Feeling the pressure: A new reality for compliance leaders

2026 KPMG Global Chief Ethics and Compliance Officer Survey

KPMG. Make the Difference.

Contents

Foreword

In today's world of compounding volatility, the role of the Chief Compliance Officer (CCO) is becoming increasingly complex. Technological change fueled by advances in artificial intelligence (AI) is more dizzying than ever. Regulators across the globe continue to press their respective priorities, which may not always align. And all this is happening while increasingly unpredictable geopolitical undercurrents make doing business harder.

As companies try to adjust to this new era, they are counting on the CCO to stay on top of myriad compliance risks and address them before they escalate into a crisis. To find out how compliance leaders are tackling these tasks, KPMG International surveyed 725 CCOs representative of the largest companies by revenue operating in six industry sectors across eight countries. The responses provide insights into their current and two-year outlook on key areas of ethics and compliance, including operational challenges, regulatory complexity, evolving technology, and a culture of value creation.

Our latest survey revealed three key themes. First, CCOs consider enhancing operational resilience as paramount to better addressing interconnected cyber, third-party, and regulatory risks. Second, although recognizing the huge potential of AI to transform compliance, they are approaching it cautiously, trying to balance wider adoption with robust governance. Third, compliance leaders are continuing in the efforts, observed over the past several years, to shift perceptions of the function as a cost center to a strategic value creator for the company. This report explores these findings in detail and offers insights from KPMG professionals that can help the compliance function create a blueprint for the future.

Annabel Reoch
Global Head of Ethics and Compliance,
KPMG International and Partner
KPMG UK

Key research findings

Operational resilience

Respondent CCOs are focused on fortifying operational resilience against all kinds of risks, threats, and financial crime

75% of CCOs say cybersecurity/data privacy are the key areas they are looking into for additional investment.

AI in compliance

CCOs are cautiously optimistic about the potential benefits of AI in compliance

68% of CCOs surveyed report they feel "mixed, leaning positive" with AI use, noting they have seen more benefits than challenges.

Compliance as a value driver

CCOs surveyed are keen to change the perception of the compliance function from a cost center to a strategic business unit that can enhance brand reputation and drive value.

67% of respondent CCOs are confident of assessing compliance synergies across functions such as legal, human resources, investigations, internal audit and operations.

Source: 2026 KPMG Global Chief Ethics and Compliance Officer Survey, KPMG International, August 2026

Operational resilience

Risks abound from cyberattacks, data breaches, and regulatory scrutiny

Key findings

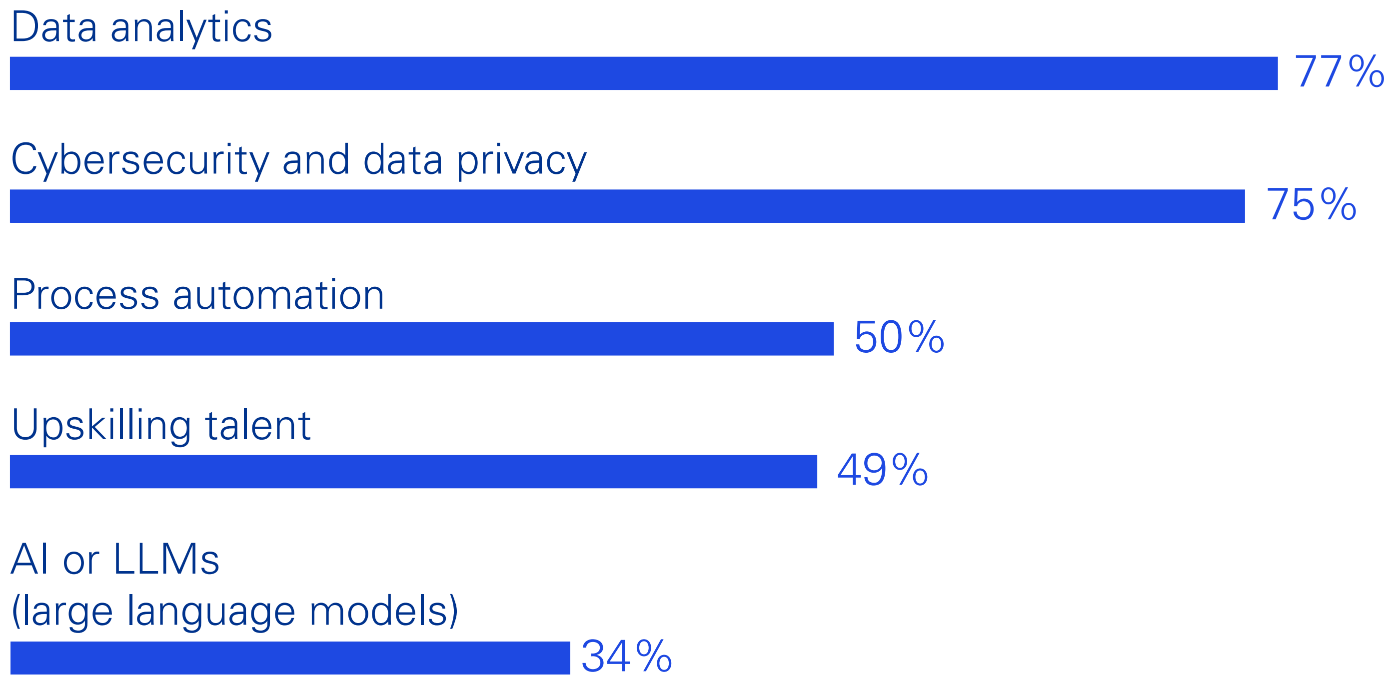
CCOs are focused on fortifying operational resilience against all kinds of risks, threats, and financial crime. Looking ahead, improving identification and management of cybersecurity risks and integrating data analytics for proactive third-party risk management (TPRM) are likely to be primary investment drivers for their organizations. At the same time, survey results reveal the traditional force of a demanding regulatory environment as the number one challenge for compliance leaders.

