KPMG

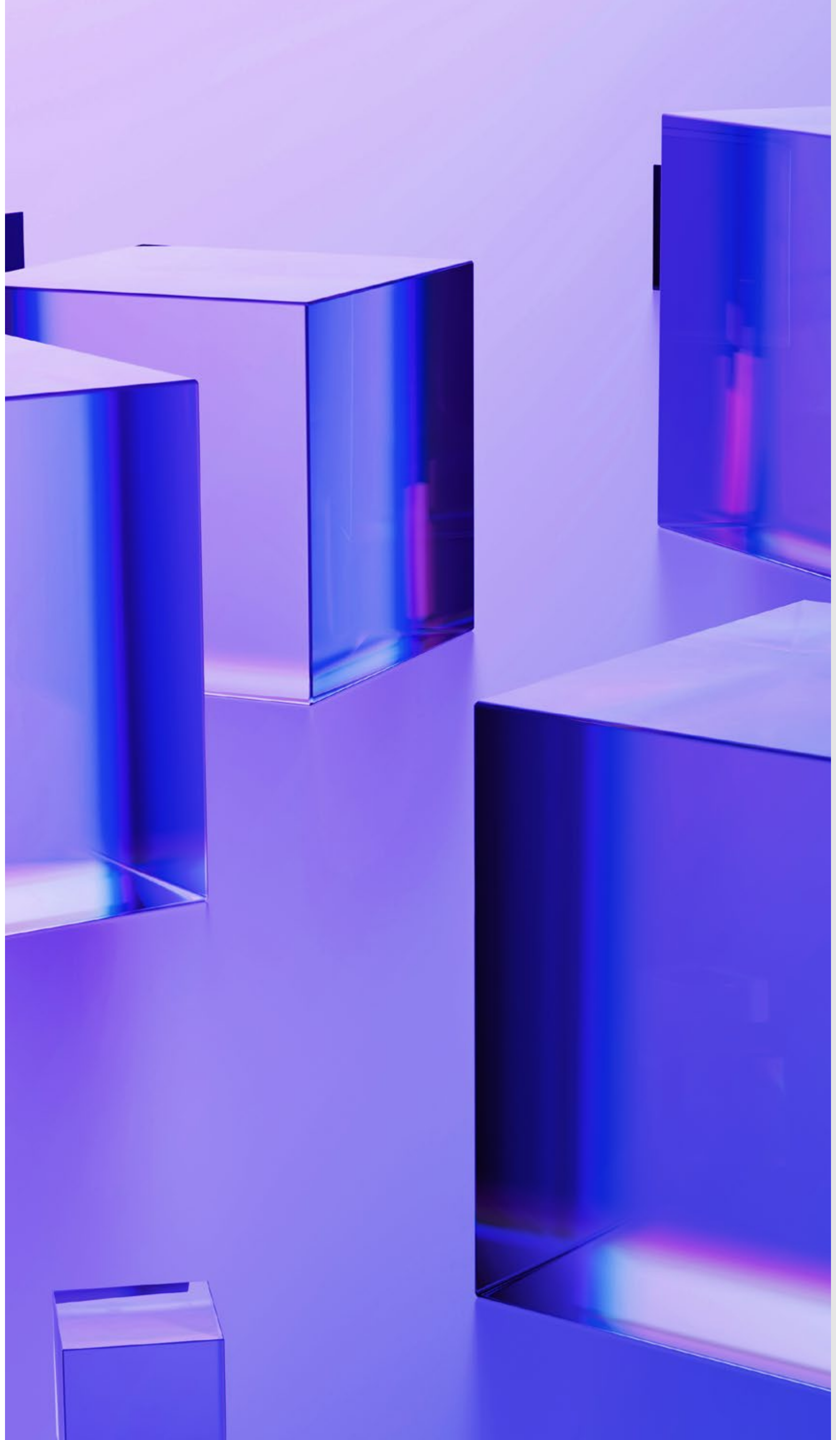
Anticipating more scrutiny

Forward focus for Ethics & Compliance

2023 KPMG Chief Ethics
& Compliance Officer Survey

kpmg.com

Contents



Introduction

The KPMG 2023 Chief Ethics & Compliance Officer Survey draws on the perspectives of 240 CCOs representative of the largest companies operating in six industry sectors to 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 firm culture, sustainability/ESG, and evolving technology.

> We are in a period of discordant and highly sensitized public policy—as well as intense regulatory activity—affecting all industries. Compliance feels acute pressure to enhance—not only to be more effective and efficient—but in order to meet increasing board and regulator expectations. Technology and data analytic investment to the Ethics & 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
& Regulatory Insights

Key findings from this year's CCO Survey include:

Pressures on compliance

73%

expect the **level of focus on compliance to increase** based on regulatory expectations and scrutiny.

Top compliance challenge

43%

of the responses indicate **new regulatory requirements as the top compliance challenge** their organization is facing.

Top compliance focus

45%

are targeting compliance around **industry-specific regulations as the most critical area to improve.**

Sustainability/ESG compliance

48%

have **not yet started implementing Sustainability/ ESG** in their compliance program.

Top compliance area to enhance

63%

expect an **increased technology budget.**

Compliance workforce

56%

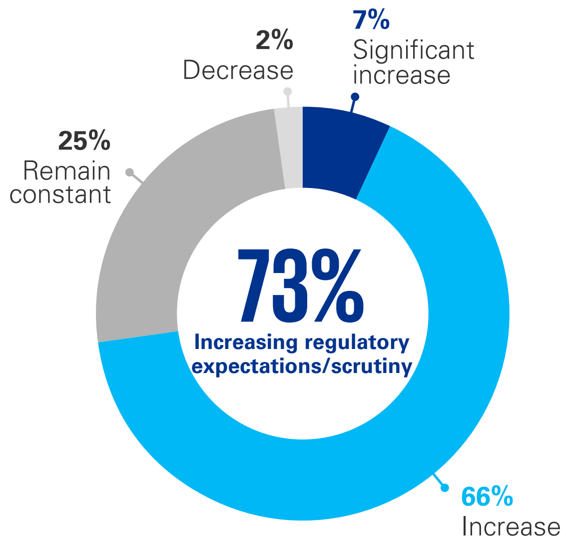
expect an **increase in the number of FTEs** in the next year.

