Stepping up to a new level of compliance

KPMG Global Chief Ethics and Compliance Officer survey

KPMG International

kpmg.com

Contents

Foreword

Public policy and regulatory activity are increasing at a rapid rate, and companies everywhere are under the spotlight. Compliance functions face multiple risks from anti-bribery and corruption, fraud and financial crime, sanctions, and, increasingly, ESG (Environmental, Social and Governance) topics like carbon footprint, modern slavery and human rights. These apply not just to the organization, but also across its value chain of suppliers, partners and other third parties.

Pressure comes from regulators, consumers, investors, employees, the media and the public. Technology, in the form of data analytics, automation and AI, offers huge potential to improve compliance performance but also brings new risks, especially regarding data privacy and security.

The Chief Compliance Officer (CCO) is at the center of this storm as companies face growing demands to meet expectations, demonstrate they are doing all they can to manage compliance risks and act swiftly to address any non-compliant activity.

About the survey

To find out how compliance leaders are addressing these challenges, KPMG surveyed 765 CCOs representative of the largest companies globally, operating in six industry sectors. The responses provide insights into their current and two-year outlook on key areas of ethics and compliance focus, including regulatory complexity, operational challenges, driving an ethical culture, ESG and evolving technology.

Annabel Reoch
Global Head of Ethics and Compliance and Partner
KPMG in the UK

Global key findings

Compliance pressures

84%

expect to face increasing regulatory expectations and scrutiny in the next two years.

Challenges ahead

34%

of CCOs say new regulatory requirements are the biggest compliance challenge, followed by data analytics (30%).

Targeting improvements

36%

rate cybersecurity as their top compliance improvement priority, followed by data privacy (35%).

ESG compliance

41%

say ESG compliance programs are still in the planning and development stage.

Technology's growing influence

70%

of CCOs anticipate an increase in technology budgets.

Workforce expansion

72%

plan to hire more compliance staff in the next year.

Compliance pressures

Navigating customer and regulatory demands

Key findings

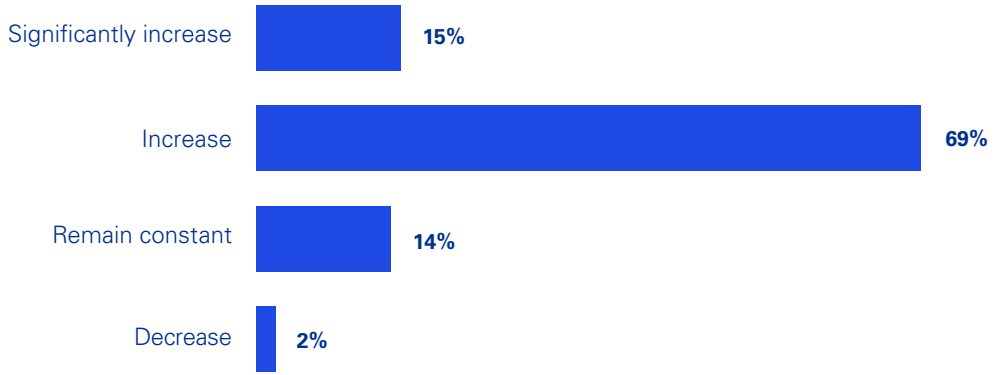
Most CCOs expect the focus on compliance to increase due to rising regulatory expectations and scrutiny, with the greatest pressure coming from customers, regulators and social policy/public perception.

Level of compliance focus

A vast majority of CCOs (84 percent) say their companies will likely face increasing regulatory expectations and scrutiny in the next two years. Interestingly, one-quarter of respondents from Canada and Europe believe expectations will significantly increase, reflecting the heightened regulatory environment in these regions. Yet, US respondents had a greater expectation that the level would remain constant, with only seven percent expecting a significant increase.

Do you expect the level of compliance focus to increase, decrease or remain constant in the next two years as compared to prior years based on regulatory expectations and scrutiny?

(Chart shows percentage of respondents who selected one option as their top choice.)



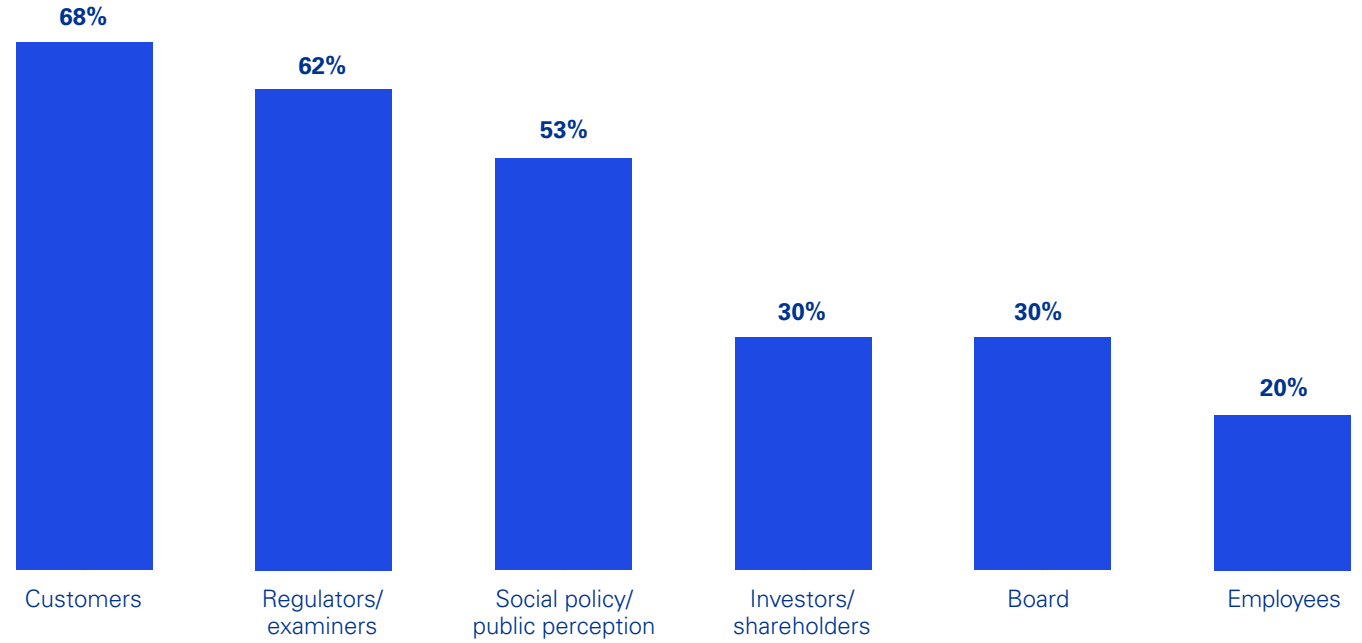
Pressure to enhance compliance

CCOs say they feel the most pressure to enhance compliance from customers (68 percent), regulators and examiners (62 percent), and social policy and public perception (53 percent). The exception is the US, where internal influences from the board and employees are seen as relatively more important, while respondents from Japan and China feel investors and shareholders have a significant impact.

When it comes to industry responses, CCOs from energy companies are the most likely to believe that social policy and public perception are the major influences. This sector is under considerable scrutiny, given its associated climate-related issues and a lack of diversity in the workforce. Women occupy only one out of five leadership roles, and they also face a higher wage gap than others.[1]

From which areas are you feeling the most pressure to enhance compliance in the coming years?

(Chart shows percentage of respondents that selected all that apply.)



[1] Ewan Thomson, "These four charts show the energy sector's gender gap and what needs to change," World Economic Forum, November 25, 2022.

KPMG insights

Key drivers behind these findings

- The pace and scale of regulatory activity is increasing compliance risks.
- Punishments can be severe, with significant fines, diversion of management time and subsequent reputational damage. In the worst instances, companies can lose stakeholders' trust which is essential to their ongoing viability and success.
- This expanding 'regulatory perimeter' increases the breadth of scrutiny and investigations, using existing regulations and jurisdictional authority. Activities increasingly under the spotlight include fraud, money laundering, carbon footprint, resource use and workers' rights — within companies and across supply chains and third parties.
- Pressure is coming from many directions, including customers, regulators, the board, employees, the public, investors and shareholders, holding companies accountable for their strategies, operations and compliance activities.
- There is no hiding place, and regulators want to see clear evidence of companies' compliance efforts, such as governance, oversight, autonomy, strong policy statements, controls and risk frameworks, data gathering and analytics, training and culture, third party due diligence, investment in appropriate skills and resources, and dynamic risk assessments. Ultimately, organizations should demonstrate "adequate" or "reasonable" procedures to ensure compliance.
- The heightened focus on corporate and individual accountability means board members, in particular, can be held accountable and responsible for compliance breaches.