Investment priorities

When increasing budgets, an overwhelming majority of CCOs surveyed say data analytics (77 percent) and cybersecurity/data privacy (75 percent) are the key areas they are looking into for additional investment. CCOs in the US feel this most acutely, with 85 percent anticipating more investment in data analytics and 87 percent in cybersecurity. However, the urgency for both was relatively low in Japan and Australia, where 69 percent and 63 percent of survey participants responded that data analytics will drive investment, while 57 percent and 58 percent, cited cybersecurity investment as an investment driver. In many cases CCOs will look at where they can share the business case and cost burden of these investments with other functions.

Figure 1: Areas for additional investment

Anticipating a budget increase, which area(s) are driving the additional need for investment?

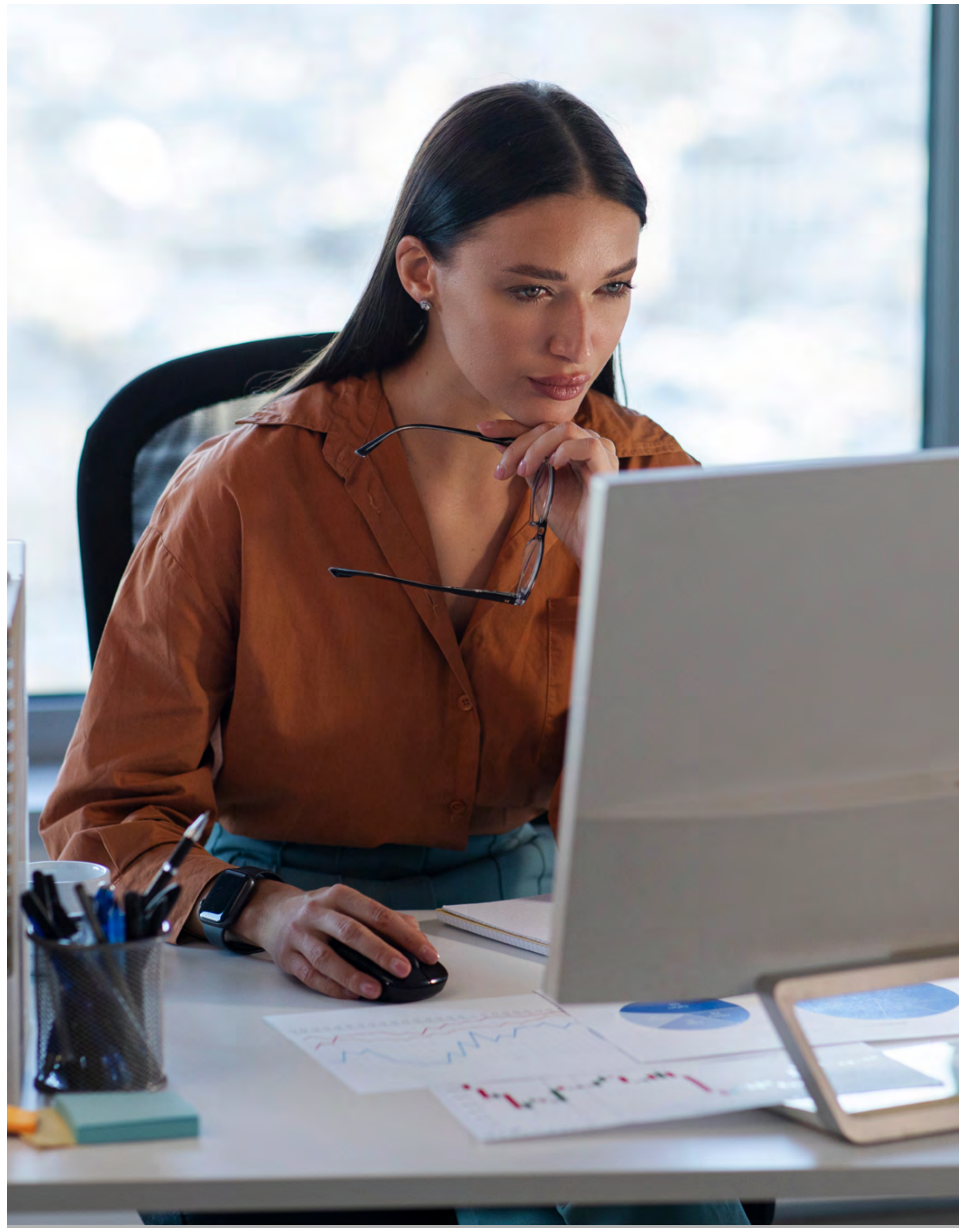


**Sum of percentages may not add up to 100% due to rounding.*

Source: 2026 KPMG Global Chief Ethics and Compliance Officer Survey, KPMG International, August 2026

> Effective CCOs are likely to align with other functions to create the business case and shared cost of operational resilience such as the implementation of technology and analytics.