Pressures on Compliance from boards and regulators

Key Findings: Most CCOs expect the focus on Compliance to increase based on increasing regulatory expectations and scrutiny, with the greatest pressure to enhance coming from their boards and regulators.

Level of compliance focus: Nearly three-fourths of CCOs (73%) note increasing regulatory expectations and scrutiny. (Figure 1)

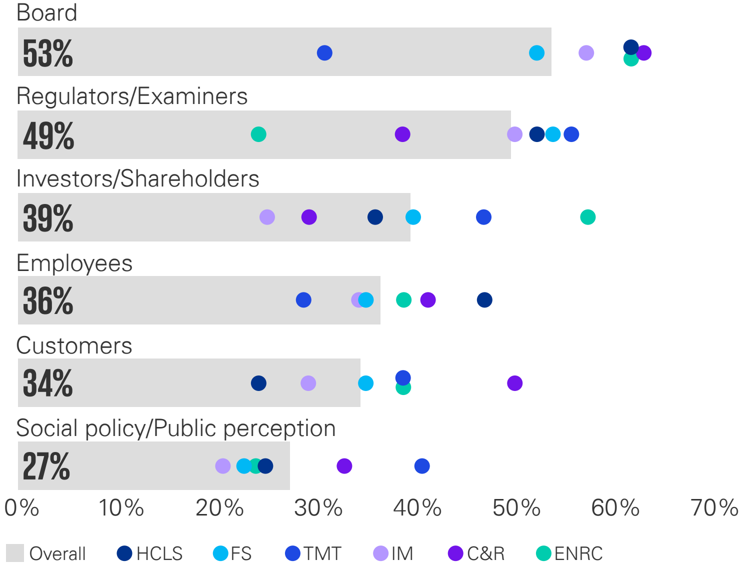
Figure 1



Pressure to Enhance Compliance: While overall CCOs say they feel the most pressure to enhance Compliance from their boards (53%) and regulators/examiners (49%) (Figure 2), there are clear industry stakeholder differences. (Figure 3)

- Board: #1 for HCLS, IM, C&R, and ENRC.
- Regulators/Examiners: #1 for FS and TMT.

Figure 2



(Respondents could choose one or more. Industry acronyms defined on page 20.)

Figure 3

Industry	Board	Regulator/ Examiner	Investor/ Shareholder	Customer	Employee	Social policy
HCLS	1	2	4	6	3	5
FS	2	1	3	4	5	6
TMT	5	1	2	4	6	3
IM	1	2	5	4	3	6
C&R	1	4	6	2	3	5
ENRC	1	5 (tie)	2	3 (tie)	3 (tie)	5 (tie)

(Ranked highest to lowest.)

What are some of the key drivers behind these findings?

- The pace and scale of regulatory activity (e.g., SEC, large global regulations) increase compliance risks and are in addition to business as usual ("BAU") compliance operations.
- The expanding "regulatory perimeter" increases the breadth of examinations and investigations, using existing regulations and jurisdictional authority.
- Regulators look for demonstrable evidence of Compliance critical challenge, domain skills, and dynamic risk assessment, as well as proper resourcing and investment.
- Rulemakings and enforcement actions consider robustness of risk frameworks across Risk and Compliance with a heightened focus on corporate and individual accountability.
- In addition to board and regulator/examiner pressures, investors/shareholders, customers, employees, and the general public (e.g., through social media) may exert pressures on companies (and hold them accountable) for their strategies, operations, and compliance activities.

What should companies actively focus on?

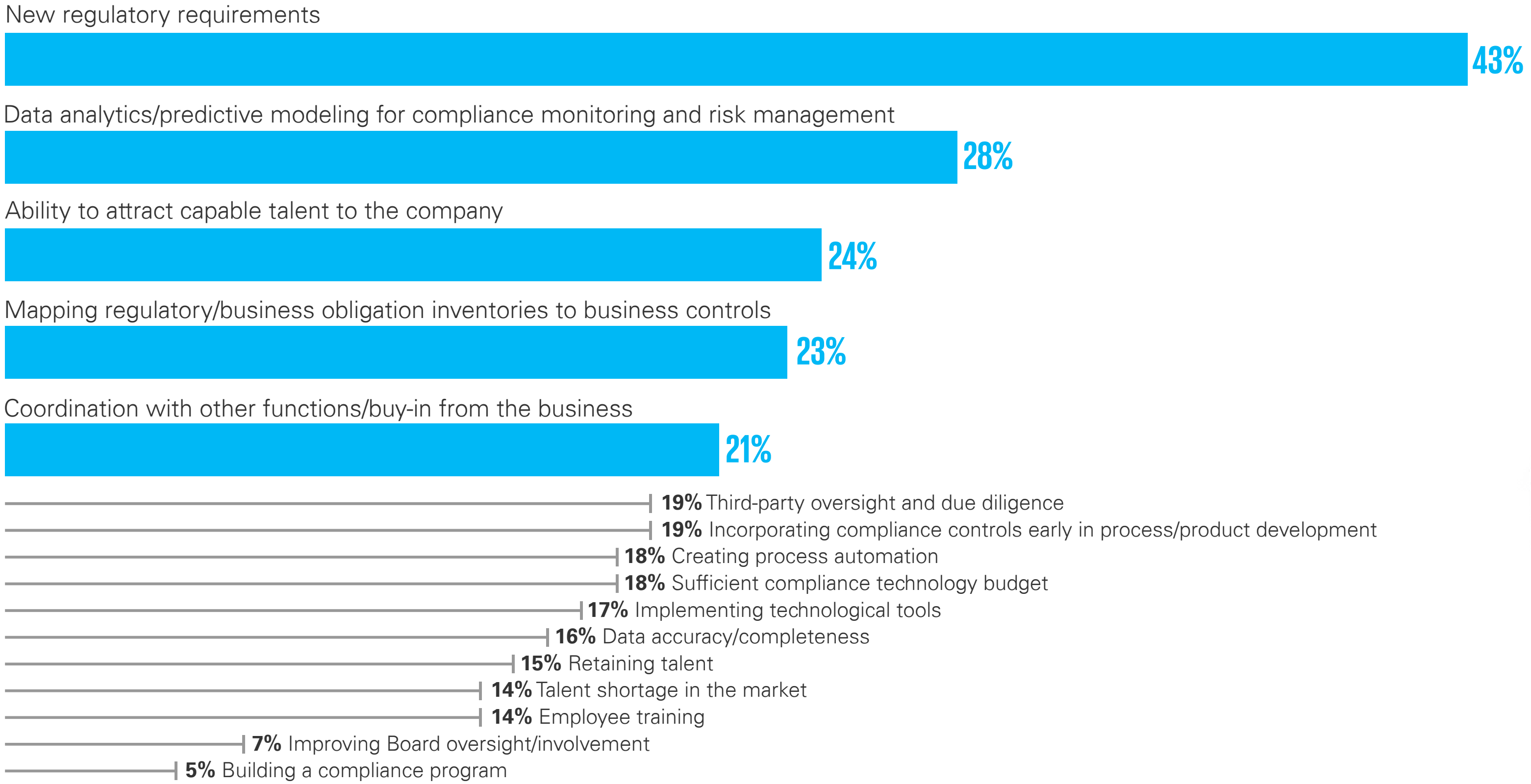
- Strengthen the role of Board and senior management:
  - Demonstrate acumen and governance domain skills.
  - Integrate critical challenge into risk and governance frameworks.
  - Enhance policies and procedures to require more, and more formalized, documentation, mapping, ownership, and controls monitoring and testing.
  - Stature Compliance comparable to other strategic functions and with comparable resourcing (investment, funding, staffing, technology).
  - Regularly review and consider CCO and management reports on compliance risks (including reputation risk, emerging risks, etc.) and potential impacts to business strategy/decisioning, risk management, the overall Compliance function, and governance and oversight.
  - Consider both current/past violations/trends and emerging risk mitigation.
  - Ensure reporting, disclosures, public statements, and marketing are consistent and align with the company's strategies and activities.
- Monitor stakeholder activity, including shareholder proposals, investor expectations, social media posts (public and employee), consumer complaints, and whistleblower activity. As appropriate:
  - Ensure timely and complete responses.
  - Document tracking, intake/resolution, reporting, audits.