> **"With more and more regulations emerging, the compliance function has a great opportunity to demonstrate its value by having frameworks and internal controls to mitigate the risk and costs of prosecution, by building a defensible position."**
>
> **Becky Seidler**
> Partner, Forensic and Dispute Advisory Services, KPMG in Canada

What should companies actively focus on?

- Strengthen the role of the board and senior management:
  - Develop a deeper understanding of compliance and build governance skills.
  - Integrate critical challenges into risk and governance frameworks.
  - Enhance policies and procedures to require more formalized documentation, mapping, and ownership and controls monitoring and testing to improve transparency.
  - Build a robust data gathering and analytical capability.
  - Elevate compliance to the level of other strategic functions and ensure comparable investment, staffing and technology. In addition, consider upskilling in areas associated with emerging risks (e.g. data analytics).
  - Regularly review and consider CCO and management reports on compliance risks (including reputation risk, emerging risks, etc.) and potential impacts on business strategy/decision-making, risk management, the overall compliance function, and governance and oversight.
  - Consider both current and past violations, trends and emerging risk mitigation.
  - Ensure reporting, disclosures, public statements and marketing are consistent, accurate and aligned with the company's strategies and activities.
  - Embed a culture of compliance with clear accountability.
- Monitor stakeholder activity, including shareholder proposals, investor expectations, social media posts (public and employee), consumer complaints and whistleblower activity. As appropriate:
  - Ensure timely, accurate and complete responses.
  - Track relevant documents, reporting and regulatory audits.
- Continually monitor the evolving regulatory environment and associated reporting requirements to stay on top of new regulations.

Challenges ahead

New regulations and data analytics top list of looming challenges

Key findings

CCOs say that new regulatory requirements (34 percent) are the greatest challenge to their compliance efforts over the next two years. Data analytics and predictive modeling come a close second (30 percent) as companies strive to identify and collate reliable, accurate data to monitor and report their compliance efforts.

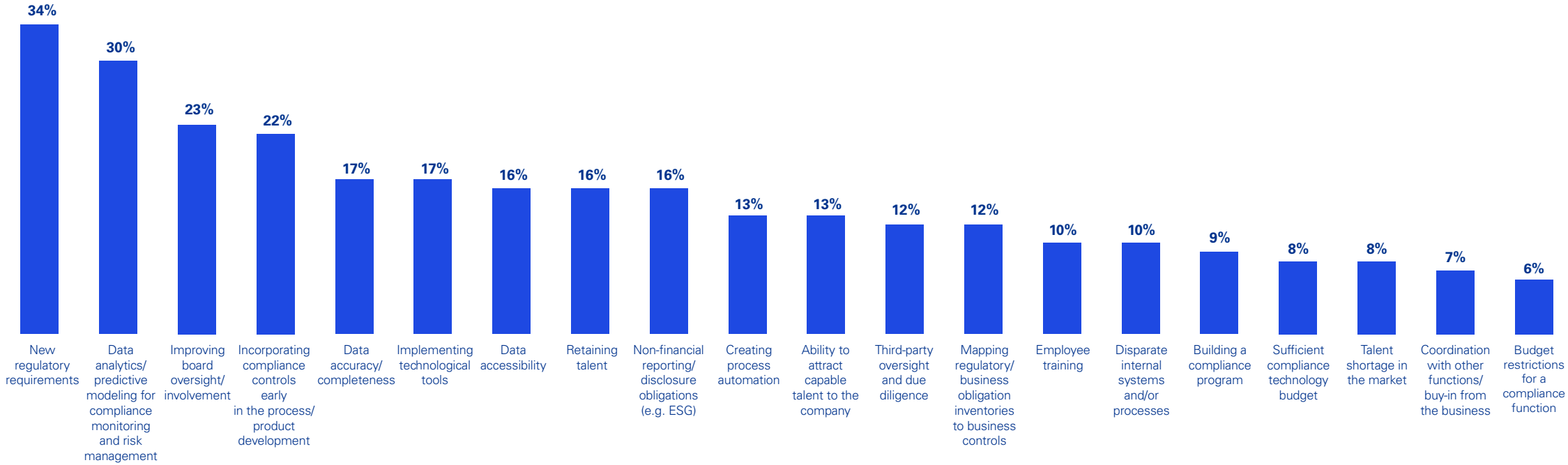
Top compliance challenges

Respondents also cite the need to improve board oversight and involvement and incorporate compliance controls early in process and product development. In the Asia-Pacific region, CCOs see talent retention as the greatest challenge, reflecting the acute skills shortages. For survey participants from China and Japan, ESG reporting comes first — as non-financial disclosure becomes mainstream.

From a sector perspective, compliance controls are especially important to energy company CCOs (39 percent), while respondents from technology, media and telecommunications companies are concerned about data analytics (37 percent).

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

(Chart shows percentage of respondents who selected each challenge in their top three choices.)



KPMG insights

Key drivers behind these findings

- An intense level of rulemaking, guidance and enforcement activity, including:
  - The US Securities and Exchange Commission (SEC) disclosure proposals on cybersecurity, climate, insider trading and claw back policies, and US Federal Trade Commission (FTC) guidelines on mergers, fair competition and data use/privacy.
  - Also, in the US, the Department of Justice (DOJ) has revised its Corporate Criminal Enforcement Policy to enhance corporate ethics and compliance.
  - In the UK, the Economic Crime and Corporate Transparency Act has fraud and corruption in its sights, while in the EU, the General Data Protection Regulation (GDPR) governs how data is used, processed and stored. Other European regulations include the German Supply Chain Due Diligence Act and the EU Whistleblower Directive.
  - Asia places a big priority on financial crime, with the Hong Kong Monetary Authority (HKMA) stating its aim to tackle fraud and the use of mule accounts to launder money, and the Monetary Authority of Singapore announcing a National Strategy for Countering the Financing of Terrorism.
  - Ukraine sanctions present further challenges, especially for companies in countries that have built up strong links to Russia.
  - Countries are issuing 'whole-of-government' multi-agency directives on regulatory policy matters, including cybersecurity, data governance, fairness and ESG. However, regulatory disparities remain across global, national and federal regulations and enforcement.
  - New developments, applications and evolving technologies, such as AI, increase regulatory scrutiny and are likely to lead to more regulations, especially enlight of the provisional EU AI Act.
  - These trends put pressure on compliance departments to introduce data-driven compliance programs, embed controls upfront and throughout process lifecycles, use new compliance tools and technology, and maintain well-staffed teams of experts.

"It's important for companies to have a proactive detection mechanism so they can take action. In an increasingly digitalized world, the control environment has lagged, leaving CCOs short of the data they need. Fully digitized controls, augmented by AI and machine learning (ML), can drive efficiency up and costs down and quickly detect fraud, misconduct and money laundering."

Lem Chin Kok
Partner, Asia-Pacific Forensic Leader
KPMG in Singapore

What should companies actively focus on?

- **Regulatory:** Address the complexity of the increasing number of new regulations and potentially divergent requirements by:
  - Enhancing coordination between compliance, government affairs, legal and public relations to assess strategic, operational and reputation risks from evolving rules.
  - Establishing a robust process to identify, track and integrate new laws and regulations into a centralized repository.
  - Initiating and maintaining dialogue with existing and new regulators.
  - Understanding where regulators are coordinated and where they diverge, especially regarding enforcement and penalties.
- **Data analytics and modeling:**
  - Prioritize investment in and transformation of the compliance program, monitoring emerging technologies and tools, and updating, integrating and consolidating programs and systems so that all relevant data flows to the compliance team.
  - Pilot new technologies and processes to demonstrate business value, operational improvements and build a larger business case (see Technology section).
  - Use data analytics to conduct monitoring and to provide insights and meaningful reporting to different stakeholders to raise awareness of risk and prioritize enhancement activities.
- **Integrated compliance view:** Pull together all the various strands of compliance, including AML, anti-bribery and corruption, cyber, data privacy, ESG, etc., into one risk oversight function. This can provide an integrated view of risk exposures and identify where there are efficiencies in the control environment that can be leveraged.
- **Talent:** Build the status and reputation of the compliance function to increase its autonomy, authority and investment, including sufficient, skilled staffing, training and development, in particular upskilling in areas associated with emerging risks and adoption of emerging technologies. (See the Workforce expansion section.)