Annabel Reoch
Global Head of Ethics and Compliance, KPMG International and Partner
KPMG UK



Regulatory pressures

When asked to identify the top compliance challenge their organizations will face in the next two years, 33 percent of CCOs said new regulatory requirements. Again, the weight placed on regulations was higher in the US — 41 percent versus 30 percent elsewhere — perhaps reflecting the unpredictable policymaking dynamic. The second biggest challenge was data analytics and predictive modeling for compliance monitoring and risk management, mentioned by 31 percent of all respondents and 36 percent of non-US compliance leaders. From stronger anti-corruption enforcement in China, France, and the UK to the rise in investigations by the German financial regulator, regulatory oversight is intensifying and will continue to drive the need for a strong and embedded compliance framework and ethical culture.

Figure 2: Top challenges to compliance efforts in the next two years

What are the top challenges your organization will face regarding its compliance efforts in the next two years?

Source: 2026 KPMG Global Chief Ethics and Compliance Officer Survey, KPMG International, August 2026

KPMG insights

Key drivers behind these findings:

Operational, regulatory, and data-driven risks are converging. Incidents such as major data breaches pose serious compliance and reputational risks for companies, potentially leading to regulatory investigations, fines, and lawsuits.

As compliance functions become more reliant on data analytics, protection of sensitive data is becoming an inherent part of their mandate. This means CCOs in many places such as Canada are becoming more involved in governance around cybersecurity and data — although in other countries, including Australia and Japan, cybersecurity responsibilities still mainly fall under the Chief Information Security Officer (CISO).

In the EU, legislation and regulations increasingly emphasize digital and operational resilience and improving oversight of supply chains.

> CCOs face an escalating challenge to keep pace with both technological threats and regulatory demands, necessitating sustained investment in both tools and people to avoid reputational harm.

Jennifer Shimek
Partner, Forensic — Ethics, Compliance & Regulatory
KPMG US

What should companies actively focus on?

01

Closing the perception gap. While CCOs perceive risks are high globally, individual companies may often underestimate their own exposure. Undertaking dynamic risk assessments to identify the interconnectedness of risk events is critical to understand and mitigate their potential impact on business operations and improve operational resilience.

02

Implement a unified risk framework. The CCO is uniquely positioned to connect the technical aspects of cybersecurity and data protection with the legal and regulatory obligations:

- Go beyond integrating cyber, data privacy, and sustainability risk domains within third-party risk management by developing a common risk taxonomy and centralized repository to get a truly integrated view of risk across the enterprise and value chain.
- Scan the regulatory horizon to keep pace with rule changes, efficiently comply with new regulation, and avoid being "caught out."
- Provide well-designed training on geopolitical uncertainty and guidance on sanctions and export controls to individuals in relevant roles, and ensure senior management receives timely risk information.

03

Conduct proactive scenario planning. CCOs should champion regular, rigorous stress tests for high-impact events such as ransomware attacks, critical third-party failures, or sudden geopolitical shifts. This will build practical memory for crisis response.

04

Elevate compliance's role in technology governance. Confirm that regulatory requirements and data protection principles are designed into systems from the outset by embedding compliance leaders in the governance process for adopting new technologies including AI adoption across the business. The CCO's role should not be limited to investigating breaches.

05

Continue to embed a strong compliance culture across the organization so that individuals feel empowered and safe to speak out if they identify a risk or concern. Early detection can help avoid a small issue becoming a large-scale crisis.

06

Enhance responses to misconduct by designing/reforming mechanisms for early detection and reporting of fraud and other incidents, including whistleblowing systems.

> "Many Japanese companies use regular personnel rotation systems, which provide employees with diverse experience and can help prevent and detect fraud early. However, such systems may also limit opportunities for ethics and compliance staff to develop specialized expertise. As a result, the use of data analytics and upskilling may be more challenging in Japan. Strengthening these areas could help the compliance function play a more strategic role."

