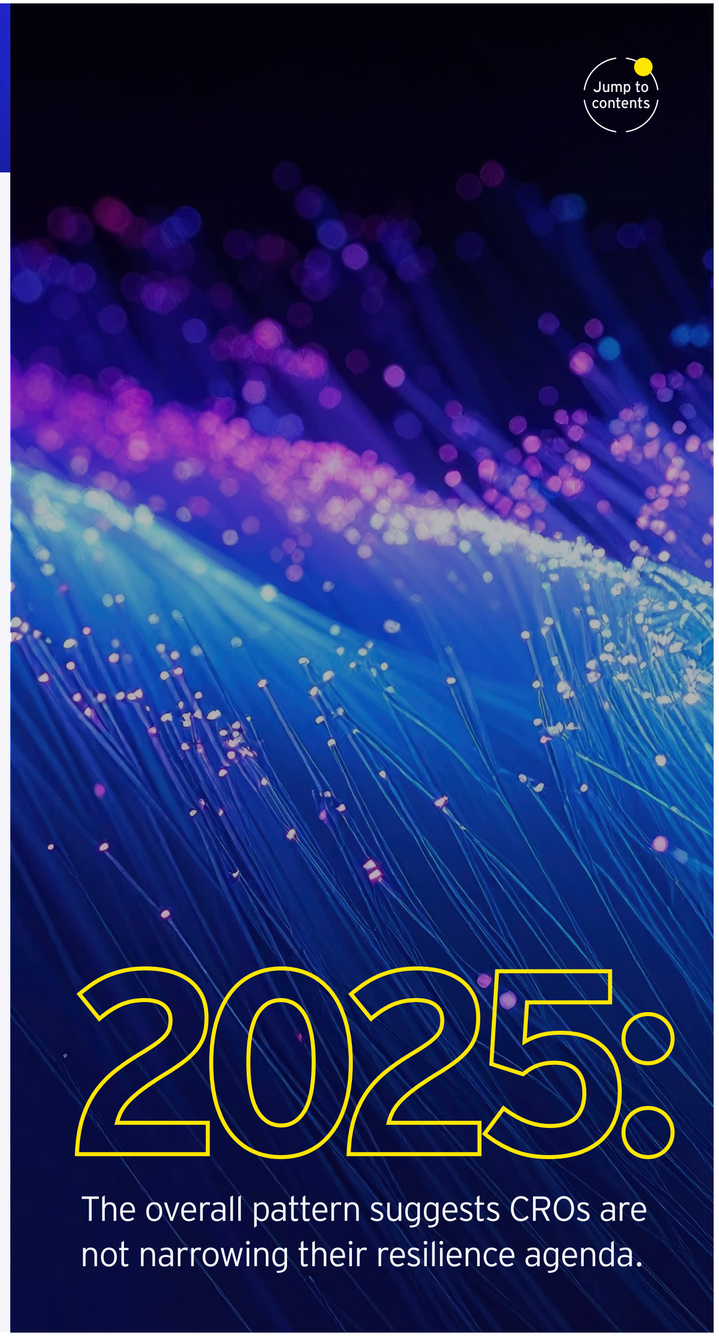
The results show a progression in emphasis:

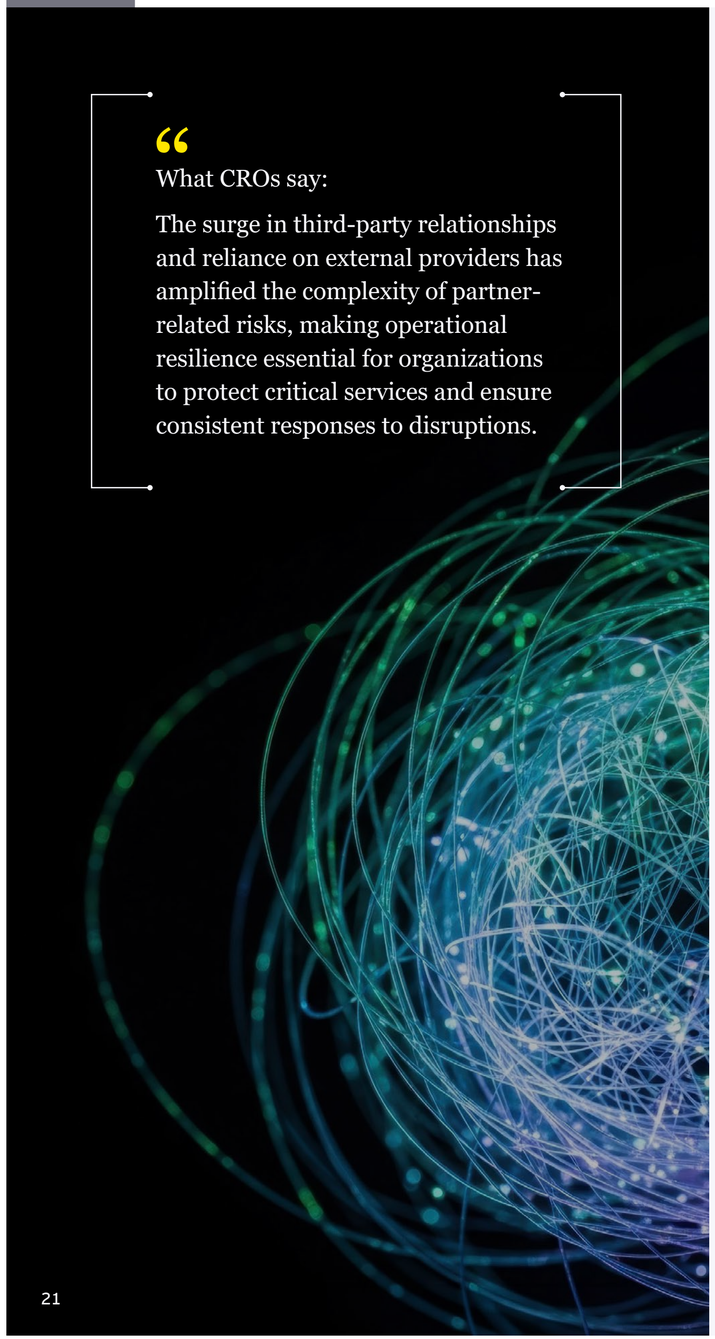
2023: resilience centered on execution levers — technology capacity and third- and fourth-party dependencies — reflecting immediate concerns about whether systems, infrastructure and external partners could withstand disruption.