Targeting improvements

CCOs focusing on cyber and data privacy

Key findings

With regulators increasingly focusing on data, respondents consider cybersecurity (36 percent) and data privacy (35 percent) as their top two process improvement priorities, followed by product safety and people's health and wellness.

Top areas to improve

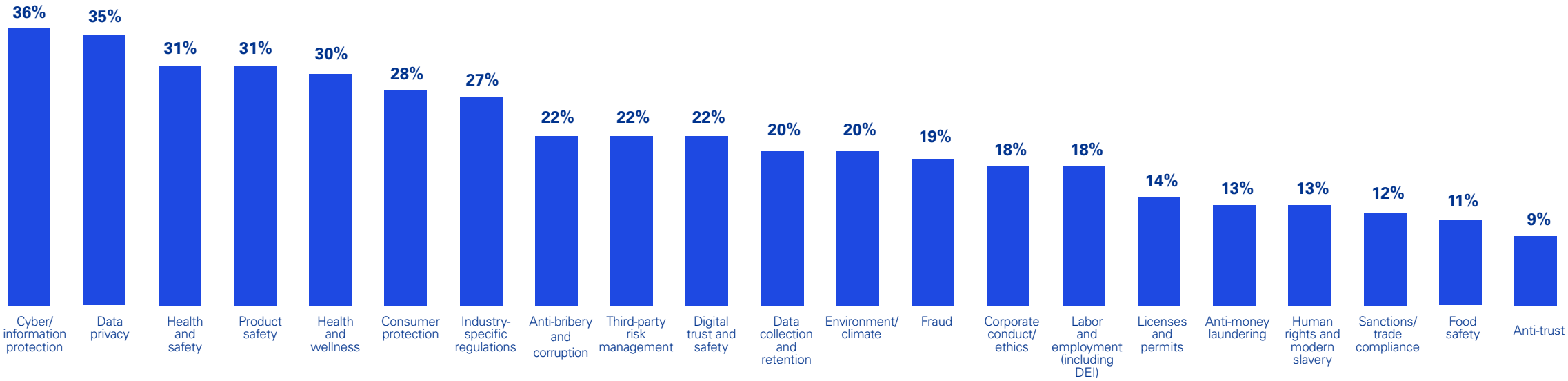
Digitalization and the growing use of AI, automation and analytics bring new risks. Companies are particularly conscious of the fines and reputational damage of cyber and data incidents. ESG, including employee well-being, is another emerging challenge CCOs are keen to embed into their processes.

Respondents from the US are most concerned about industry-specific regulations (45 percent), reflecting the heightened compliance environment. The introduction of GDPR should explain why data privacy is such an important topic for CCOs from European companies (50 percent). In Asia-Pacific, on the other hand, environment and climate has the highest response, followed by fraud. Indeed, fraud is the number one area Australian CCOs focus on (47 percent) to improve their processes and controls.

Digging deeper into different industries, healthcare and life sciences respondents say they are especially keen to carry out process improvements in health, safety and employee well-being (88 percent). In the energy sector, where projects are often based in developing nations, human rights and modern slavery receive the highest score (78 percent).

What processes are targeted for improvement related to compliance obligations?

(Chart shows percentage of respondents who selected each challenge in their top five choices.)



Demonstrating business value

According to the CCOs surveyed, communications (64 percent) and reporting (62 percent) are the two preferred routes to demonstrate the business value of compliance. Promoting a compliance culture also scores highly, whereas corporate conduct and ethics ranks low (with a score of just 18 percent), suggesting that companies should be careful that their compliance message is consistent with their actual behavior.

Respondents from US companies stood out from other regions by emphasizing technology and AI (51 percent) as a tool for showing value. It's a similar story for CCOs from the technology, media and telecommunications sector, who place a higher value on the power of technology (77 percent) than their peers in other industries.

In order to demonstrate the business value of compliance, which areas do you hope to enhance within the next one to two years?

(Chart shows percentage of respondents who selected each area in their top three choices.)

KPMG insights

Key drivers behind these findings

- With a stream of new regulations and heightened scrutiny, businesses are under pressure to show that they deliver value from compliance through ethically strong cultures, the use of cutting-edge technology and clear accountability.
- National regulators increasingly demand cross-agency collaboration via initiatives such as the US SEC cyber risk management proposals, the Federal Trade Commission (FTC) data safeguards rule and Certified Information Systems Auditor (CISA) incident reporting.
- Consumer protection is a growing focus centered around fairness, data privacy and use, fraud and scams. With regulations like GDPR, companies need to show they are taking adequate steps to prevent data misuse.
- Third-party risk management is also on the regulators' agenda, including the proposed EU Corporate Sustainability Due Diligence Directive (CSDDD) and other directives looking at cybersecurity, operational resiliency, data use and privacy, emissions, use of raw materials, and human rights.
- The expanded use of sanctions and trade restrictions, coupled with complexities in areas such as beneficial ownership, means that companies need strong visibility over their global operations to remain compliant.

> **"We need an integrated view of compliance that covers money laundering, bribery and corruption, plus cyber and data, rolled into one risk oversight function. By moving these topics together, companies can share data, take a similar approach to risk and assurance, use standardized controls, and give a more complete picture of risk exposure."**
>
> **Alex Geschonneck**
> Partner, EMA Forensic Leader, KPMG in Germany

What should companies actively focus on?

- Companies should seek to optimize their compliance programs through:
  - Greater collaboration between compliance, senior leadership and the board, as well as with IT, legal, procurement and other departments responsible for areas that fall within the remit of compliance, like data security and third-party engagement.
  - Assessing regulatory change management processes and ensuring they fully capture applicable global, local, federal and state regulations — and relevant divergences.
  - Identifying which compliance areas are most relevant and result in the greatest risk to the organization and assigning clear responsibilities for managing those risks.
  - Monitoring emerging risks such as fraud, ESG and AI — and working with internal stakeholders to determine if new controls need to be integrated into existing frameworks or if new compliance policies are needed.
  - Evolve identity and access management programs for employees, customers and vendors to address cyber and data privacy threats.
  - Embed fairness across all customer impact points from product and service design, marketing and advertising, disclosures, servicing, customer interactions (including complaints management), and M&A activity.
  - Facilitate easy information exchange internally and with business partners to enable supplier due diligence and ongoing compliance. Execute dynamic third-party risk assessments and assess whether third-party risk management meets or exceeds global and jurisdictional regulatory expectations (e.g. anti-bribery and corruption, data privacy, anti-money laundering (AML), modern slavery and sanctions).
  - Monitor geopolitical events, sanctions activity and regulatory requirements in areas related to cybersecurity, data privacy, beneficial ownership and trade finance.

ESG compliance

A work in progress

Key findings

Just seven percent of CCOs say their ESG compliance programs are fully developed and operational, reflecting the evolving nature of sustainability. Half of respondents have implemented their programs, with 41 percent still in the planning and development stage. Policy management is the number one area marked for development.