Mariko Yamada
Director, Forensic & Risk Advisory
KPMG Japan

AI in compliance

An exciting technology but short on human trust

Key findings

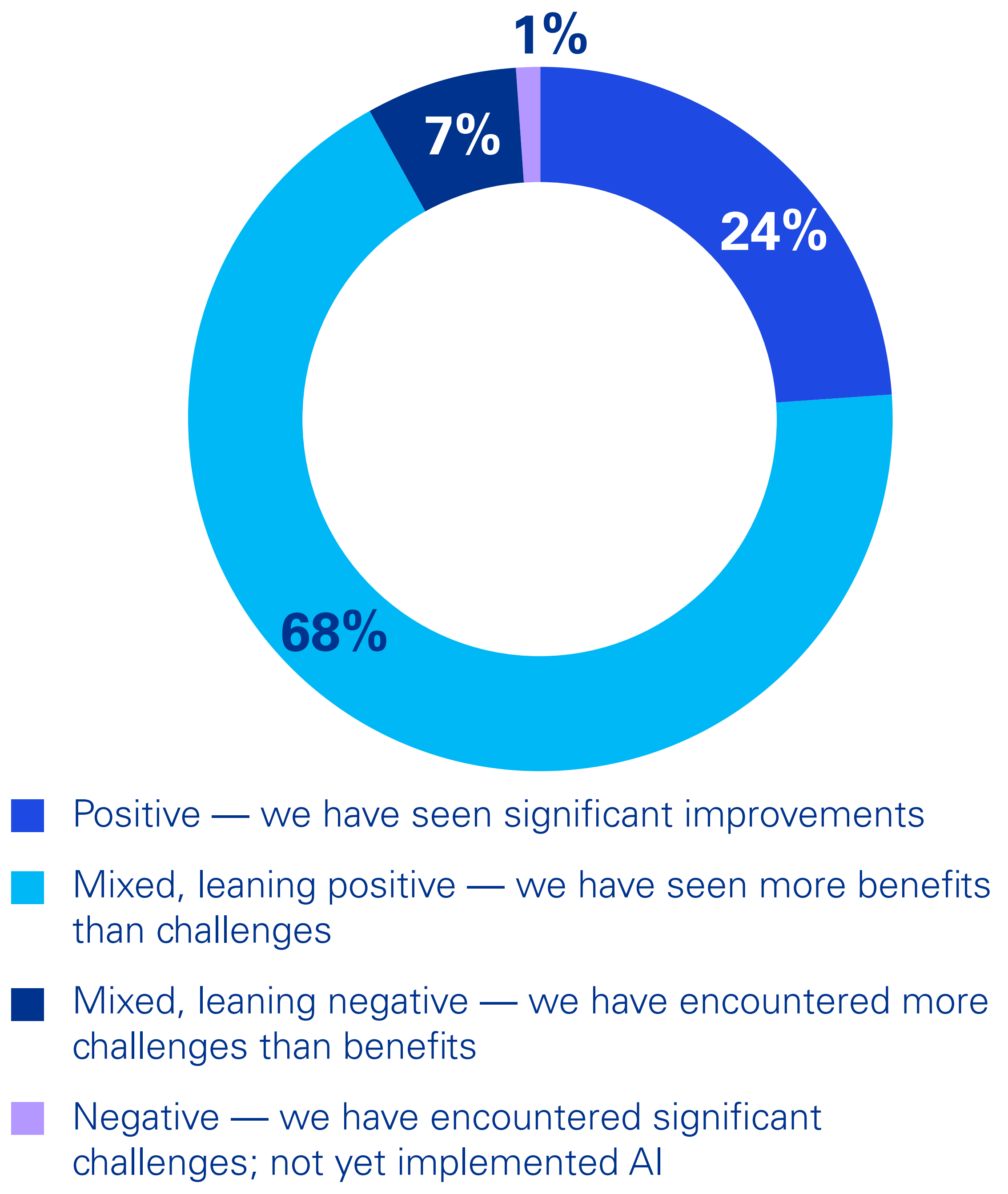
In general, CCOs surveyed are cautiously optimistic about the potential benefits of AI in compliance. While globally, a majority of respondents say their AI experience has been positive, many companies seem to be still in the early, experimental stages of adoption. AI use in surveyed markets is mostly for routine tasks such as email reviews and document analysis, as the need for human oversight remains a hurdle for more complex tasks.

AI is making a good impression

More than two-thirds (68 percent) of CCOs surveyed report they feel "mixed, leaning positive" with AI use, noting they have seen more benefits than challenges. And another 24 percent say they have seen significant improvement in compliance efficiencies and effectiveness. This positive sentiment is strongest in China (35 percent) despite challenges with data privacy and model building. Some CCOs in Australia had significant challenges and cited negative AI experiences.

Figure 3: Effectiveness and efficiency of AI

What is your organization's experience with using artificial intelligence (AI) to improve compliance efficiencies and effectiveness?



**Sum of percentages may not add up to 100% due to rounding.*

How CCOs are using automation and AI

CCOs are deploying AI most often for compliance risk assessment and management (50 percent), data visualization and predictive analytics (44 percent), and employee training and awareness (44 percent). However, AI use is limited for tasks such as hotlines and investigations (4 percent), contract compliance and anti-money laundering (12 percent), and legal document drafting and reviews (17 percent).

This seems to indicate that there is a lack of confidence with AI's capabilities in compliance activities that demand more complexity, sensitivity, and human analysis.

Figure 4: Automation/AI/machine learning use cases

For which of the following use cases does your organization use automation or AI/machine learning in your compliance management practices?

Source: 2026 KPMG Global Chief Ethics and Compliance Officer Survey, KPMG International, August 2026

KPMG insights

Key drivers behind these findings:

Being cautious about AI is prudent. The technology holds immense promise, but its application in a highly regulated context of compliance can be fraught, with potential algorithmic bias, lack of transparency, an unclear AI regulatory framework, and compliance risks related to using it.

AI has dual aspects: It can be a useful tool in compliance functions for risk assessment, but there are wider considerations about how to implement it ethically. While there is optimism, the reality on the ground is more challenging given the need for human oversight. Poor quality and disparate data can often be a blocker to full-scale AI adoption as the results may include false positives, inherent bias, or overwhelm the user.

AI governance and how it's managed is a fundamental issue. CISOs, CCOs, or professionals in equivalent positions can't possibly know what all the AI models and agents at their organizations are doing. The biggest fear with AI reliance is not being aware of something that should have been reported.

Technology alone is not a silver bullet. A successful modern compliance function depends on having the right talent with the right skills, operating within a strong ethical culture. However, the survey highlights that less than one-quarter of respondents are very well prepared for "upskilling compliance professionals" (21 percent) and "enhancing compliance culture" (20 percent).

> "It can be difficult to understand how AI algorithms arrive at their decisions. This 'black box' challenge makes it difficult for CCOs to validate compliance decisions and identify bias. As AI automates more entry-level tasks, junior employees have fewer opportunities to develop the expertise needed to evaluate AI outputs — skills that compliance teams will need in the future."

Verena Hinze
Partner, Governance, Risk, Compliance & Forensic
KPMG Germany

What should companies actively focus on?

01

Trust in AI adoption starts with compliance leadership. CCOs have a key role to play in helping their organizations adopt AI in a trusted manner. An effective compliance program should include criteria to evaluate how companies are assessing and managing risks related to the use of new technology such as AI.