2024: the focus shifted toward greater structure and accountability. Governance and oversight rose to the top, alongside cyber and critical business service frameworks, signaling stronger senior-level visibility and clearer coordination across resilience disciplines.

2025: cyber emerges as the leading resilience priority, while governance and critical business service frameworks remain high. The overall pattern suggests CROs are not narrowing their resilience agenda; they are managing cyber, governance, service continuity and third-party exposure as interconnected requirements.

Jump to contents





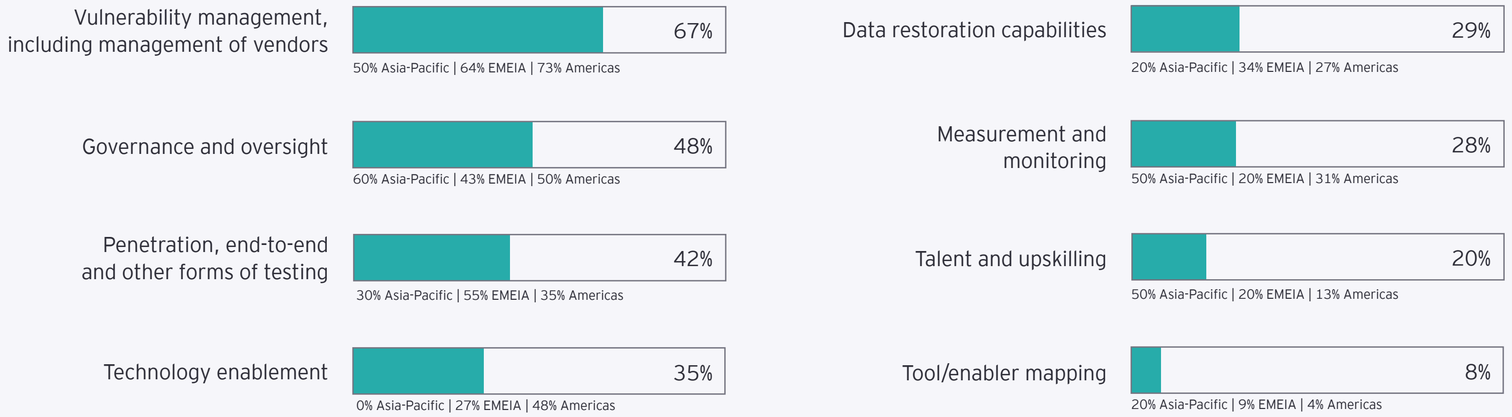
> What CROs say:
>
> The surge in third-party relationships and reliance on external providers has amplified the complexity of partner-related risks, making operational resilience essential for organizations to protect critical services and ensure consistent responses to disruptions.

Jump to contents

As resilience expectations mature, the emphasis is shifting from identifying priority areas to strengthening the capabilities that make resilience repeatable and measurable, especially across vendor ecosystems and critical services.

Vulnerability management rises as a leading capability (including vendor management), underscoring the importance of proactively identifying and addressing vulnerabilities that can cascade across cyber defenses, governance and service continuity.

Figure 11: What capabilities is your organization most focused on enhancing to address the operational resilience priority areas you identified in the previous question?



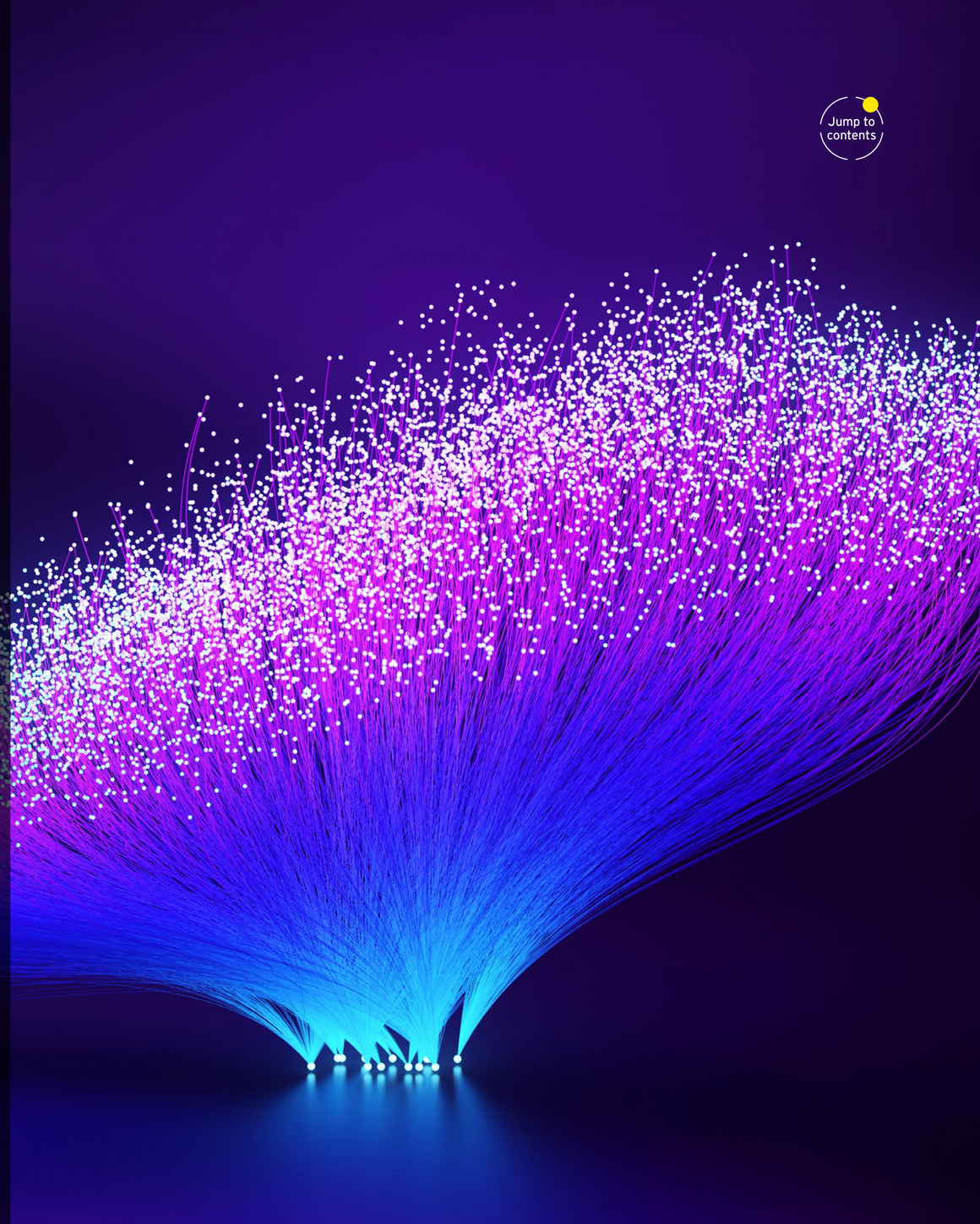
Overall, the findings point to a shift from building resilience capabilities to governing resilience as an ongoing discipline – with more structured approaches that integrate cyber, critical services and third-party dependencies to sustain trust under stress.