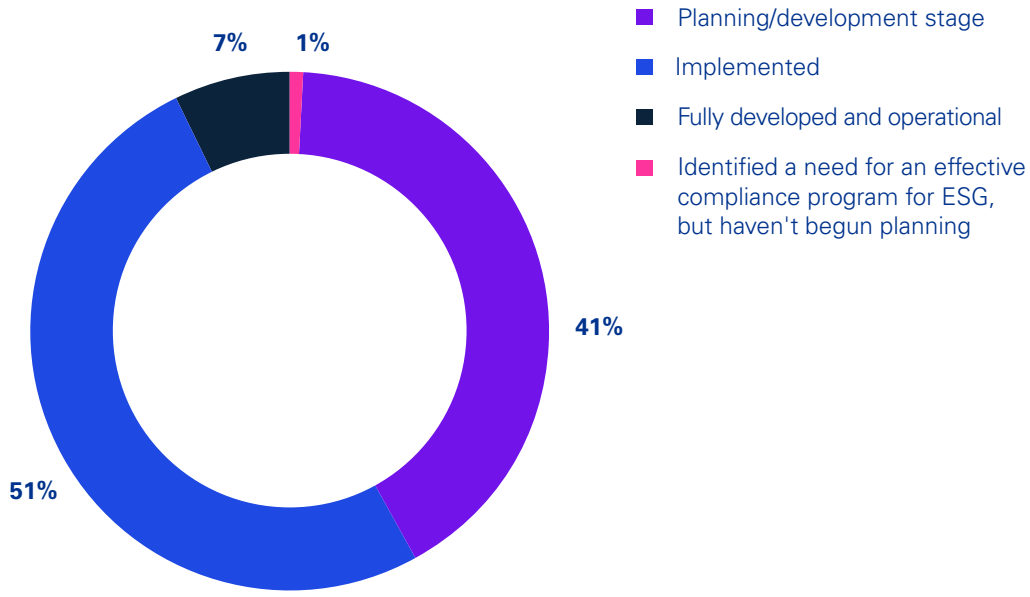
Early on the maturity curve

ESG compliance is still in a relatively nascent phase, as companies absorb new regulations and consider the transition to net zero, low waste, circular business models and social impact. The majority of respondents are at the planning or implementation stage.

The responses are fairly consistent across geographies. Chinese companies surveyed are ahead in implementing programs (59 percent), while those from Australia are playing catch-up (43 percent). More than two-thirds (65 percent) of CCOs from energy companies say their organization has implemented its ESG compliance program, which likely reflects the pressure on this industry to become more sustainable.

How would you assess the maturity level of your compliance program for ESG?

(Chart shows percentage of respondents who selected one option as their top choice.)

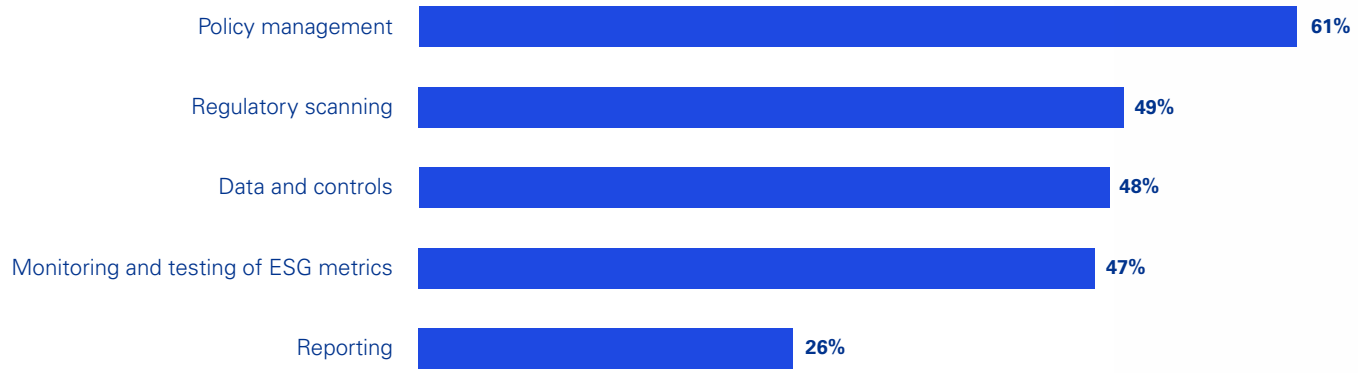


Areas for improvement

CCOs aim to enhance several areas of compliance in the next two years. Respondents from Canada and Europe are prioritizing policy management as they adapt to highly regulated environments. In Asia-Pacific, there is a strong focus on the monitoring and testing of ESG metrics. Participating companies from the financial services sector are most likely to want to improve their data and controls to keep up with regulators' expectations.

In which areas do you most want to mature your compliance program for ESG in the next two years?

(Chart shows percentage of respondents who selected each area in their top three choices.)



KPMG insights

Key drivers behind these findings

- Continually evolving requirements from local, national and international regulations. Public policy and stakeholder sensitivities around ESG, causing operational challenges and reputational risk. Customers, employees and investors may avoid companies who can't demonstrate strong ESG credentials as it relates to sustainability, diversity and workforce relations.
- ESG may not be fully aligned with and integrated into corporate strategy, which may mean that metrics are neither comprehensive nor reliable, increasing greenwashing risk. Business units may, therefore, struggle to implement the company's ESG strategies and policies.
- Many companies lack a coherent approach to ESG compliance in terms of tracking regulations, assessing risks, and gathering, sharing and reporting information. This can hinder the design and implementation of an ESG compliance program.

> **"As companies are increasingly being held to account by multiple stakeholders, it's critical to embed controls to help address environmental and social impact and avoid greenwashing. CCOs have a key role in the design and implementation of a robust framework that's aligned to the Corporate ESG Strategy, helping to ensure ESG risk is monitored and reported data is complete and accurate."**
>
> **Annabel Reoch**
> Global Head of Ethics and Compliance and Partner, KPMG in the UK

What should companies actively focus on?

- Enhance coordination between government affairs, legal, compliance, public relations, and business units to assess strategic, operational, and reputational impacts of emerging risks, laws, and regulations.
- Drive awareness of evolving regulatory risks, the current state of preparedness and risk assessment, and the strengthening of risk mitigation controls.
- Build teams focused on country-specific reporting requirements.
- Align voluntary and mandatory reporting and identify any contradictions between reporting jurisdictions.
- Accelerate the ESG compliance program by:
  - Establishing areas of business, including compliance, that take explicit accountability of the E, S and G.
  - Working with internal stakeholders to determine if new ESG controls need to be designed and integrated into an existing framework.
  - Positioning compliance as a coordinator and collaborator with senior leadership and the board, as well as ensuring appropriate investment in the ESG compliance function.
  - Ensuring the company can navigate local, national and global requirements aligned to its ESG commitments.
  - Integrating diversity into recruitment, training and career development with clear targets.
  - Ensuring that the company's Supplier Code of Conduct sets expectations for suppliers and their staff consistent with the company's ESG strategies, policies and commitments. Periodically review suppliers' compliance with agreed standards for products, facilities, business practices, and supply chain and with applicable regulations.
  - Ensure that all communications and reporting are validated to avoid errors or accusations of greenwashing.
  - Using ESG as a value driver for ethical business practices and good corporate citizenship.

Technology's growing influence

Compliance technology budgets on the rise

Key findings

Most respondents feel that technology budgets will increase, focusing on data analytics, cybersecurity and data privacy, and process automation. Most companies are some way off achieving technology maturity, especially regarding automation and AI.

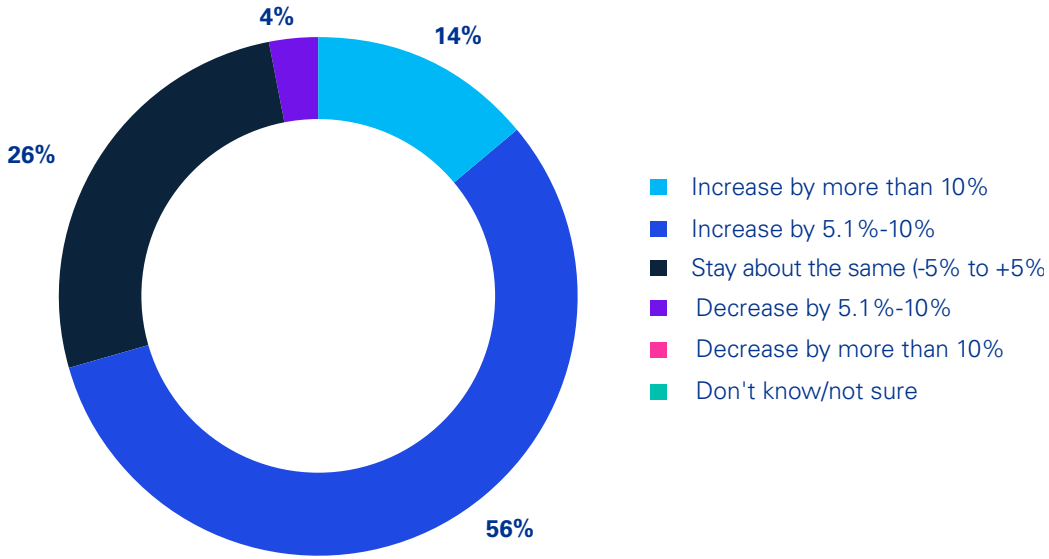
Optimism over budget increases

Seven out of ten CCOs surveyed expect their technology budgets to increase, with 56 percent anticipating a five to ten percent hike. German executives are the most optimistic — 23 percent say budgets should increase by more than 10 percent. At the other end of the scale, a higher proportion of Australian CCOs say their technology budgets will fall.