New regulatory requirements top list of looming challenges

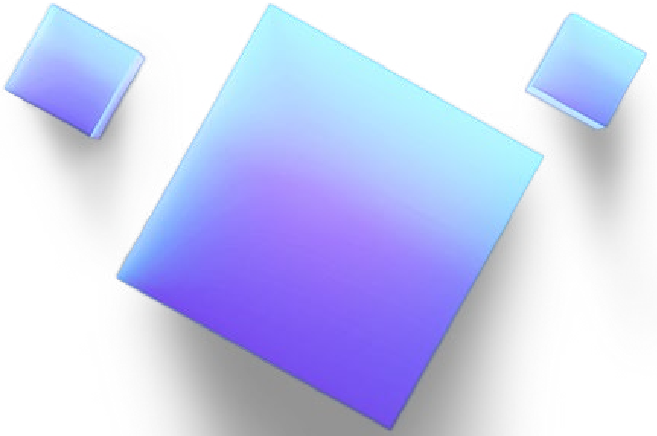
Key Findings: CCOs say that new regulatory requirements pose the greatest challenge to their compliance efforts over the next two years followed by data analytics/predictive modeling and attracting capable talent.

Top Compliance Challenges: CCOs note significant compliance challenges in a variety of areas. (Figure 4)

Figure 4



(Respondents could choose one or more.)



KPMG Insights

What are some of the key drivers behind these findings?

- Intense level of rulemaking/guidance and enforcement activity, including:
  - SEC disclosure proposals (e.g., cyber, climate), insider trading, and clawback policies.
  - FTC guidelines on mergers, fair competition, and data use/privacy.
  - DOJ "Monaco Memo" revising its Corporate Criminal Enforcement Policy to enhance corporate ethics and compliance, including matters of individual accountability, voluntary self-disclosure, and compliance culture.
- The Administration is issuing "whole-of-government"/multi-agency directives on regulatory policy matters (e.g., cybersecurity, data governance, fairness, sustainability/ESG), yet there are regulatory disparities across U.S./global and federal/state issuances.
- New developments, applications, and evolving technologies open up discussion for regulatory scrutiny and new regulation.
- Compliance priorities, including implementing a data-driven compliance program; embedding controls upfront and throughout process lifecycles; increasing awareness of Compliance tools and technology; and maintaining the needed numbers of skilled resources.

What should companies actively focus on?

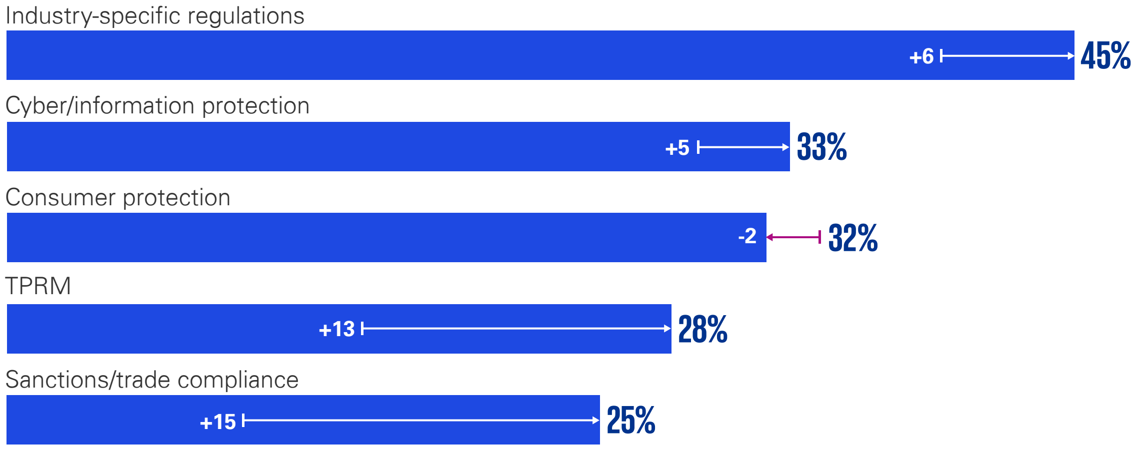
- **Regulatory:** Address the complexity of increasing numbers of new regulations and potentially divergent requirements by:
  - Enhancing coordination between areas (Compliance, Government Affairs, Legal, Public Relations) to assess strategic, operational, and reputation risks from evolving rules.
  - Establishing a robust process to identify, track, and integrate new laws and regulations into a centralized repository.
  - Initiating/maintaining dialogues with existing and new regulators.
  - Understanding the coordination of activities between regulators and any alignment/divergence in their enforcement priorities.
- **Talent:** Stature Compliance comparably with other strategic functions within the organization, including the quality of autonomy, empowerment, visibility, and investment, including sufficient and skilled staffing, training and development, and the adoption of current/emerging technologies. (See Workforce section)
- **Data Analytics & Modeling:** Prioritize investment in, and transformation of, the compliance program; monitor emerging technologies and tools and update programs/systems, as appropriate; phase-in new technologies/processes by starting with "pilots" to demonstrate business value, operational improvements, and build larger business case. (See Technology section.)