CHAPTER

4

Internal controls: modernizing for a tech-enabled risk environment

Insurance organizations continue to prioritize internal controls as boards and regulators raise expectations for clear, defensible evidence of control effectiveness.



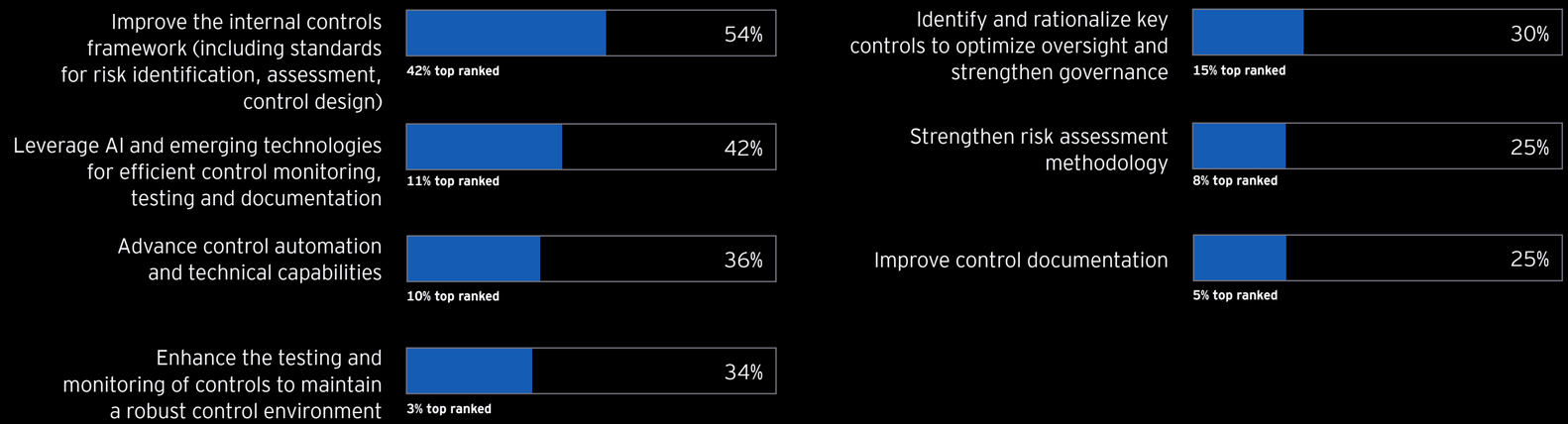
Jump to contents

Jump to contents

Over the past three years, the focus has shifted from strengthening foundational frameworks to modernizing how controls are executed, monitored and evidenced through technology and data-driven approaches:

- **2023:** standardized control frameworks, increased automation and closed execution gaps across first and second lines.
- **2024:** operationalized controls with greater emphasis on design, performance metrics, testing coordination, oversight, and early use of AI and analytics for control design and monitoring.
- **2025:** accelerated technology-enabled execution, AI adoption and greater clarity about which controls matter most and how effectively they operate. Companies also reflect the need to streamline fragmented compliance efforts due to expanding regulatory requirements.

Figure 12: What are the organization's top three priorities in the next 12 months related to enhancing the internal control environment?



> What CROs say:
>
> The rapid expansion of regulatory requirements has often resulted in fragmented compliance efforts, underscoring the need to rationalize and streamline controls.

Jump to contents

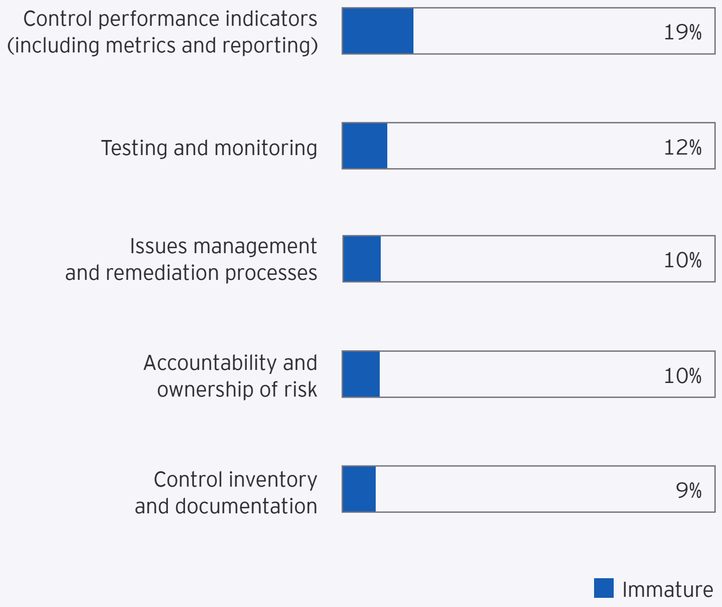
Regional patterns reinforce a common direction — toward more agile, risk-based control environments supported by automation and analytics — while highlighting different starting points and constraints:

- **Americas:** Automated control testing and AI-enabled monitoring are increasingly integrated with broader AI and data strategies, with an anticipated shift toward increased monitoring and reduced reliance on testing.
- **EMEIA:** Emphasis remains on governance, control design and defensibility under regulatory scrutiny.
- **APAC:** Control modernization is constrained less by intent than by data quality and system fragmentation.

> “
> What CROs say:
>
> The CEO’s key responsibility toward control functions is to provide light, not heat.