Compared to other sectors, respondents from healthcare and life sciences, industrial manufacturing, and consumer and retail companies are less hopeful of budget increases.

How will your technology budget for your ethics and compliance function change in the next year as compared to the following year?

(Chart shows percentage of respondents who selected each area in their top three choices.)

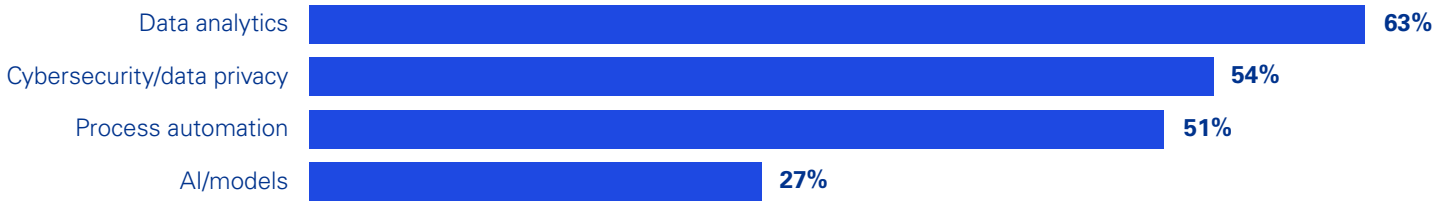


Where is the extra budget going?

Data analytics is the top area for investment (63 percent), followed by cybersecurity and data privacy, and process automation. When looking at different sector priorities, energy sector respondents are heavily oriented towards process automation (84 percent), while their peers in technology, media and telecommunications plan to invest significantly in AI (75 percent) — the latter are at the center of AI developments and may have a firmer idea about how to use this exciting technology.

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

(Chart shows percentage of respondents that selected all that apply.)



Emerging technology maturity

Across the respondents, there is limited automation maturity, with one-third (33 percent) using bots for repetitive manual processes and just 23 percent harnessing data analytics and predictive modeling for compliance monitoring and risk management. Virtually none of the respondents say they leverage AI to perform more complex decision-making.

Interestingly, US CCOs appear ahead of the rest of the world in using ERP solutions and data analytics but are less likely to utilize bots.

How would you assess compliance's current level of automation maturity?

(Chart shows percentage of respondents who selected one option as their top choice.)

Automation priorities

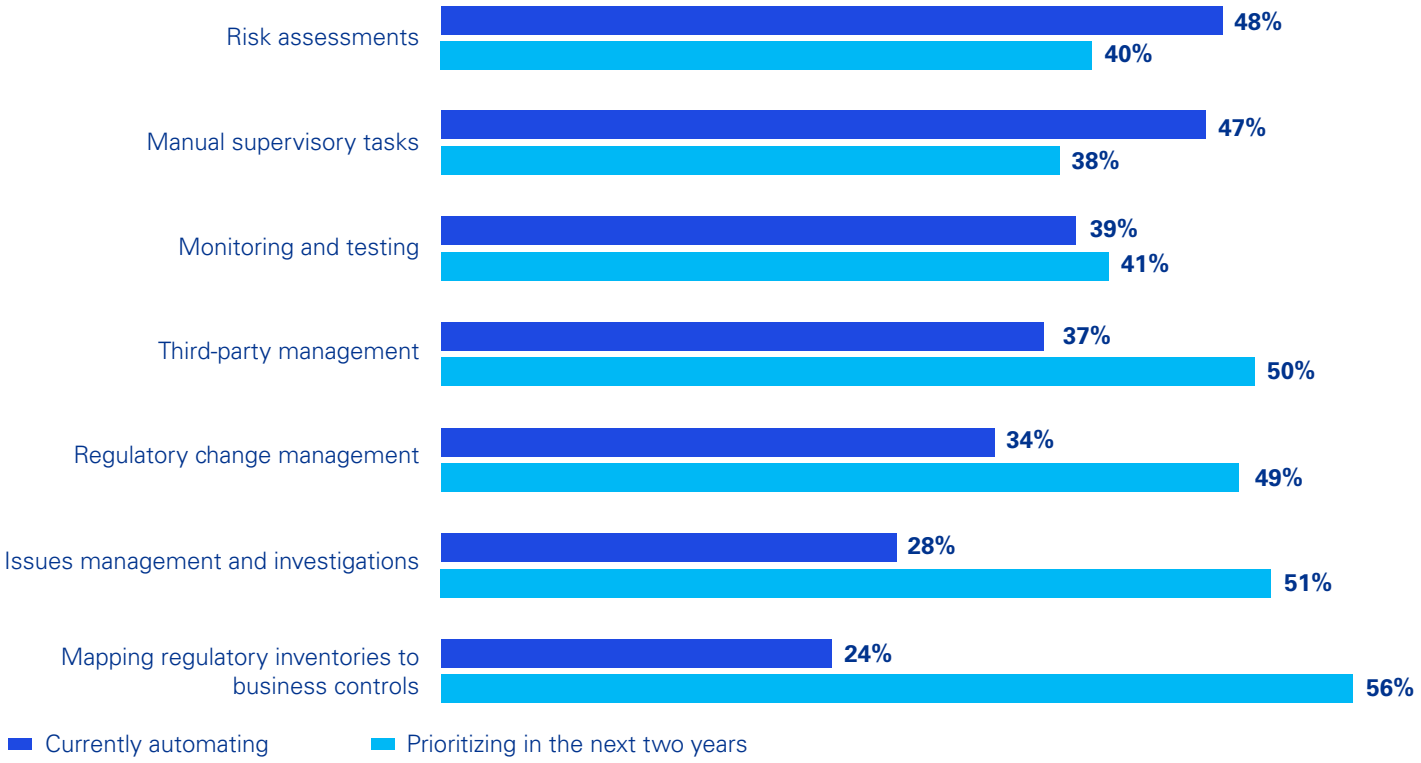
Over the past two years, many companies have begun automating processes. Building on this effort, CCOs have prioritized automating the following areas over the next two years:

- Risk assessments
- Monitoring and testing
- Issues and investigations
- Regulatory mapping
- Manual supervisory tasks
- Regulatory change management
- Third-party management

According to the survey, US companies are ahead in automating monitoring and testing and third-party management (58 percent and 51 percent, respectively). However, companies from Australia and Japan are most likely to have automated risk management and investigations. Asia-Pacific respondents generally appear behind the curve in terms of automation maturity.

Which of the following ethics and compliance areas are you currently automating? Which areas have the greatest priority to automate in the next two years?

(Chart shows percentage of respondents that selected all that apply.)



KPMG insights

Key drivers behind these findings

- Heightened regulatory scrutiny of new technology such as digital devices, AI, machine learning (ML), automation, advertising and model bias.
- Regulators increasingly expect:
  - Technology resiliency across legacy and newer systems, threat and vulnerability detection, mitigation and remediation and continuity planning.
  - Technology risk management, including risk assessments, monitoring and controls.
  - Operational resiliency, including governance practices to maintain critical operations and cyber and third-party risk management.
- Growing regulatory focus on consumer data privacy, collection, use, retention and disposal — companies are under pressure to monitor transactions and staff more closely. However, CCOs are grappling with multiple ERP systems across countries as they try to achieve real-time monitoring. Control environments have not digitalized at the same pace as the rest of the business.
- Strong focus on cloud adoption and compliance performance of service providers.
- Evolving conversation on AI, including:
  - Design, use and deployment of automated systems
  - Creating safe and effective systems
  - Algorithmic discrimination protection
  - Data privacy
  - Consumer notice and explanation
  - Human alternatives, considerations and fallbacks.
- Addressing the need for technology and data-driven skills to implement compliance programs and tools.

"Technology and data analytics investment in the ethics and compliance function is no longer a 'nice-to-have'; it's a necessity to help mitigate, measure and identify risk."

Amy Matsuo
Principal and National Leader,
Compliance Transformation and Regulatory Insights,
KPMG in the US

What should companies actively focus on?