Industry regulations top list of key areas for compliance focus

Key Findings: Consistent with the challenges to meet increased regulatory scrutiny and expectations, most CCOs say they are targeting improvement in processes related to industry-specific regulations.

Top areas to improve: CCOs target processes in these areas as the top areas to improve Compliance. (Figure 5)

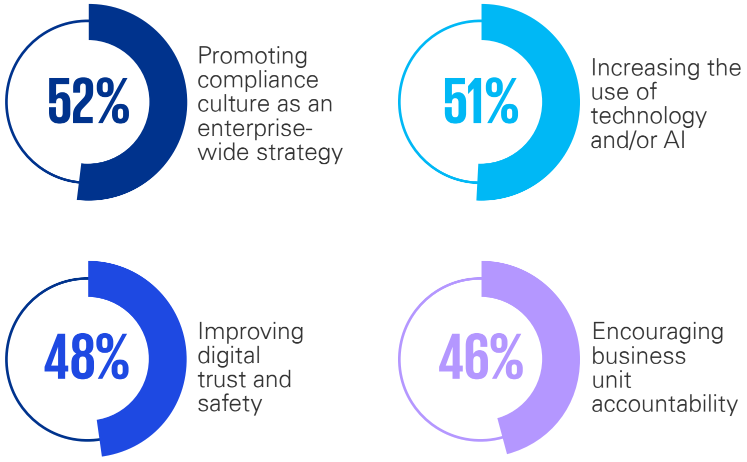
Figure 5 (+/– percentage point change from 2021)



(Respondents could choose one or more.)

Demonstrating "Business Value": CCOs cite plans to demonstrate the "business value" of Compliance in the next two years via the following methods. (Figure 6)

Figure 6



(Respondents could choose one or more.)

What are some of the key drivers behind these findings?

- New regulations, continued regulatory discord, and heightened regulatory/stakeholder scrutiny, while needing to drive "business value," culture, technology/AI, digital trust and safety and business unit accountability.
- Administration directives for increasing regulatory cross-agency focus (e.g., SEC cyber risk management proposals, FTC data safeguards rule, CISA incident reporting).
- Continuing attention and broad application to consumer protections, including fairness, data privacy and use, and fraud/scams.
- Third-party risk management challenges (e.g., cybersecurity, operational resiliency, data use and privacy, ethical supply chain).
- Expanded use of sanctions and trade restrictions, coupled with complexities in areas such as beneficial ownership.

What should companies actively focus on?

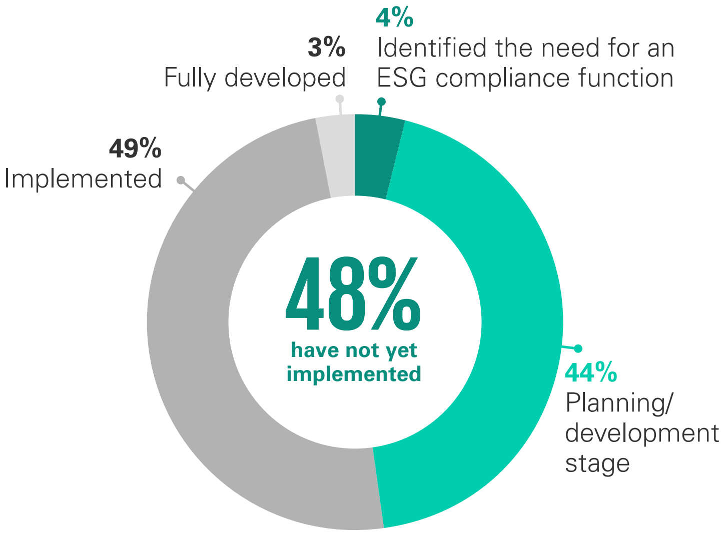
- Companies should look to optimize their compliance programs by:
  - Positioning compliance as a coordinator/collaborator with senior leadership and the board.
  - Assessing current regulatory change management processes and ensuring they fully capture applicable global, federal, and state regulations and relevant divergences.
  - Working with internal stakeholders to determine if new controls need to be designed and integrated into existing frameworks or if new or separate compliance policies are appropriate in emerging/developing regulatory areas (e.g., sustainability/ESG, AI).
- Evolve identity and access management programs (customer, vendor, enterprise) to ensure appropriate preventions against cyber and data privacy threats.
- Prioritize and embed fairness across all customer impact points from product/service design, marketing/advertising, disclosures, servicing, customer interactions (including complaints management) as well as mergers and acquisitions activities.
- Execute dynamic third-party risk assessments and assess whether third-party risk management meets or exceeds global and jurisdictional regulatory expectations (e.g., data privacy, anti-money laundering, sanctions).
- Monitor developments related to geopolitical events; sanctions activity; and regulatory requirements in areas related to cybersecurity, data privacy, beneficial ownership, and trade finance.

Sustainability/ESG compliance in development

Key Findings: About half of CCOs say they are in the process of implementing Sustainability/ESG compliance programs, though nearly as many say they are still in the planning and development stages. Key areas of focus include monitoring and testing, regulatory scanning, and policy management.