To execute against these priorities, organizations must understand where their internal control frameworks stand in terms of maturity and where modernization efforts will have the greatest impact. Survey responses most frequently identify gaps in control performance indicators (19%), testing and monitoring (12%), and issues management/remediation processes and accountability/ownership of risk (10% each, respectively).

Figure 13: How mature are the following components of the internal control framework?

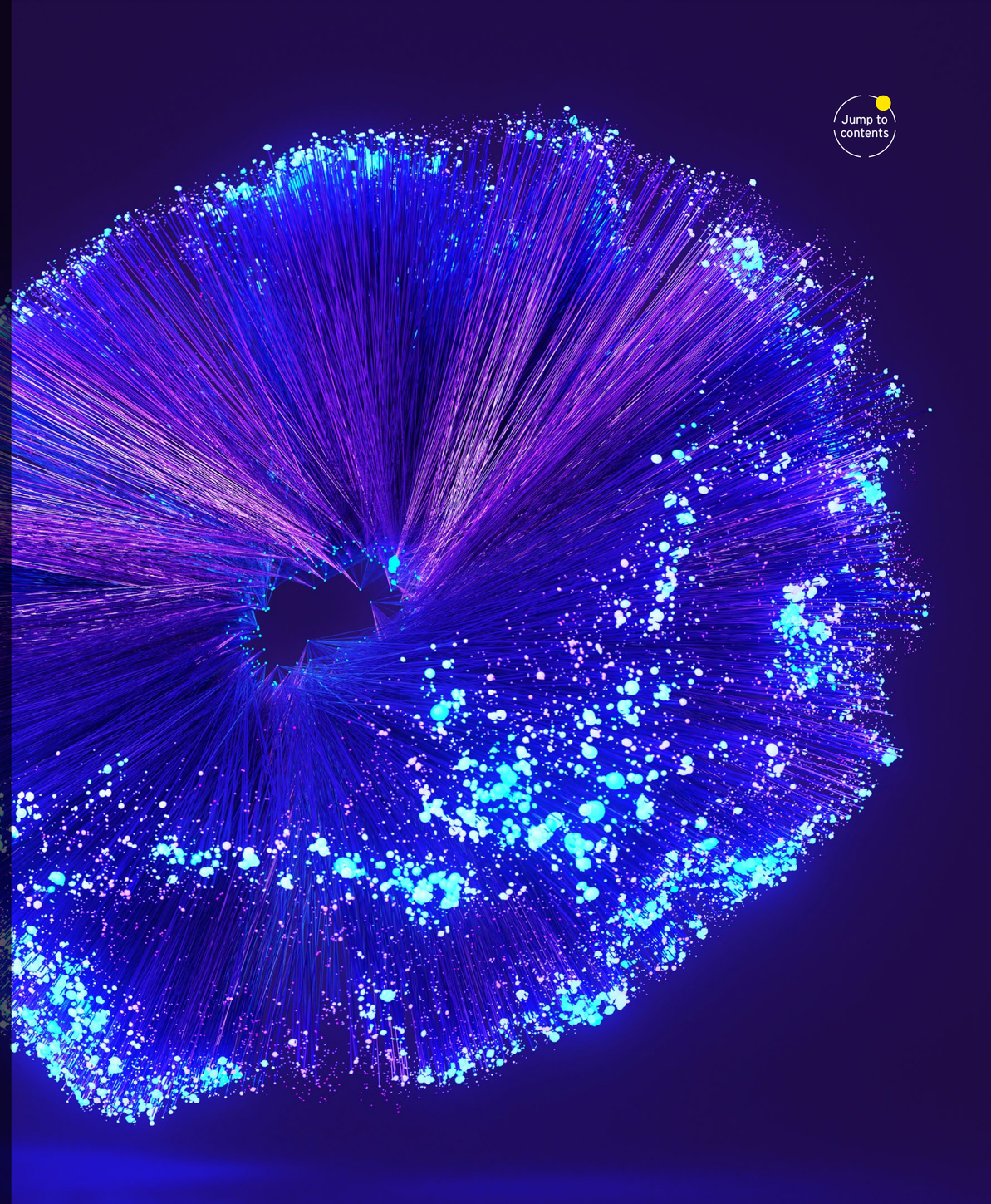


These findings point to a clear modernization agenda: strengthen the metrics and reporting that demonstrate control performance, improve testing and monitoring discipline and close the loop on remediation through clearer ownership and more consistent issue management. Targeted investment in these areas supports a more efficient, tech-enabled control environment that increases coverage and delivers timely insight into control effectiveness.

CHAPTER 5

Skills and talent: evolving the digitally fluent risk workforce

Survey findings suggest risk management teams are entering a period of more stable headcount, with productivity gains increasingly driven by technology, automation and evolving role design rather than broad hiring expansion.



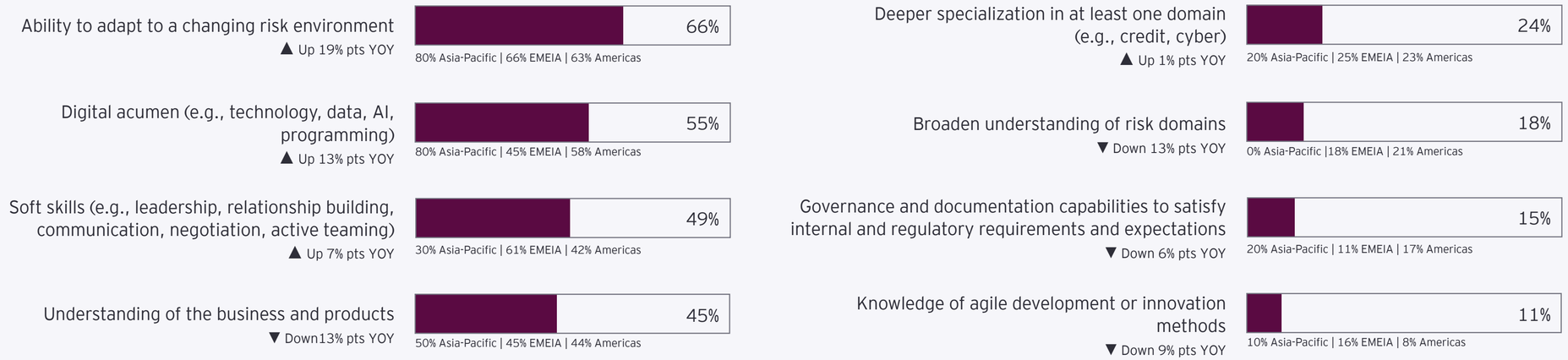
Jump to contents

Jump to contents

Skill priorities – adaptability and digital acumen lead

CROs are prioritizing a targeted set of capabilities to keep pace with a more technology-driven risk environment. Adaptability (66%) and digital acumen (55%) lead, alongside continued emphasis on soft skills and an understanding of the business – reflecting a shift toward more strategic risk partnering as automation expands.