- As companies invest in technology, data analytics and automation, they should consider 'privacy-by-design' — embedding consumer privacy into new technologies to prevent privacy vulnerabilities from malware, fraud, identity theft, insider risk and reputation risk.
- Companies should prioritize investment in and transformation of their compliance programs, acknowledging the value it brings:
  - Encourage a data-driven culture.
  - Phase in new technologies and processes through pilots to demonstrate business value and operational improvements and build a larger business case.
  - Effectively use data analytics to identify highest risk transactions for review and monitoring.
  - Evaluate, integrate and automate metrics to generate compliance insights.
  - Scale up predictive monitoring.
  - Implement a data-driven approach to compliance, including strong data governance, resourcing, controls and automation to continuously improve.
  - Harness AI and automation to conduct fast, comprehensive data searches that spot risks internally and across the supply chain.
  - Periodically assess the effectiveness of new technologies and processes and revise as needed.
  - Monitor emerging technologies and tools and update programs.
- Demonstrate to regulators effective board reporting and oversight of technology and associated risks, including:
  - Quality and timeliness of operational and risk metrics.
  - Depth of insight and transparency provided by senior management and risk metrics.
  - Meaningful challenge and corrective action tracking.
  - Periodic review of risk appetite and tolerances.

Workforce expansion

Compliance functions set to boost workforce numbers

Key findings

Despite economic uncertainty, most CCOs anticipate increasing the number of full-time employees in the next year. Ethics and compliance training is high on the agenda to improve performance, as well as leveraging skillsets from other business functions.

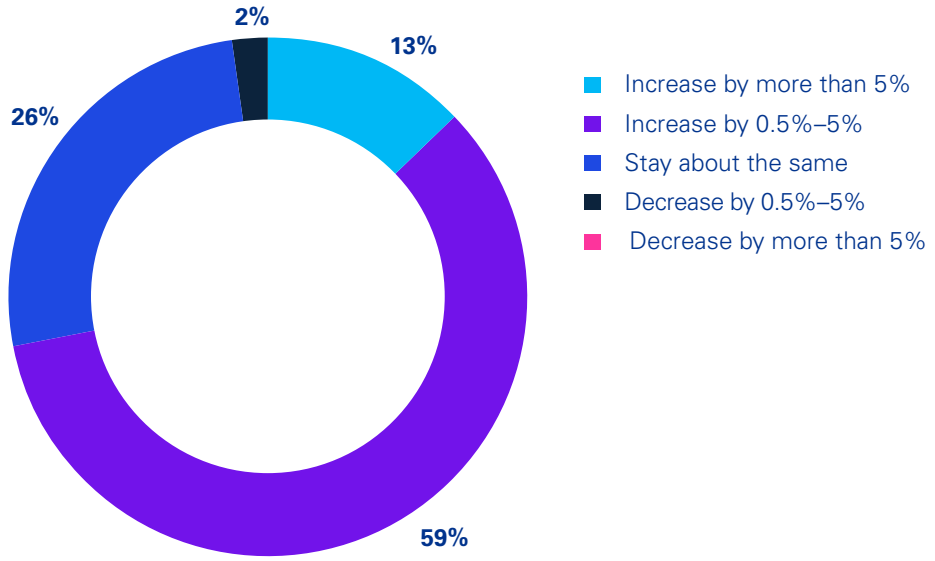
On a hiring mission

The majority of CCOs (72 percent) say they plan to hire more staff, with most expecting a modest increase of up to five percent. Respondents from France and Germany have the most ambitious recruitment targets, as do energy companies — a potential consequence of the robust regulations impacting these geographies and industries.

In Asia-Pacific, talent retention is cited as the biggest compliance challenge over the next two years, reinforcing the need to bring in new people and engage current staff. This region hosts many fast-growing companies, putting compliance skills in high demand. Higher salaries in more developed markets may also lure away high level people.

How will the number of full-time employees within your ethics and compliance function change in the next year?

(Chart shows percentage of respondents who selected one option as their top choice.)

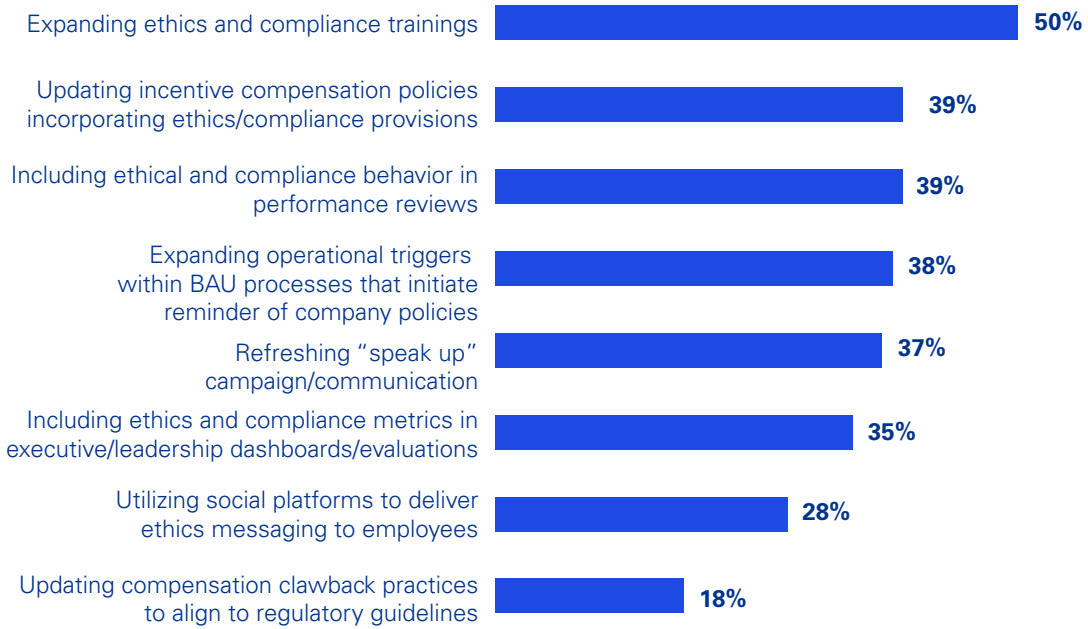


Forging a compliance culture

Expanding ethics and compliance training (50 percent) is the prime tactic for promoting compliance behavior and culture. CCOs also plan to include appropriate compliance behavior in performance reviews, incentive plans and leadership KPIs.

What areas are you expanding to help promote/incentivize compliance behavior/culture?

(Chart shows percentage of respondents who selected each area in their top three choices.)

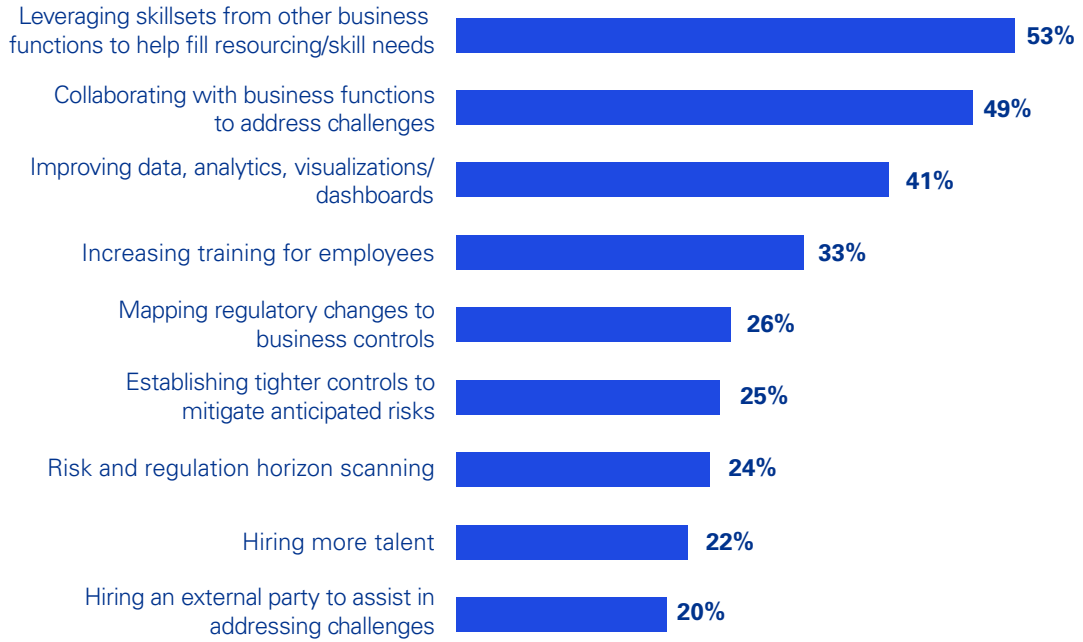


A 'whole of business' effort to tackle compliance challenges

CCOs taking part in the survey acknowledge that the compliance function alone cannot address the many ethics and compliance challenges facing their organizations. The top response (53 percent) is to leverage skillsets from other business functions to help fill resourcing and skill needs.