Maturation: About half of the CCOs (48%) have either identified the need for but have not yet begun planning for an ESG compliance program or are in the planning and development stage of building it out. Another 52% are implementing an ESG compliance program. (Figure 7)

Figure 7



Areas to Enhance: Many CCOs are looking to enhance sustainability and ESG compliance programs over the next two years. Areas prioritized for enhancement include: (Figure 8)

Figure 8

(Respondents could choose one or more.)

What are some of the key drivers behind these findings?

- Divergence and continually evolving expectations/ requirements across federal, state, and international regulations.
- Public policy sensitivities around sustainability/ESG, causing operational challenges and reputational risk.
- Defining the role of compliance with sustainability/ ESG (inclusive of regulation tracking, compliance risk assessment, etc.) can create both design and implementation challenges in building out an ESG compliance program.
- Progress of the business line in implementing the company's sustainability/ESG strategies and policies as well as data input challenges associated with E, S, and G metrics.

What should companies actively focus on?

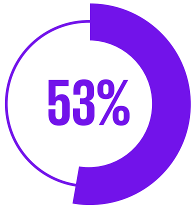
- In response to the divergence and continuous evolution of federal, state, and international ESG regulations, companies should consider:
  - Enhancing coordination between areas such as Government Affairs, Legal, Compliance, Public Relations, and business units to assess strategic, operational, and reputational impacts of emerging risks and evolving laws and regulations.
  - Driving awareness across the organization of current/evolving regulatory risk applicability, the current state of preparedness/risk assessment, and the strengthening of risk mitigation controls.
  - Building teams focused on jurisdiction-specific reporting requirements.
  - Aligning voluntary and required reporting and disclosures and identifying any contradictions between reporting jurisdictions.
- To avoid design and implementation challenges in building out an ESG compliance program, companies should consider:
  - Establishing areas of business, including compliance, that take explicit accountability of the E, S, and G.
  - Working with internal stakeholders to determine if new sustainability/ESG controls need to be designed and integrated into an existing framework.
  - Positioning compliance as a coordinator/collaborator with senior leadership and the board, as well as ensuring appropriate investment in the ESG compliance function (people, processes, and technology).
  - Ensuring the company can navigate federal/state/global requirements aligned to its ESG commitments.
  - Ensuring that the company's Supplier Code of Conduct set expectations for suppliers and their staff that are consistent with the company's sustainability/ESG strategies, policies, commitments, and periodically review suppliers' compliance with their agreements (e.g., products, facilities, business practices, supply chain) as well as applicable laws and regulations, validating content messaging, reporting elements, and stakeholder responses prior to issuance.
  - Using Sustainability/ESG as a value driver for ethical business practices and "good corporate citizenship."

Compliance technology & data analytics top areas to enhance

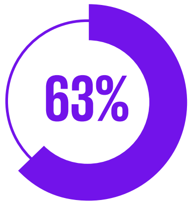
Key Findings: The majority of CCOs name technology and data analytics as the top area to enhance in the next two years. Related budget increases will focus on cybersecurity/data privacy, data analytics, process automation, and AI.

Budgetary Increases: More than half of CCOs (63%) are looking to increase their technology budgets for the ethics and compliance function, while the majority (53%) plan to enhance technology and data analytics. (Figure 9)

Figure 9

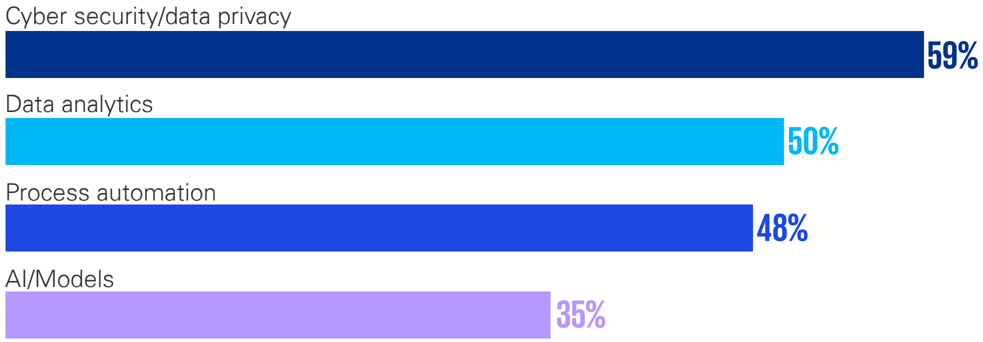


Look to enhance technology and data analytics



Expect increase in technology budget

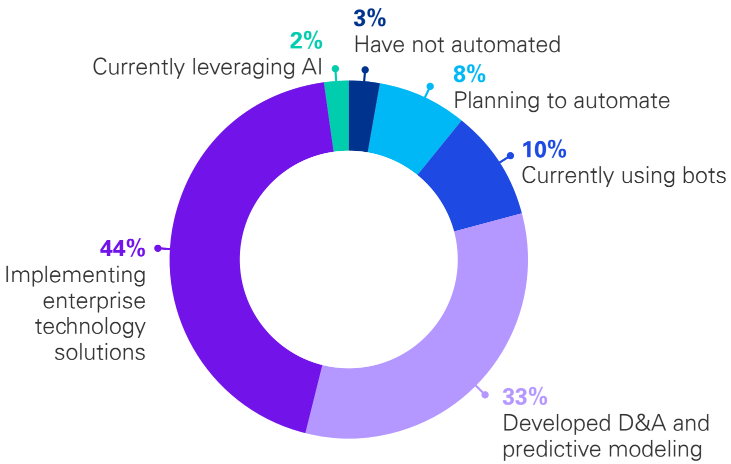
Drivers of budget spend:



(Respondents could choose one or more.)