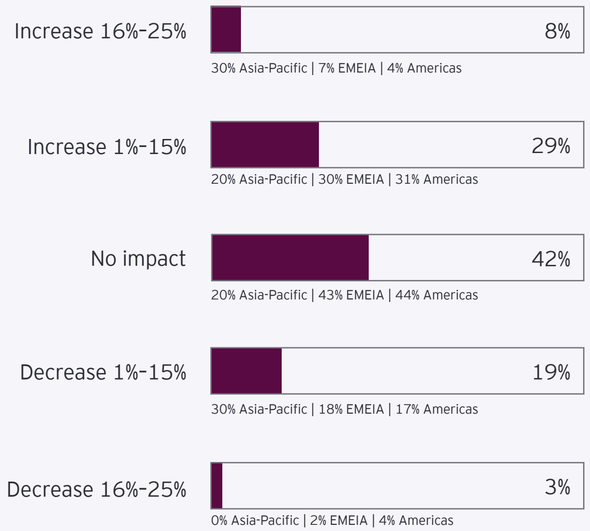
Figure 14: Over the next three years, what are the top skill sets your organization believes risk management resources should prioritize to better manage risk?



Staffing outlook – stabilization with selective growth

Compared with prior years, respondents anticipate less hiring in the second-line risk function. Close to half (42%) expect no change in full-time equivalents (FTEs) (up from 27% last year), while fewer anticipate growth compared to last year (37% vs. 65%).

Figure 15: Expected change in the number of FTEs in risk management (second line) over the next three years



Drivers behind staffing changes – automation plus regulation, growth and strategic initiatives

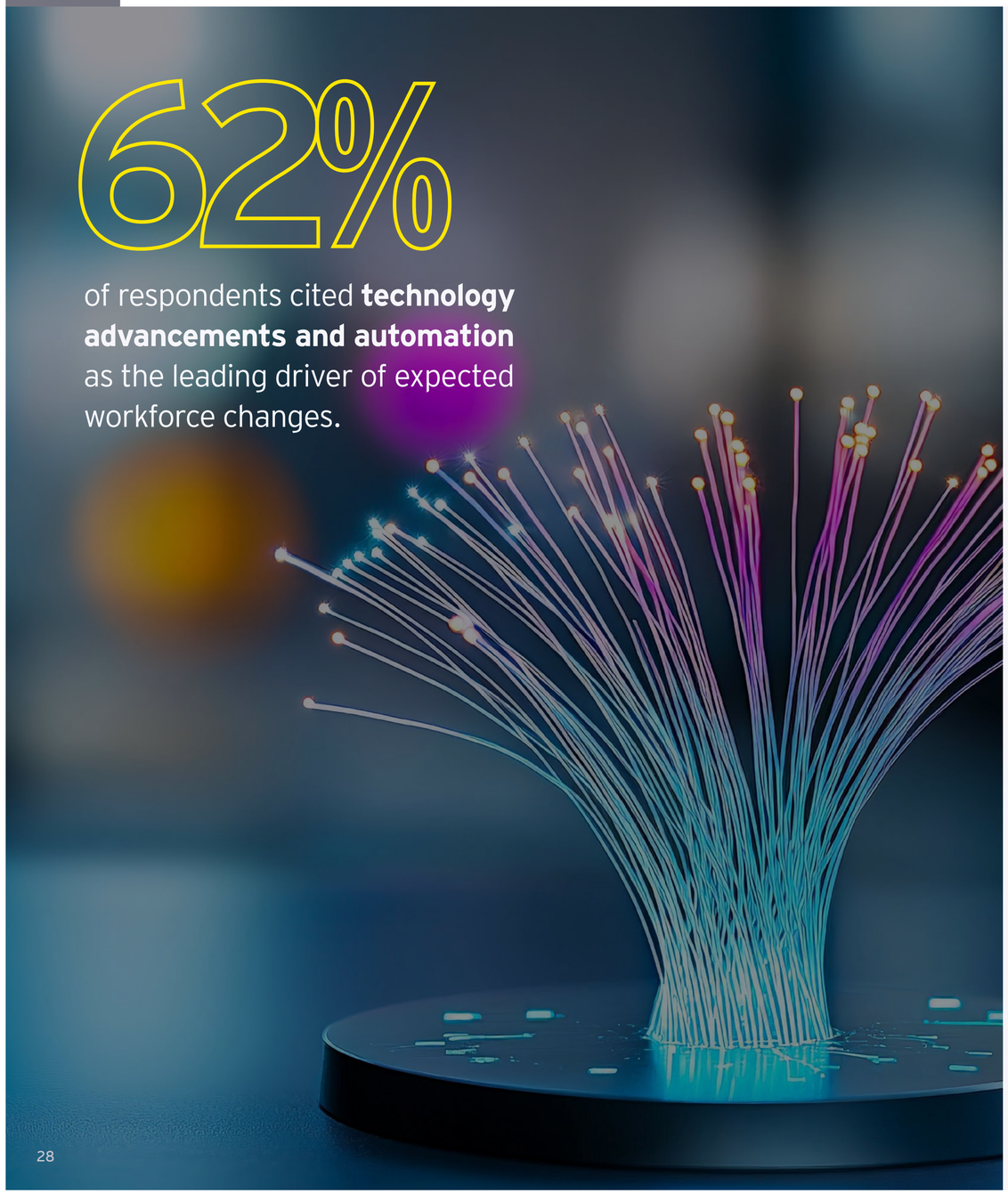
Expected workforce changes reflect multiple drivers. While technology advancements and automation are the most frequently cited factor (62%), regulatory requirements (39%) and business expansion (34%) also materially shape staffing plans, with additional influence from cost measures and strategic initiatives such as new ventures and M&A. AI and digital transformation continue to play a significant role in shaping risk management teams, but it is only one part of a complex landscape. Survey data reveals regional nuances in expectations for changes to FTEs across the second-line risk function:

- 60% of APAC CROs and 45% of EMEIA CROs cite increased regulatory requirements as a primary factor, highlighting the complexities of the regional compliance landscape.
- 70% of APAC CROs reference an expansion of business operations (compared to 30% and 31% among EMEIA and Americas CROs, respectively), reflecting the region's rapid growth.
- 25% of CROs in the Americas cite a focus on strategic initiatives, such as new ventures and M&A activity, playing a role in reshaping their team size and structure.