02

AI adoption requires sustained executive commitment. Secure leadership support for long-term, strategic implementation of AI across the business with its integration into core processes. Ensure C-suite and senior management buy-in on related investment and budget allocations. Companies should be willing to embrace real change to roles, team structures, workflows, and risk assessment methodologies to see positive material impact.

03

Establish a formal AI governance framework. Trust in AI is likely to remain a barrier until companies seek to build it through transparent and well-considered governance structures and investments in AI literacy. Create a dedicated framework that defines ethical guidelines, clarifies roles for AI oversight (e.g., CCO vs. CISO vs. chief data officer), and establishes a formal process for vetting, approving, and monitoring all AI tools used in the organization.

> “How do you monitor the use of AI within businesses? Are there compliance breaches that people would never know about? There’s a concern about whether compliance functions have the right capabilities in this new world.”
>
> **Martin Dougall**
> Partner, Forensic
> KPMG Australia

04

Maturity and readiness should be clearly understood. Assess your organization’s current deployment of automation/AI and readiness for future use cases. It’s essential for companies to understand where their compliance teams stand with actual uses of AI and what is required to improve the status quo. Adopt a “crawl, walk, run” implementation strategy. Start with low-risk, high-return AI use cases to build confidence and competence before expanding to more complex applications. Regularly verify the effectiveness of AI use through testing and monitoring.

05

Data quality is a prerequisite for effective AI use. Undertake a data cleanse/cleanup exercise prior to any deployment to ensure the output is useful and actionable.

06

Prioritize “human-in-the-loop” systems and explainability. Ensure new AI tools and use cases are rolled out in a safe environment with human analysis of output before going live. A human-in-the-loop approach helps to ensure that the compliance team can validate, understand, and ultimately defend the outputs of any AI model. Another critical success factor will be the accuracy and completeness of the data AI is processing and how well compliance professionals understand what the technology is doing (i.e., avoiding black-box scenarios with results that can’t be explained or acted upon).

07

Proactively address AI upskilling. Establish a formal training program for compliance professionals, focusing on data literacy, how AI models work, and interpreting and challenging AI-generated insights.

Compliance as a value driver

Looking up from the rule books

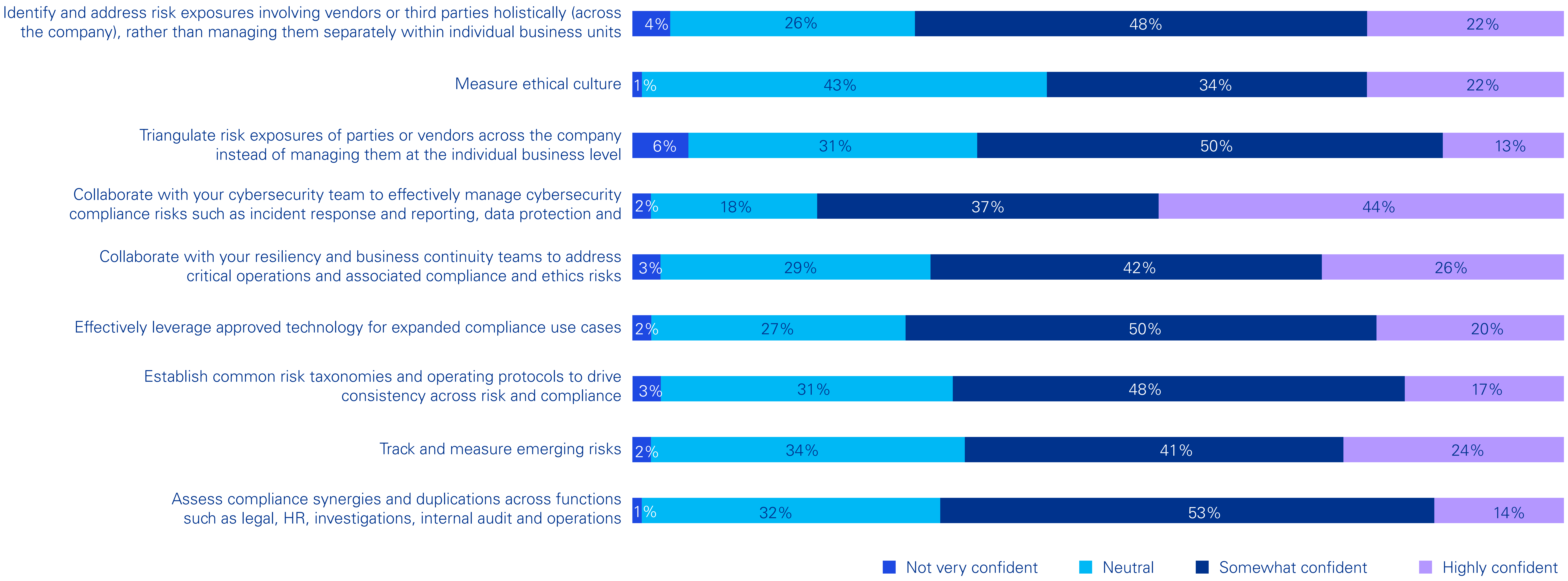
Key findings

The CCO has shifted from a traditionally reactive steward of rules and procedures to a proactive, data-driven leader who not only manages risk but also enables growth. Business priorities vary across countries, but overall, CCOs are keen to change the perception of the compliance function from a cost center to a strategic business unit that can enhance brand reputation and drive value.