Current Maturation: Very few CCOs (2%) are currently leveraging AI though many (44%) are implementing enterprise technology solutions or have developed data analytics and predictive modeling (33%). Still fewer (10%) are currently using automated bots or are in the planning/development stage (8%). (Figure 10)

Figure 10



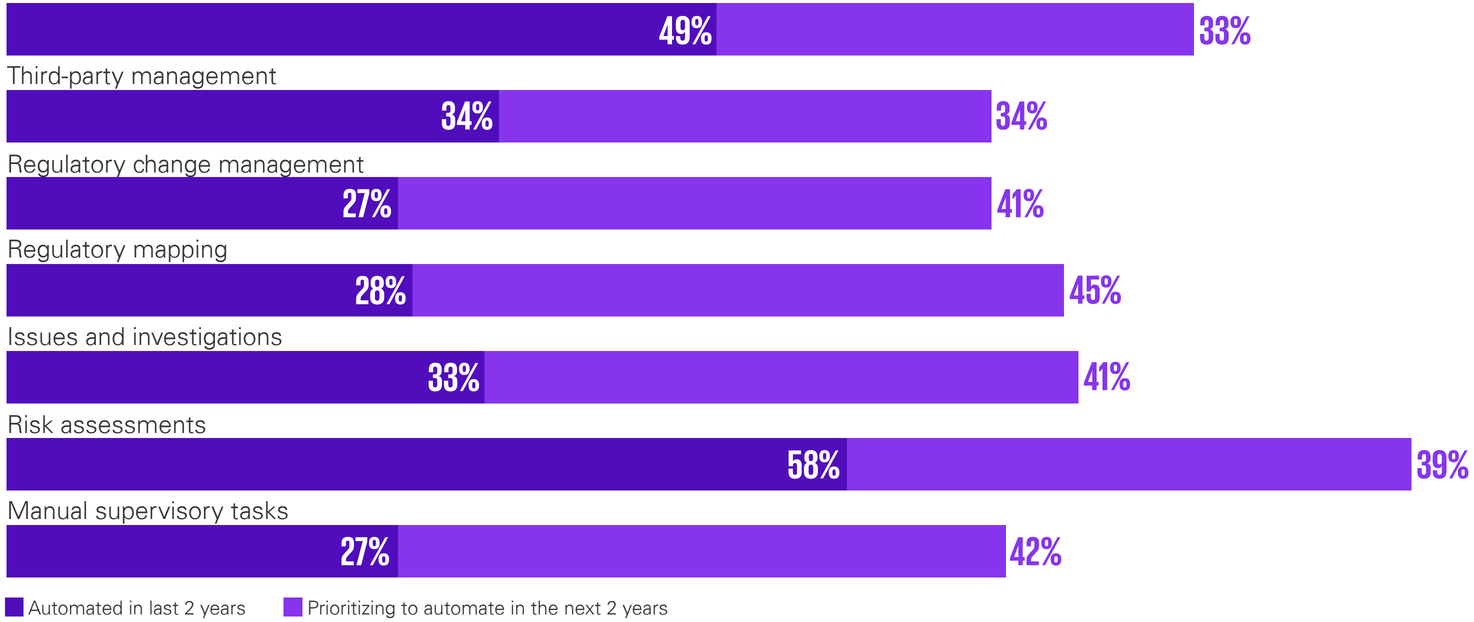
Key Findings continued:

Future Tech Focus/Maturation: Over the past two years, many companies have begun automating processes. Building on this effort, CCOs say they have prioritized automating the following areas over the next two years. (Figure 11)

Drivers:

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

Figure 11



(Respondents could choose one or more.)

KPMG Insights

What are some of the key drivers behind these findings?

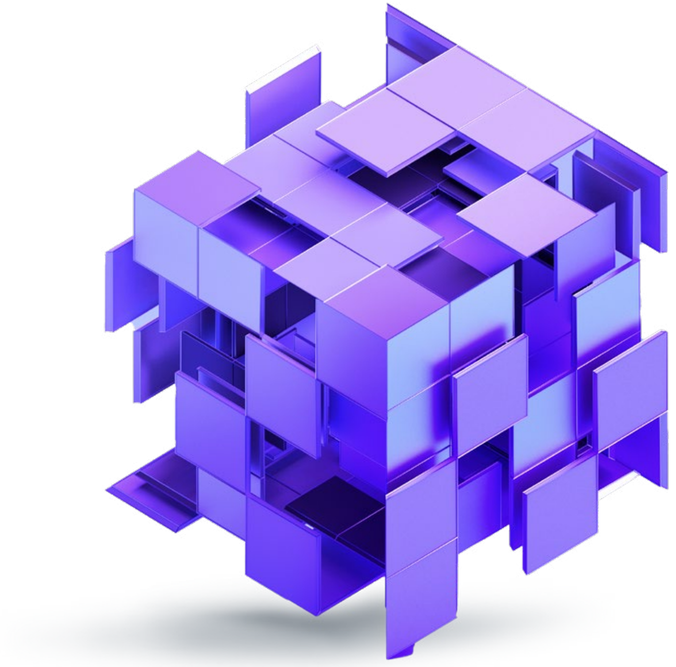
- Heightened regulatory scrutiny of new technology uses internally and externally (e.g., digital devices, AI, machine learning, automation, advertising, and model bias).
- Heightened regulatory expectations for technology resiliency, including legacy and newer systems, threat/vulnerability detection, mitigation, and remediation and continuity planning; technology risk management, including risk assessments, monitoring, and controls; and operational resiliency, including governance practices to maintain critical operations and cyber and third-party risk management.
- Heightened regulatory focus (including governance and controls) on consumer data privacy, collection, use, retention, and disposal (e.g., FTC ANPR on commercial surveillance and data security, and information orders to social media and video streaming companies; CFPB information orders to Big Tech and BNPL lenders and NPR on Section 1033).
- Focus on cloud adoption (e.g., Treasury report on key challenges, FTC RFI on cloud service providers).
- The Administration's "Blueprint for an AI Bill of Rights", outlining principles for the design, use, and deployment of automated systems, including safe and effective systems; algorithmic discrimination protections; data privacy; consumer notice and explanation; and human alternatives, considerations, and fallbacks.
- Need for tech- and data-driven skill sets to implement compliance program and related tools.

What should companies actively focus on?