How are you equipping yourselves to prepare for these challenges?

(Chart shows percentage of respondents that selected all that apply.)



KPMG insights

Key drivers behind these findings

- Companies face growing regulatory scrutiny and increasing reporting requirements, with boards under pressure to demonstrate compliance effectiveness.
- In a harsh and uncertain economic climate, companies should show their commitment to ethics and compliance by investing in resources.
- There are more and more regulations and enforcement relating to accountability:
  - Promoting and supporting a culture of compliance, including voluntary self-disclosure through incentives and metrics.
  - Hold accountable individuals who commit and profit from misconduct.
  - Enforcement actions against executives for unethical sales practices, misleading disclosures and other unacceptable actions.

What should companies actively focus on?

- Empower the compliance function to give it a stature comparable to other business functions, with greater autonomy to make important decisions.
- Invest in compliance to ensure sufficient people, skills, and critical technologies and build a strong employee value proposition to attract and retain talent.
- Regularly assess compliance employees' skills to identify gaps and opportunities for repurposing their skills for best advantage.
- Enhance the compliance program to include both incentives and deterrents related to individual accountability, compliance metrics and measurements, and corporate culture.
- Identify and report any issues promptly, with clear escalation and resolution procedures, including measures to hold responsible individuals accountable.

> **"To address the talent gap, CCOs can foster a network of specialists who have a day-to-day role in the business but also have a 'compliance hat.' The range of required skills extends to automation, data analytics, cyber and data protection, and it's essential to be able to call on subject matter experts around the organization."**
>
> **Annabel Reoch**
> Global Head of Ethics and Compliance
> and Partner
> KPMG in the UK

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 the board and committee(s) regularly updated on regulatory and compliance changes, including regulatory examination and enforcement expectations?

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?

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 of retaliation?

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?

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?

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 testing

- 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?

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?

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?

How this connects with what we do

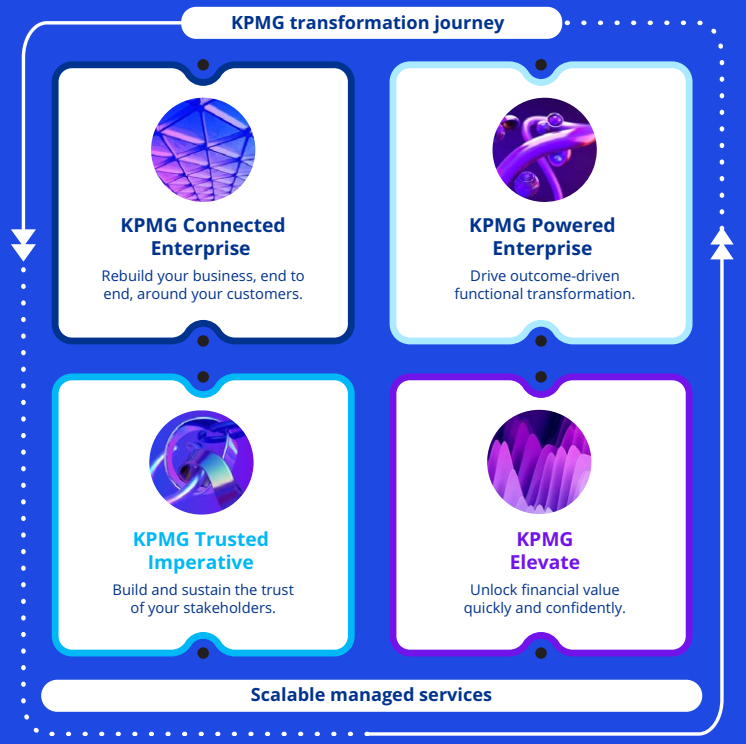
Threats to organizational integrity are increasing, whether from within or outside the organization. Fraud, corporate crime, commercial disputes, litigation, data security and regulatory requirements can impact finances, integrity and reputation. There is also the increasing sophistication of organized crime and terrorism, as well as new challenges from technology, cross-border disputes, emerging markets, complex supply chains and intellectual property theft. Proactively monitoring and responding to these risks can help mitigate threats, enhance resilience and build trust.

KPMG forensic professionals extend across a multitude of dimensions, from bolstering controls and helping ensure compliance to conducting meticulous investigations and developing integrated solutions. Anchored in these efforts is the cultivation of trust — an indispensable foundation for sustainable success.

KPMG firms' professionals encompass a diverse range of skills, including forensic accountants, investigators, data scientists, compliance practitioners and cyber response experts. From proactive prevention to meticulous detection and resolute response, we focus not just on mitigating risks but also shielding you from reputational and financial impacts.

Learn more at: kpmg.com/forensic

In addition, KPMG firms' suite of business transformation technology solutions can help you engineer a different future — of new opportunities that are designed to create and protect value.



How KPMG in Poland can help you?

KPMG advises clients at all stages of fraud risk management. We offer fraud prevention and detection services, as well as advice on regulatory and litigation matters. We support businesses in implementing effective compliance systems, conduct investigative audits, detect irregularities and provide up-to-date expertise on how to avoid potential losses from fraud.

Forensic services at KPMG in Poland

Investigative audits

Investigative audits make it possible to detect the causes of fraud and irregularities, to determine their extent and their impact on company operations. KPMG can also secure the necessary evidence for further disciplinary or judicial proceedings.

Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)

KPMG conducts detailed compliance assessment of existing policies, procedures and related processes against national and international AML/CFT regulations and market best practices, tailoring the proposed solutions to the client organisation's business needs.

Computer forensic

KPMG has the tools and experience to obtain and analyse digital evidence from a variety of sources, such as data from financial/accounting systems. We can identify suspicious transactions, irregularities, links between entities or attempts to manipulate financial data.

Counteracting corruption

KPMG conducts independent reviews and assessments of the client's anti-corruption controls and internal procedures. We also provide professional support to clients in reviews related to regulations in other countries, such as the FCPA (Foreign Corrupt Practices Act) or the UK Bribery Act. We work closely with our clients, ensuring that the proposed solutions are appropriately tailored to the needs of their organisations.

Business intelligence

KPMG provides business intelligence services, including the search, review and analysis of publicly available information about individuals and business entities, their business relationships, financial situation, as well as their modus operandi and strategy. KPMG has advanced tools to support and automate due diligence analysis, providing access to a wide range of data sources from many countries around the world.

Whistleblowing

KPMG offers comprehensive assistance in designing and implementing a whistleblowing system. We support clients in handling whistleblower reports and conducting internal investigations. We offer an online platform that enables both whistleblower reporting of abuse and the management and handling of reports by organisations. Moreover, we support clients in conducting internal investigative work.

Iwona Sprycha
Partner
Head of Forensic and Dispute Services
Deal Advisory
KPMG in Poland
M: +48 692 403 605
E: isprycha@kpmg.pl

Zbigniew Czyżewski
Associate Director
Forensic and Dispute Services
Deal Advisory
KPMG in Poland
M: + 48 509 413 383
E: zczyzewski@kpmg.pl

KPMG's ESG compliance services

Challenge

A wide range of ESG-related issues require constant monitoring of both the external environment (legislative, financial), as well as internal data, rules and strategies.

Opportunity

KPMG services can help in strengthening internal knowledge and understanding of ESG-related risks and compliance requirements, allowing for a consistent and holistic corporate approach.

Selected services:

ESG diagnosis and strategy

Getting to know the way the company includes environmental, social and governance considerations in their operations – as well as how external ESG conditions influence its business model – can be a first step in creating a coherent strategy, forming a coherent vision as well as allowing the creation of suitable compliance tools.

Climate and ESG risk analysis

Understanding the regulatory and financial environment and wider economic, social and environmental trends shaping the market will lead to a more resilient business model, allowing for adequate resource allocation for priority areas – including in compliance.