CCOs are increasingly collaborating across functions to support business objectives. A significant segment of our survey respondents (81 percent) say they are confident in collaborating with cybersecurity teams to effectively manage cybersecurity compliance risks; 68 percent are confident in collaborating with resiliency and business continuity teams to address critical operations; and 67 percent are confident in assessing compliance synergies across functions such as legal, human resources, investigations, internal audit and operations.

Figure 5: Confidence in ability to accomplish business objectives

How confident are you in your organization's ability to accomplish the following?



Source: 2026 KPMG Global Chief Ethics and Compliance Officer Survey, KPMG International, August 2026

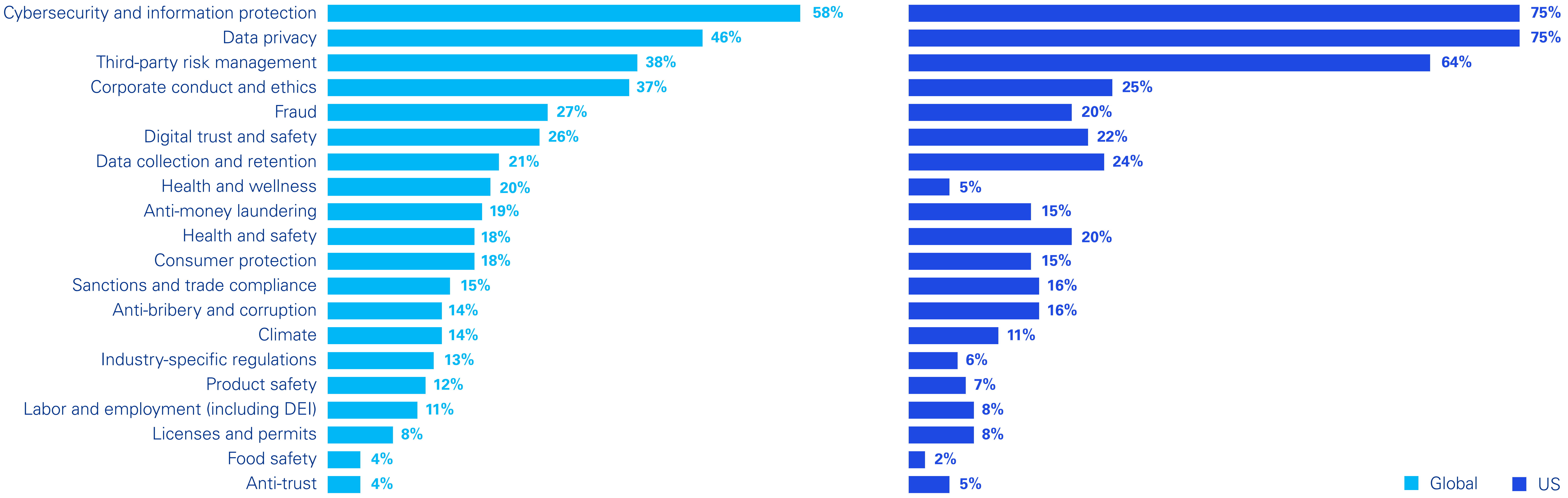
**Sum of percentages may not add up to 100% due to rounding.*

Fragmentation on sustainability

Due to different political and regulatory attitudes, compliance leaders are diverging on sustainability issues. While 14 percent of non-US CCOs say climate will be a top area of compliance efforts in the next two years, 11 percent of CCOs in the US agree. A similar gap exists on labor and employment: 11 percent versus 8 percent, respectively. However, across all regions, both topics rank far below core compliance concerns such as cybersecurity, data privacy, third-party risk management, ethics and fraud.

Figure 6: Process efficiency targets in the next two years

What are the top areas of compliance targeted for process efficiency in the coming two years? (e.g., simplification or automation, etc.)?



Source: 2026 KPMG Global Chief Ethics and Compliance Officer Survey, KPMG International, August 2026

KPMG insights

Key drivers behind these findings:

With successful companies constantly assessing budgets and cost-out initiatives, CCOs should be seeking to demonstrate the value the compliance function brings to the organization — such as the improvement in brand value (leading to increased sales) and protection from regulatory scrutiny and fines.

In an era of regulatory and geopolitical uncertainty, CCOs are under pressure to demonstrate a strategic ability to anticipate evolving expectations of the compliance function, assess complex legal and regulatory requirements, and respond to ramifications of political upheavals.

Sustainability rules, norms, and practices are becoming inconsistent across different jurisdictions. Efforts are still in the early stages in some countries while being deprioritized in others.

> "CCOs in Canada face particular challenges around sustainability expectations, which continue to evolve amid shifting enforcement stances. They must balance stakeholder expectations with an uncertain regulatory trajectory."

Becky Seidler
Partner, Forensic Investigation, Integrity & Dispute Services
KPMG Canada

What should companies actively focus on?

01 **Embed compliance into strategic business planning for proactive risk management.** The CCO should be a strategic partner, not a reactive advisor. Ensure that compliance has a permanent seat at the table during strategic planning for new markets, products, or deal activities. Meanwhile, compliance leaders should be seeking to articulate the function's value to the board and C-suite. For example, use data visualization to create compelling narratives on how compliance investments protect the company and enable growth.

02 **Strengthen public disclosures on sustainability.** As scrutiny for "greenwashing" intensifies, the compliance function should play a central role in reviewing and validating public-facing claims and disclosures. This can help ensure that sustainability reporting is as rigorous and defensible as financial reporting.

03 **Develop a robust compliance data analytics strategy.** Leverage data to gain insights into compliance performance, identify emerging risks, and measure the effectiveness of controls. This helps allocate resources more efficiently and demonstrate return on investment for compliance programs.