- As companies invest in technology, data analytics, and automation, they should consider "privacy-by-design" principles—embedding consumer privacy into the design, operation, and management of new technologies with the goal of preventing privacy vulnerabilities (e.g., malware, fraud, identity theft, insider risk, reputation risk).
- To avoid design and implementation challenges in building out an ESG compliance program, companies should consider:
  - Establishing areas of business, including compliance, that take explicit accountability of the E, S, and G.
  - Working with internal stakeholders to determine if new sustainability/ESG controls need to be designed and integrated into an existing framework.
  - Positioning compliance as a coordinator/collaborator with senior leadership and the board, as well as ensuring appropriate investment in the ESG compliance function (people, processes, and technology).
  - Ensuring the company can navigate federal/state/global requirements aligned to its ESG commitments.
  - Ensuring that the company's Supplier Code of Conduct set expectations for suppliers and their staff that are consistent with the company's sustainability/ESG strategies, policies, and commitments, and periodically review suppliers' compliance with their agreements (e.g., products, facilities, business practices, supply chain) as well as applicable laws and regulations, Validating content messaging, reporting elements, stakeholder responses prior to issuance.
  - Using sustainability/ESG as a value driver for ethical business practices and "good corporate citizenship."

What should companies actively focus on? *(continued)*

- Companies should prioritize investment in, and transformation of, their compliance programs, and view it as value-generating. Senior leadership should consider:
  - Encouraging a data-driven culture across the company.
  - Phasing-in new technologies/processes by starting with "pilots" to demonstrate business value, operational improvements, and build larger business case.
  - Evaluating, integrating, and automating metrics to identify and highlight key insights into compliance efforts.
  - Implementing a data-driven approach to compliance, including strong data governance, resourcing, effective controls, and automation, to create a dynamic and continuously improving compliance program.
  - Periodically assessing the effectiveness and efficiencies generated by the new technologies/processes and revising as needed.
  - Monitoring emerging technologies and tools and updating programs/systems as appropriate.
- Companies should be able to demonstrate to regulators effective board reporting and oversight of technology and associated risks, including:
  - The quality and timeliness of operational and risk metrics.
  - The depth of insight/transparency provided by senior management and risk metrics.
  - Meaningful challenge and corrective action tracking.
  - Periodic review of the risk appetite and tolerances.



Accountability and talent shortages top workforce worries

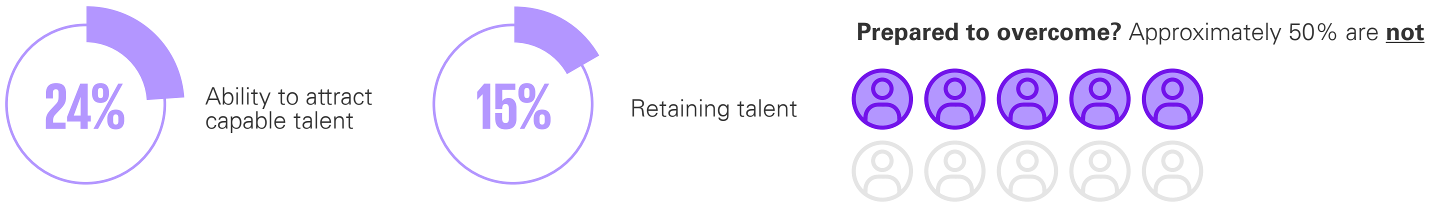
Key Findings: Despite economic uncertainties, the majority of CCOs anticipate increasing the number of full-time employees in the next year—even though attracting and retaining talent are key workforce challenges within this area.

Accountability: CCOs identify the top areas of focus for promoting compliance behavior/culture and driving accountability.

Figure 12

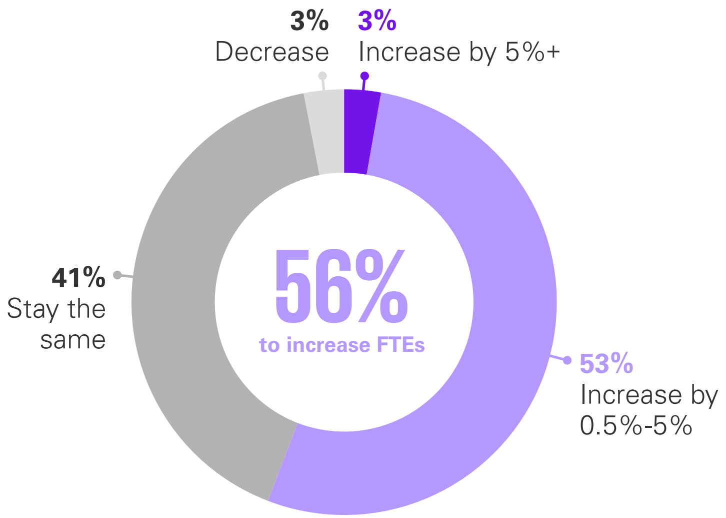
Talent Shortages/Retention: CCOs note both the ability to attract capable talent (24%) and retaining talent (15%) as key compliance workforce challenges. Furthermore, approximately half of the respondents say they are not prepared to overcome these talent-related challenges. (Figure 13)

Figure 13



Compliance FTEs: The majority of CCOs (56%) note an increase to compliance FTEs in the next year, with most (53%) reporting an increase of 0.5%-5%. (Figure 14)

Figure 14



KPMG Insights

What are some of the key drivers behind these findings?

- Regulatory and supervisory scrutiny as well as new regulatory expectations/requirements are top risks.
- Board and regulatory critical challenge pressures on the effectiveness of Compliance.
- Despite economic uncertainty, commitment to retain and/or expand Compliance FTEs demonstrates the importance of, and commitment to, Ethics & Compliance.
- Regulatory and enforcement accountability actions, including:
  - DOJ revisions to Criminal Division policies (as outlined in the "Monaco Memo") to provide incentives to promote and support a culture of compliance, including "cooperation credit" related to voluntary self-disclosure and compensation structures.
  - DOJ statements that its top priority in corporate ethics and compliance matters is to hold accountable individuals who commit and profit from misconduct.
  - Enforcement actions against executives (e.g., sales practices misconduct; misleading disclosures).
  - SEC final rule on clawback policies.