70%

of **APAC** CROs reference an **expansion of business operations.**

Jump to contents



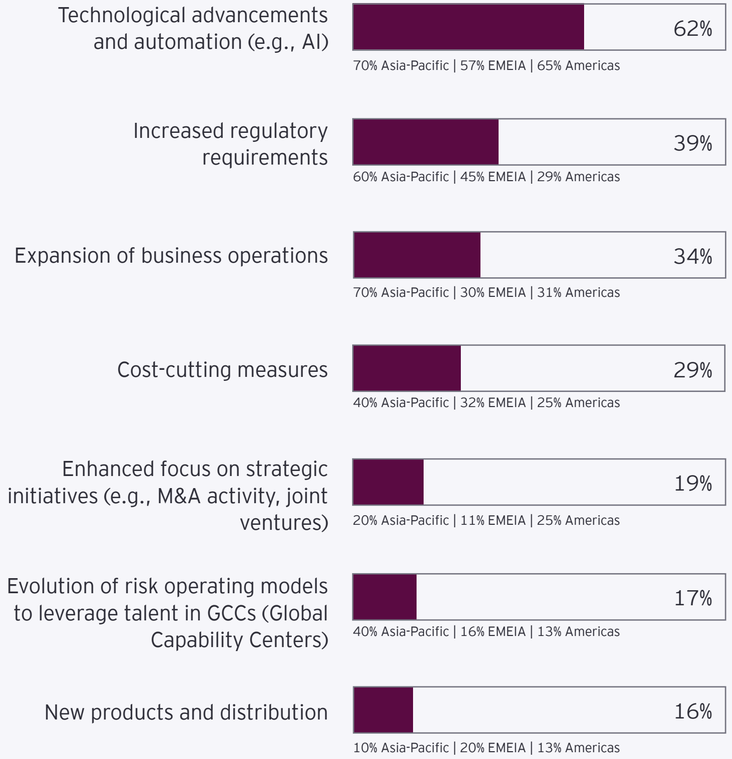
62%

of respondents cited **technology advancements and automation** as the leading driver of expected workforce changes.

Jump to contents

While automation and digitalization — including AI — are enabling risk teams to manage greater workloads with the same or fewer staff, factors like regulatory requirements, expansion of business operations and enhanced focus on strategic initiatives are also significant contributors to expected shifts in risk function staffing.

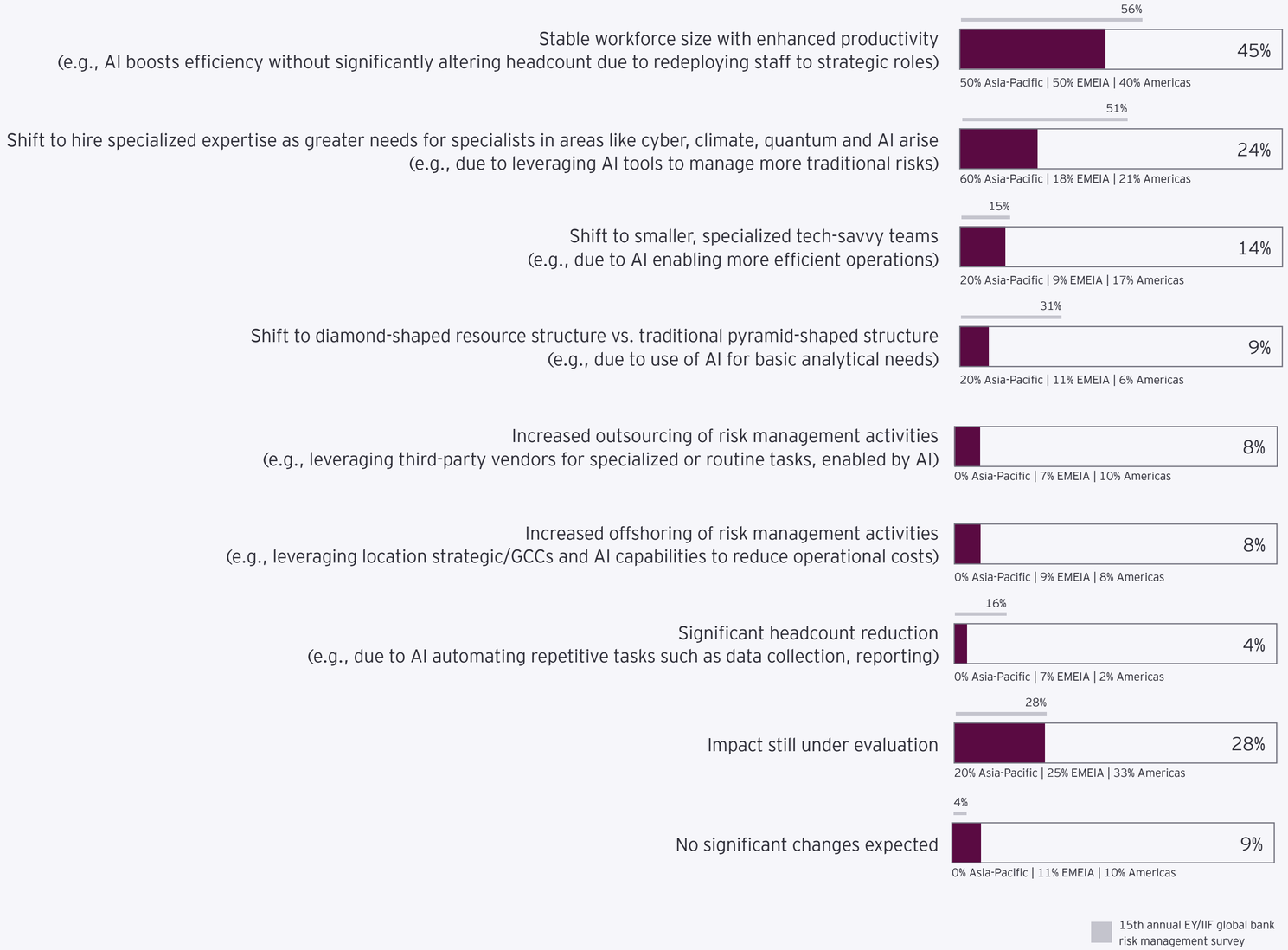
Figure 16: What factors are driving your organization's expected changes in the number of FTEs across the second-line risk function over the next three years?



AI's impact on risk teams – productivity gains, more specialists and ongoing evaluation

Results point to three primary expectations for AI's impact on risk teams: improved productivity within a stable headcount, increased hiring of specialist expertise and continued evaluation as use cases mature.

Figure 17: Expected impact of AI on the size and composition of risk management workforce in next three years



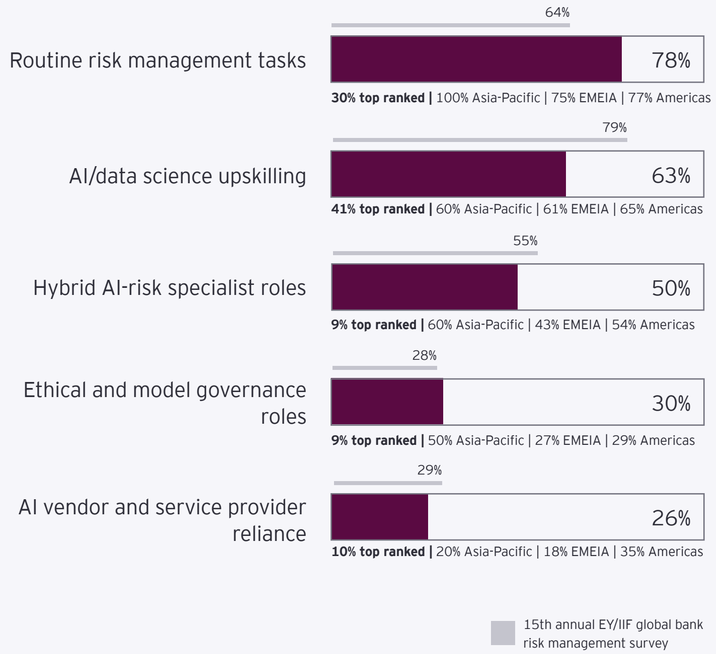
Jump to contents

Roles evolving most – upskilling, automation of routine work and new hybrid roles

Jump to contents

As AI absorbs a greater share of routine and analytical tasks, CROs expect the greatest changes in upskilling, redesigning routine work, and creating new hybrid roles that combine domain risk expertise with AI and data capabilities.

Figure 18: Over the next three years, which skills and roles within your risk management team do you expect to evolve most significantly in response to AI?



For risk leaders, workforce strategy can no longer be separated from technology strategy. As automation and AI absorb a greater share of routine and analytical work, CROs must deliberately redesign roles, upskill teams and rebalance capacity toward judgment, insight and business partnership. The ability to translate productivity gains into stronger resilience and enterprise value will increasingly define second-line effectiveness.

> “
> What CROs say:
>
> In the future, essential skills for risk professionals will include AI literacy, data governance and the ability to communicate complex challenges clearly to diverse stakeholders.

Looking ahead

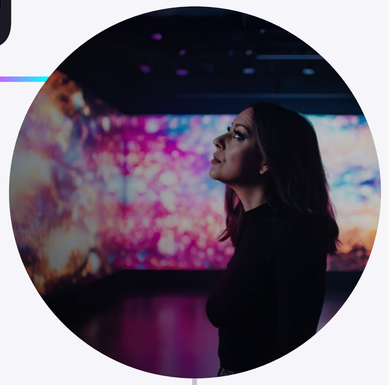
Insurers are entering a period where data-driven transformation will define the next generation of the industry — and the role of risk management. Risk leaders are navigating constant uncertainty, contending with both the internal challenge of a shifting workforce and the external dynamics of new geopolitical concerns. In the wake of this turbulence, the most successful firms will be those that shed historical silos and legacy approaches, taking incremental steps toward a trigger-based, strategy-first architecture that is tailored to their size, sector and culture.

Over the next year, expect insurers to accelerate adoption of AI-enabled risk tools, with a focus on real-time analytics and continuous controls monitoring. CROs will prioritize enhancing operational resilience and third-party risk management, responding to heightened regulatory scrutiny and evolving threats. As new technologies and geopolitical shocks reshape the risk landscape, organizations will invest more in talent development and upskilling, especially in areas like cyber and data governance. Success in the industry will increasingly depend on anticipating disruptions, adapting rapidly and embedding risk management seamlessly across business units.

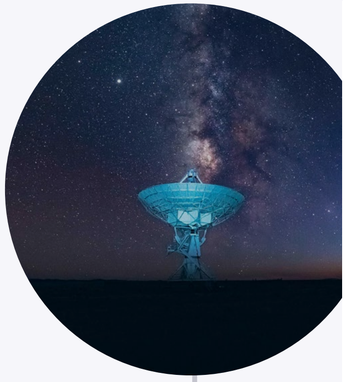
As the insurance risk landscape becomes more digitally exposed, geopolitically sensitive and data-dependent, CROs will increasingly be called upon to assume more strategic responsibilities. In the same way, the risk workforce will require a shift — while headcount may remain stable, productivity continues to rise as automation grows. Organizations will continue to seek deeper specialization in cyber, climate, AI and data. Skills such as adaptability and digital acumen emerge as essential for navigating a more volatile, tech-driven future.