04 **Foster a strong ethical culture from the top down.** A strong culture reduces the likelihood of misconduct. Work with leadership to integrate ethical considerations into decision-making processes, reward ethical conduct, and ensure a clear channel for reporting concerns without fear of retaliation.

05 **Implement a clear and accessible compliance training and communication program.** Move beyond generic, annual training. Tailor content to specific roles and risks, using engaging formats. Regular, targeted communications make employees active participants in risk management.

06 **Streamline and harmonize global compliance processes.** For multinational organizations, simplify and standardize compliance processes where appropriate, leveraging technology to create efficiency and consistency. This reduces complexity, lowers costs, and ensures a unified approach to managing compliance risks across different jurisdictions.

07 **Integrate compliance into the performance management framework.** Work with HR to incorporate compliance objectives and ethical behavior into employee performance reviews and incentive structures. This reinforces the message that compliance is a shared responsibility and a critical component of individual success.

08 **Engage independent experts to review the effectiveness of the compliance program.** This provides an objective assessment, identifies gaps, and offers external validation that the program is fit for purpose and continuously improving.

Compliance essentials

Key questions for the compliance program

The compliance function, led by the CCO, should drive an effective compliance program in line with an overall sound compliance framework. This means identifying and building controls to mitigate a new series of potential legal, reputational and compliance risks. Some key questions to ask of your compliance program include:

Governance and culture

- Are board and committee(s) regularly updated on regulatory and compliance changes, including regulatory assessments and enforcement expectations?

Policies and procedures

- Do written policies and procedures reflect actual practice?
- Are written policies and procedures regularly reviewed and updated for changing compliance concerns, such as sustainability, models and AI?

Third-party risk management

- Is risk-based assessment and testing of third-party relationships adequately assessed in due diligence and conducted via ongoing monitoring and testing — to ensure they comply with regulatory requirements and organizational policies?

Compliance risk assessment

- Does the risk assessment incorporate both qualitative and quantitative data and inputs?
- Based on the assessment, are sufficient economic, technological and human resources allocated to compliance?
- Is the risk assessment dynamic, incorporating changes in business operations and strategy?

Communication and training

- Is there a compliance training program that includes an annual and formalized training calendar?
- Is compliance training sufficiently tailored to individuals' roles and responsibilities?

Issues management and investigations

- Are protocols established for handling data and evidence (physical and digital), as well as resolution, communication and disclosure?
- Does the review or investigation include root cause analysis and "lessons learned" protocols?

People, skills and accountability

- Are roles and responsibilities clearly articulated, and does the company demonstrate that compliance responsibilities matter through performance reviews and compensation?
- Are disincentives built into the incentive plans to discourage misconduct?
- Do you have a strong compliance culture where employees feel safe to speak out without fear or retaliation?

Technology and data analytics

- How does the organization leverage data to support compliance risk assessments, monitoring and surveillance methodologies, and transaction and control testing?
- Does the organization have the policies, procedures and technology in place to ensure emerging technologies are implemented responsibly (to take account of AI data, privacy, ethics and governance, etc.)?

Monitoring and reporting

- Are key performance indicators (KPIs) used to monitor compliance with regulations and compliance effectiveness?
- Are compliance key risk indicators (KRIs) established and tracked regularly, and do they link to the organization's risk appetite and tolerance?

Meet the authors

Annabel Reoch
Global Head of Ethics and Compliance,
KPMG International and Partner
KPMG UK

Annabel is a Chartered Accountant and a partner in the UK firm's Forensic practice.

As Global Head of Ethics and Compliance, she specializes in business conduct and integrity, leading KPMG Forensic ABC and ESG Integrity services across the global network.

Annabel can assist organizations in identifying, mitigating, and responding to complex ESG risks, encompassing anti-bribery and corruption, fraud and financial crime, human rights, greenwashing, and sustainability fraud, in line with UK and international regulations.

Matthew McFillin
US Forensic Leader
KPMG US

Matthew McFillin serves as US Forensic Leader for the KPMG US practice. He advises attorneys, audit committees, and corporate leadership on complex investigations involving financial statement fraud and anti-bribery and corruption matters and has frequently worked with regulators including the SEC and U.S. Department of Justice on high-profile global investigations and compliance engagements.

Jennifer Shimek
Partner, Forensic: Ethics, Compliance
& Regulatory
KPMG US

Jennifer is a partner in the KPMG US Advisory practice, specializing in regulatory enforcement and compliance within the healthcare and life sciences and consumer and retail sectors. With nearly 30 years of industry experience, she advises global pharmaceutical, biotech, and healthcare organizations on FCPA matters, investigations, due diligence, and compliance programs. She previously served as Office Managing Partner for the KPMG US Short Hills office from 2020 to 2025 and brings firsthand operational insight from prior healthcare executive leadership roles.