CSRD-compatible ESG reporting

The sustainability reporting challenge in the European Union in the coming years will have a growing influence on the market – both for companies with legal obligations to disclose their ESG metrics, as well as for those in supply chains of business partners required to act. This will lead to a wider market shift that require a robust compliance analysis.

ESG Due Dilligence in M&A

Checking the way a corporate merger or acquisiton may influence ESG ratings or indicators is becoming a source of interest due to issues of compliance or access to finance that becomes a challenge as banks and other entities decide to limit their exposure, eg. to fossil fuels and practices seen as incompatible with the green economic transition.

Sustainability as a Service (SaaS)

As ESG issues establish themselves as a clear, long-term market trend a growing trend in sustainability-related knowledge building and sharing practices follow. Despite that fact companies feel that the access to a well-qualified specialists in ESG issues remains limited due to a rising need for their services. KPMG expert support aims to bridge this gap.

KPMG ESG Digital Toolbox

Well designed digital tools can help in ESG-related data gathering, allowing for better compliance policies and practices. We offer a wide range of such tools that can be tailored to sector- or company-specific needs, whose use will help in creating coherent answers to ESG-related risks, including (but not limited to) compliance issues.

Justyna Wysocka-Golec
Partner Associate
Head of ESG, Climate & Nature Consulting
KPMG in Poland
M: +48 664 718 815
E: jwysocka-golec@kpmg.pl

KPMG's Cyber Security services

Why KPMG

Our security experts performed **over 1000 cyber security assingments** for Polish and international clients (including **pharmaceutical sector**)

We actively participate in branch organizations (e.g. we are leading **OWASP** Chapter in Poland)

We share our **knowledge** on security conferences,post graduate studies and mentoring **SANS Institute** in the area of applications security

Our deep technical cyber security skillshare confirmed with numerous **certifications**

We understand today's advanced cyber threats, since our penetration tests revealed many **zero-day vulnerabilities** in applications utilized all over the world

We ensure the security of processed data of our customers - the information security management system implemented in our organization has been certified for compliance with **ISO 27001**.

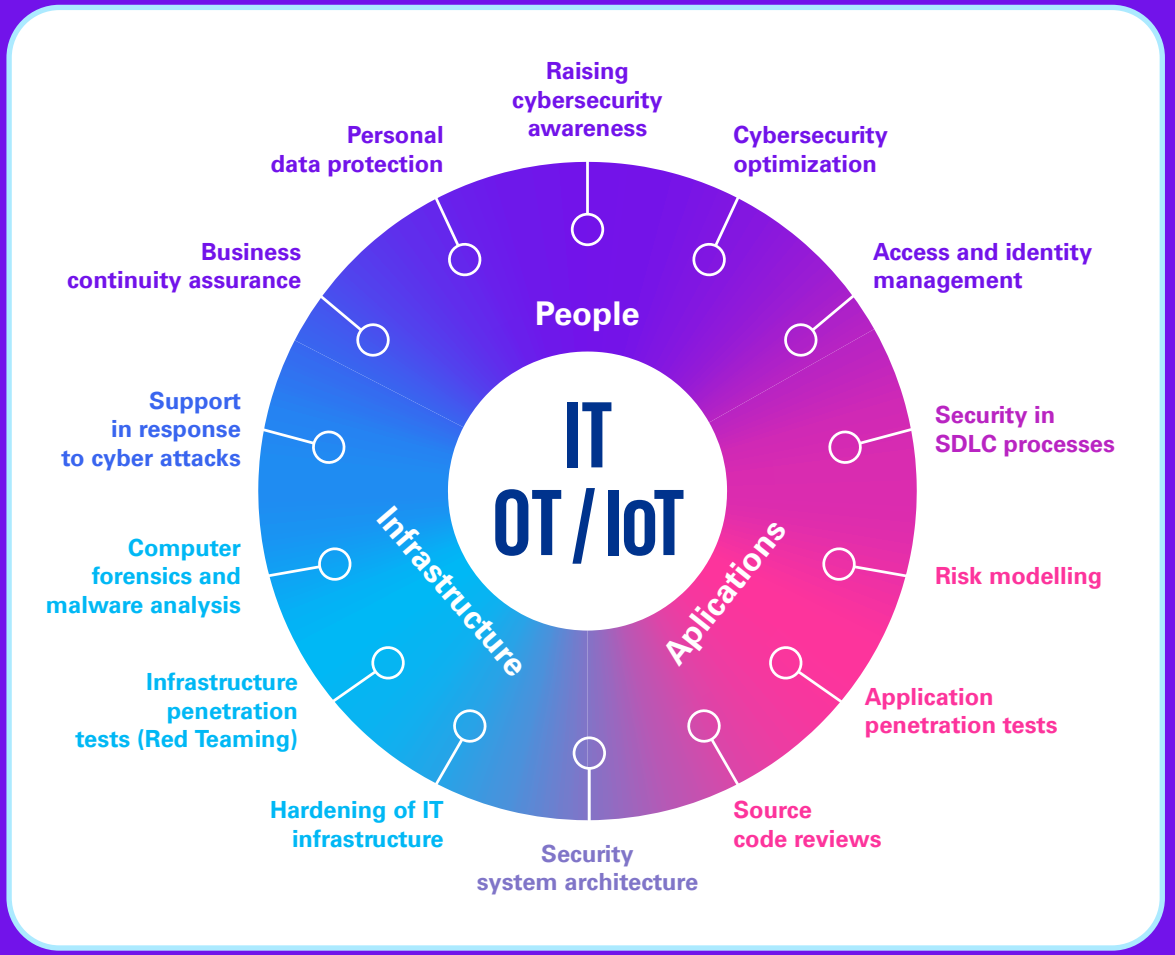
Cyber Security Team in Poland

In order to meet the expectations of its customers, KPMG has built a regional competence center in Poland, employing experts with deep technical knowledge and extensive experience gained during the implementation of hundreds of ICT and ICS security projects in Poland and all over the world.

The Cyber Security team provides a wide range of advisory services, taking a comprehensive approach to information protection.

We support our clients in securing infrastructure, applications and taking care of the human factor, i.e. proper organization, processes and employees' knowledge in the field of information protection.

We help our clients both in preparing for cyber-attack defense and in taking appropriate actions when a cyber-attack has already taken place.



Michał Kurek
Partner
Consulting
Head of Cybersecurity
in Poland and CEE
KPMG in Poland
M: +48 660 440 041
E: michalkurek@kpmg.pl

Research methodology

KPMG surveyed 765 Chief Ethics and Compliance Officers (CCOs) from large companies across various countries. To ensure the accuracy of the results, the survey data was normalized to account for the larger response population from the US.

Australia: 75	China: 75	Germany: 75	UK: 75
Canada: 75	France: 75	Japan: 75	US: 240

Industries represented:

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

Acknowledgments

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

Global contributors

Alex Geschonneck
Partner, EMA Forensic Leader
KPMG in Germany

Annabel Reoch
Global Head of Ethics and Compliance and Partner
KPMG in the UK

Lem Chin Kok
Partner, Asia-Pacific Forensic Leader
KPMG in Singapore

Benjamin Cowley
Manager, Forensic
KPMG in the UK

Amy Matsuo
Principal and Compliance Transformation and Regulatory Insights Leader
KPMG in the US

Becky Seidler
Partner, Forensic and Dispute Advisory Services
KPMG in Canada

Eliza Morris
Senior Manager, Forensic
KPMG in the UK

Tom Barrett
Senior Manager, Forensic
KPMG in the UK

Contacts

Mark Miller
Global Forensic Leader
KPMG International and Partner
KPMG in the US
marcmiller@kpmg.com

Annabel Reoch
Global Head of Ethics and Compliance
and Partner
KPMG in the UK
annabel.reoch@kpmg.co.uk

Alex Geschonneck
Partner, EMA Forensic Leader
KPMG in Germany
ageschonneck@kpmg.com

Enzo Carlucci
Partner, Americas Forensic Leader
KPMG in Canada
ecarlucci@kpmg.ca

Lem Chin Kok
Partner, Asia-Pacific Forensic Leader
KPMG in Singapore
clem@kpmg.com.sg

kpmg.com

Designed by Evalueserve.

Publication name: Stepping up to a new level of compliance | Publication number: 139109-G | Publication date:January 2024

Document Classification: KPMG Public