Jump to contents

Further reading



2026 EY/IIF global bank risk management survey

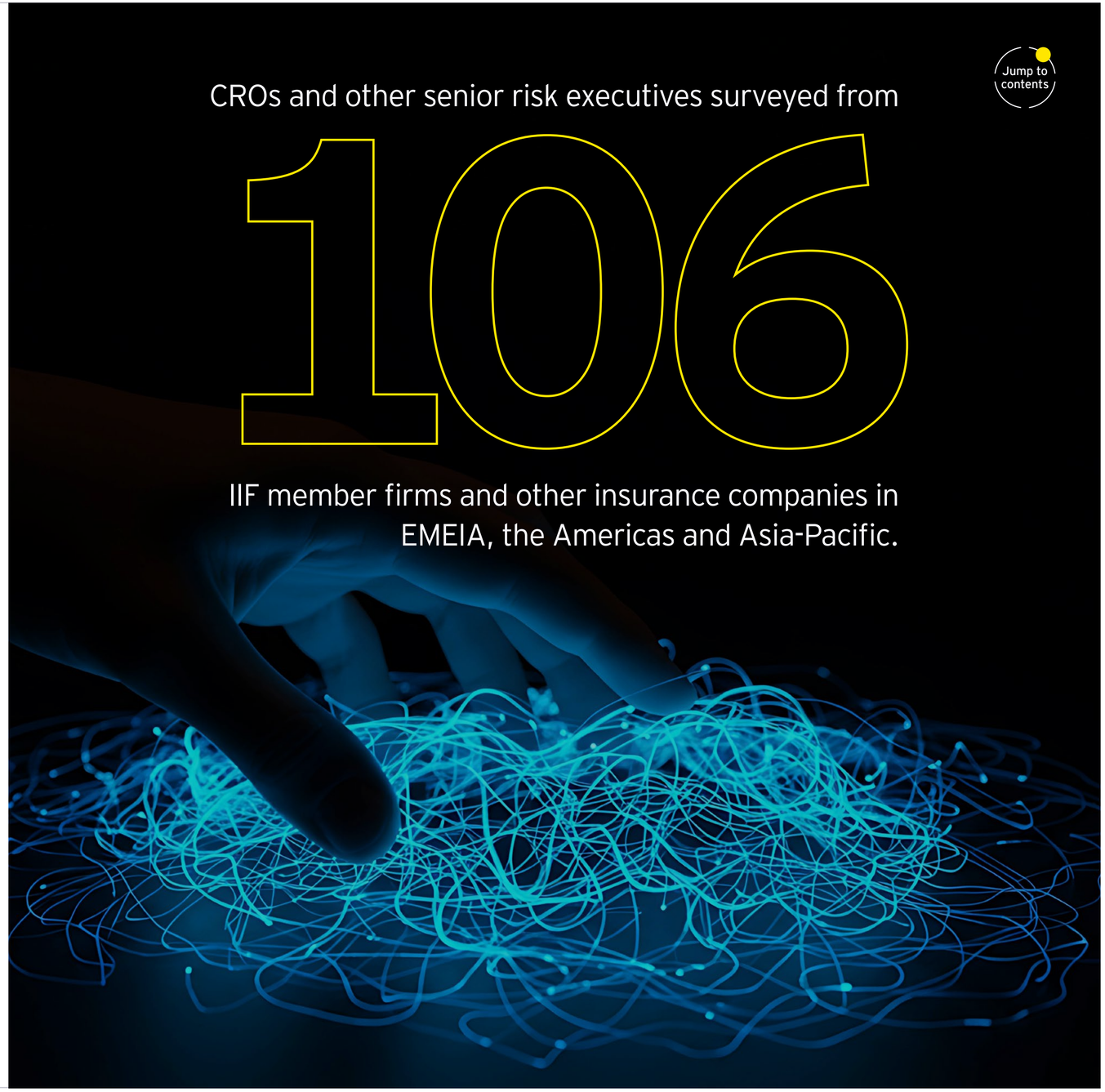


Global Risk Transformation Series

2026 Global Insurance Outlook

Research methodology and participants

The global EY organization, in collaboration with the IIF, surveyed CROs and other senior risk executives from 106 IIF member firms and other insurance companies in EMEIA, the Americas and Asia-Pacific between November 2025 and January 2026. Participants were interviewed, completed an online survey or both. The research included a cross-section of the insurance sector in terms of asset size, geographic reach and line of business (e.g., property and casualty, life, health, reinsurance and specialty).



Contacts

Jump to contents

EY Global Risk Insurance Survey Leaders

Jonathan Zhao
EY Global Insurance Leader (Hong Kong)
jonathan.zhao@hk.ey.com

Tom Campanile
EY Global Financial Services Risk Consulting (US)
thomas.campanile@ey.com

Stuart D. Doyle II
US Insurance Risk & Regulation Leader (US)
stuart.doyleii@ey.com

Tze Ping Chng
Asia-Pacific Consulting Insurance Sector Leader (Hong Kong)
tze-ping.chng@hk.ey.com

Eamon McGinnity
UK Insurance Risk & Regulation Leader (UK)
eamon.mcginnity@uk.ey.com

Pierre Santolini
Europe Insurance Risk & Regulation Leader (France)
pierre.santolini@fr.ey.com

EY Super Region Leaders

Jeff Gill
EY US Insurance Leader, US
jeffrey.gill@ey.com

Janice Deganis
EY Canada Insurance Leader, Canada
janice.c.deganis@ca.ey.com

Anita Sun-Young Bong
EY Asia East Insurance Leader, South Korea
sun-young.bong@kr.ey.com

Rick Huang
EY Greater China Insurance Leader, China
rick.huang@cn.ey.com

Stacey Hooper
EY Oceania Insurance Leader Australia
stacey.hooper@au.ey.com

Philip Vermeulen
EY Europe West Insurance Leader, Switzerland
phil.vermeulen@ch.ey.com

Lampros Gkogkos
EY Europe Central – CESA Insurance Leader, Greece
lampros.gkogkos@gr.ey.com

Gabriella Selvander Hedvall
EY Europe Central – Nordics Leader, Sweden
gabriella.selvanderhedvall@se.ey.com

Martina Neary
EY UKI Insurance Leader, UK
mneary@uk.ey.com

Jaco Louw
EY Africa and India Insurance Leader, South Africa
jaco.louw@za.ey.com

Jonathan Matchett
EY MENA Insurance Leader, South Africa
jonathan.matchett@sa.ey.com

IIF contacts

Philippe Brahin
Head Insurance and NBFI Regulatory Affairs
pbrahin@iif.com

Melanie Idler
Associate Policy Advisor
midler@iif.com

A special thank you to these contributors:

Rasika Karnik
Patricia Davies
Krista Vivian
Cassidy Zimmerman
Ella Abbott
Edmond Nana Jimngang
Benjamin Alter
Chloe Ostroff
Andre Kohler
Kristin Bekkeseth
Marcelo Lustosa

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 002861-26Gbl
2603-11240-CS
ED None

About the Institute of International Finance

The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks and development banks.

The Institute of International Finance (IIF)
1333 H St NW, Suite 800E
Washington, DC 20005-4770
USA

Tel: +1 202 857 3600
Fax: +1 202 775 1430
www.iif.com
info@iif.com