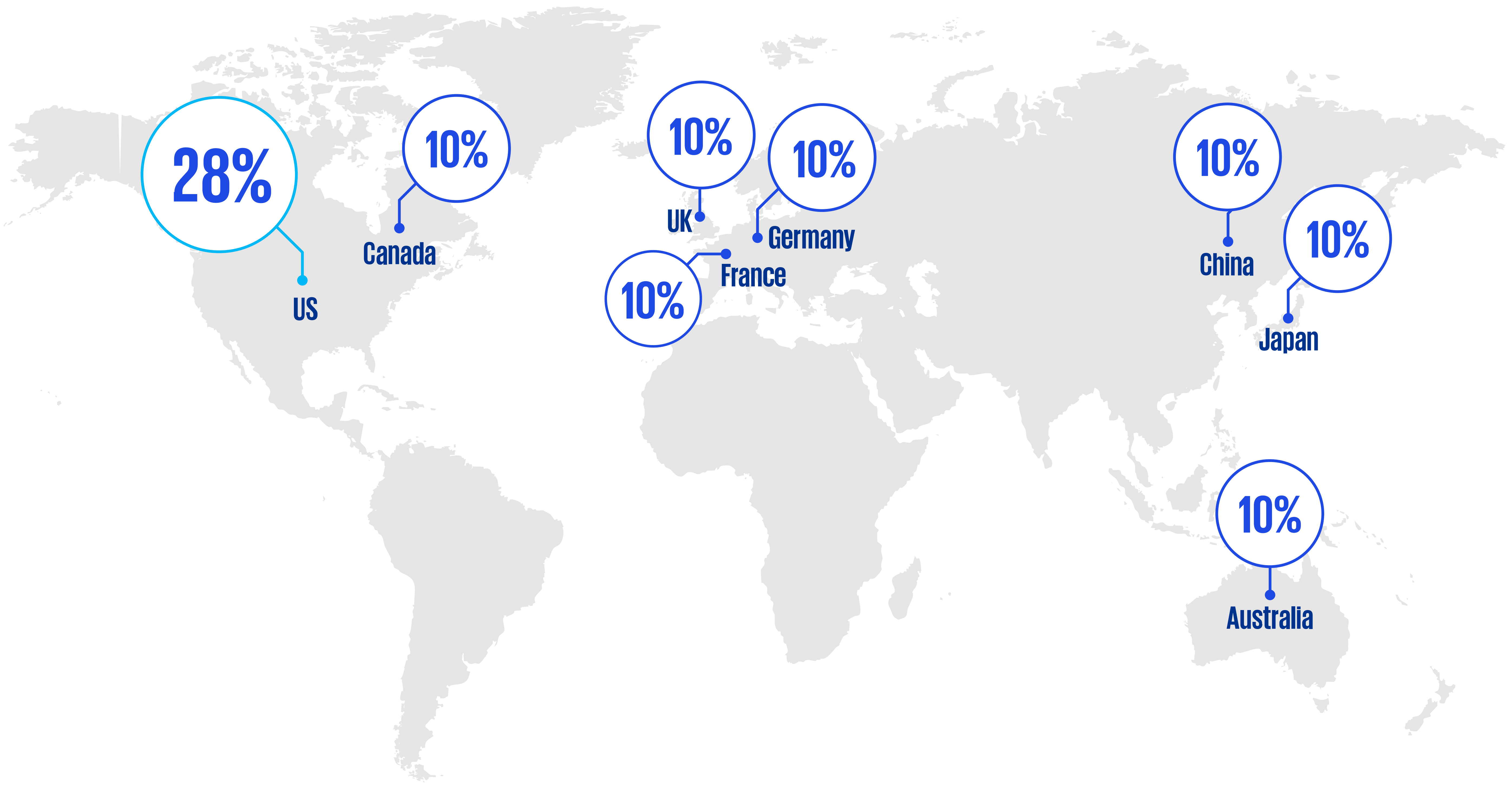
Eliza Morris
Director, Forensic Investigations & Compliance
KPMG UK

Eliza is a director at KPMG UK with over 12 years' experience advising organizations on financial crime risk, including bribery and corruption, fraud, tax evasion, and sanctions. She specializes in business conduct and integrity, with expertise in the UK Bribery Act, U.S. FCPA, Fraud Act, and Economic Crime and Corporate Transparency Act. Eliza can help clients with the design and implementation of global compliance programs, leads complex investigations, and brings in-house experience as a former Global Ethics and Compliance Leader.

Research methodology

KPMG surveyed 725 Chief Ethics and Compliance Officers (CCOs) representative of the largest companies by revenue operating in six industry sectors across eight countries.

To ensure the accuracy of the results, the survey data was normalized to account for the larger response population from the US.



**Sum of percentages may not add up to 100% due to rounding.*

Industries represented:

- Healthcare and Life Sciences (HCLS)
- Banking, Capital Markets and Insurance (FS)
- Industrial Manufacturing (IM)
- Consumer and Retail (C&R)
- Technology, Media, and Telecommunications (TMT)
- Energy and Natural Resources (ENRC)

Contacts

Annabel Reoch
Global Head of Ethics and Compliance,
KPMG International and Partner
KPMG UK

Alexander Geschonneck
Global Head of Forensic,
KPMG International and Partner
KPMG Germany

Matthew McFillin
US Forensic Leader
KPMG US

Jennifer Shimek
Partner, Forensic: Ethics,
Compliance & Regulatory
KPMG US

Eliza Morris
Director,
Forensic Investigations & Compliance
KPMG UK

Acknowledgements

This report would not be possible without the invaluable analysis, insights, and production contributions of colleagues around the world.

Mariko Yamada
Director, Forensic &
Risk Advisory
KPMG Japan

Verena Hinze
Partner, Governance, Risk,
Compliance & Forensic
KPMG Germany

Martin Dougall
Partner, Forensic
KPMG Australia

Becky Seidler
Partner, Forensic Investigation,
Integrity & Dispute Services
KPMG Canada

Thais de Caumont
Senior Manager,
Advisory Forensic
KPMG France

Kevin Jin
Partner
KPMG China

Designed by Evalueserve.

Publication name: 2026 KPMG Global Chief Ethics and Compliance Officer Survey | Publication number: 140321-G | Publication date: August 2026