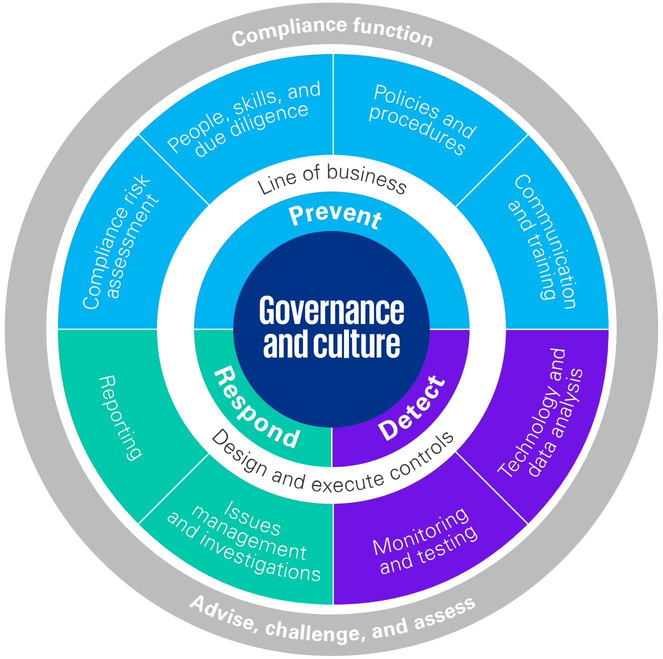
What should companies actively focus on?

- Stature Compliance comparably with other strategic functions within the organization, including the quality of autonomy, empowerment, and visibility.
- Assess employee value proposition in order to attract and retain necessary compliance talent.
- Ensure appropriate investment in the Compliance function, including sufficient and skilled staffing, training and development, and the adoption of current/emerging technologies.
- Conduct skills assessments and time measurement analyses to examine needed skills and possible gaps, as well as where Compliance FTEs may be repurposed for higher value.
- Enhance the compliance program to include both incentives and deterrents related to individual accountability, compliance metrics/measurements, and corporate culture.
- Ensure the demonstrable reporting of timely issues identification, notification, escalation, and resolution/remediation, including measures to hold responsible individuals accountable.

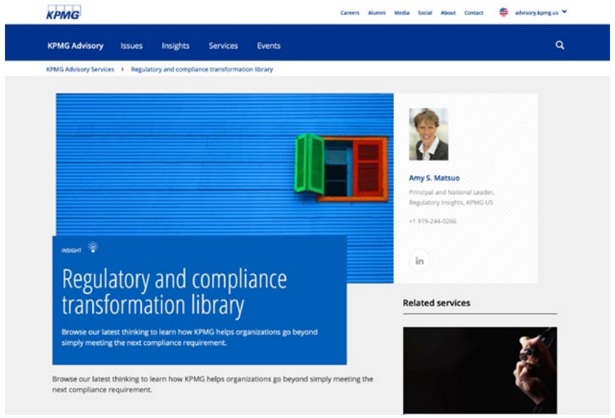
KPMG Insights: The future of compliance

Compliance must 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:

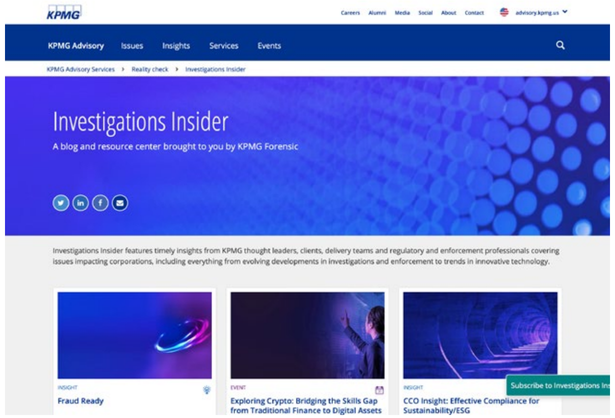
Governance and culture	• Are the board and committee(s) regularly updated on regulatory and compliance changes including regulatory examination and enforcement expectations?
Compliance risk assessment	• Does the risk assessment incorporate both qualitative and quantitative data/inputs? • Based on the assessment, are sufficient economic, technological, and human resources allocated to compliance?
People, skills, and due diligence accountability	• Are roles and responsibilities clearly articulated and does the company demonstrably show that compliance responsibilities matter (e.g., performance reviews, compensation impacts)? • Are disincentives built into the incentive plans to discourage misconduct?
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 and models/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 (e.g., considerations around AI security, ethics and governance, etc.)?
Monitoring and testing	• Is risk-based assessment and testing of third-party relationships for compliance with regulatory requirements and organizational policies adequately assessed in due diligence and conducted via ongoing monitoring/testing?
Issues mgmt. and investigations	• Are protocols established for handling data and evidence (documentary 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/tolerance levels?



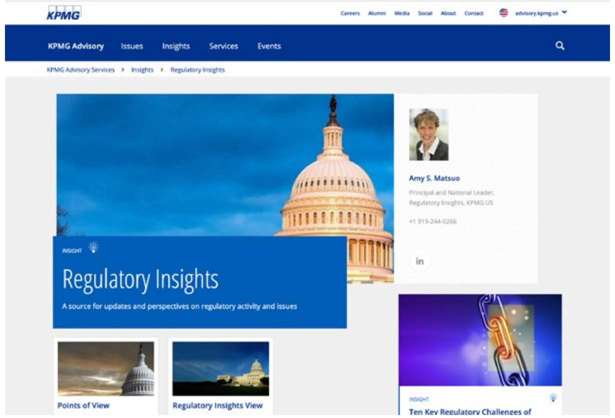
KPMG Insights: Relevant resources



Compliance Transformation Library



Investigations Insider



Regulatory Insights

Research methodology

KPMG surveyed 240 Chief Ethics and Compliance Officers (CCOs) representative of Fortune 500 companies across the following industries:

- 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)

For more information, contact us:

Amy Matsuo
Principal and National Leader
Compliance Transformation (CT)
& Regulatory Insights
amatsuo@kpmg.com

Dan Click
Consumer Markets and
Industrial Manufacturing CT Lead
dclick@kpmg.com

Travis Canova
Energy CT Lead
lcanova@kpmg.com

John Kemler
Technology, Media, and
Telecommunications CT Lead
jkemler@kpmg.com

Mike Lamberth
Insurance CT Lead
mlamberth@kpmg.com

Brent McDaniel
Consumer and Retail CT Lead
bmcdaniel@kpmg.com

Anthony Monaco
Government CT Lead
amonaco@kpmg.com

Jaime Pego
Healthcare CT Lead
jpego@kpmg.com

Jennifer Shimek
Healthcare & Life Sciences CT Lead
jshimek@kpmg.com

Todd Semanco
Financial Services CT Lead
tsemanco@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia