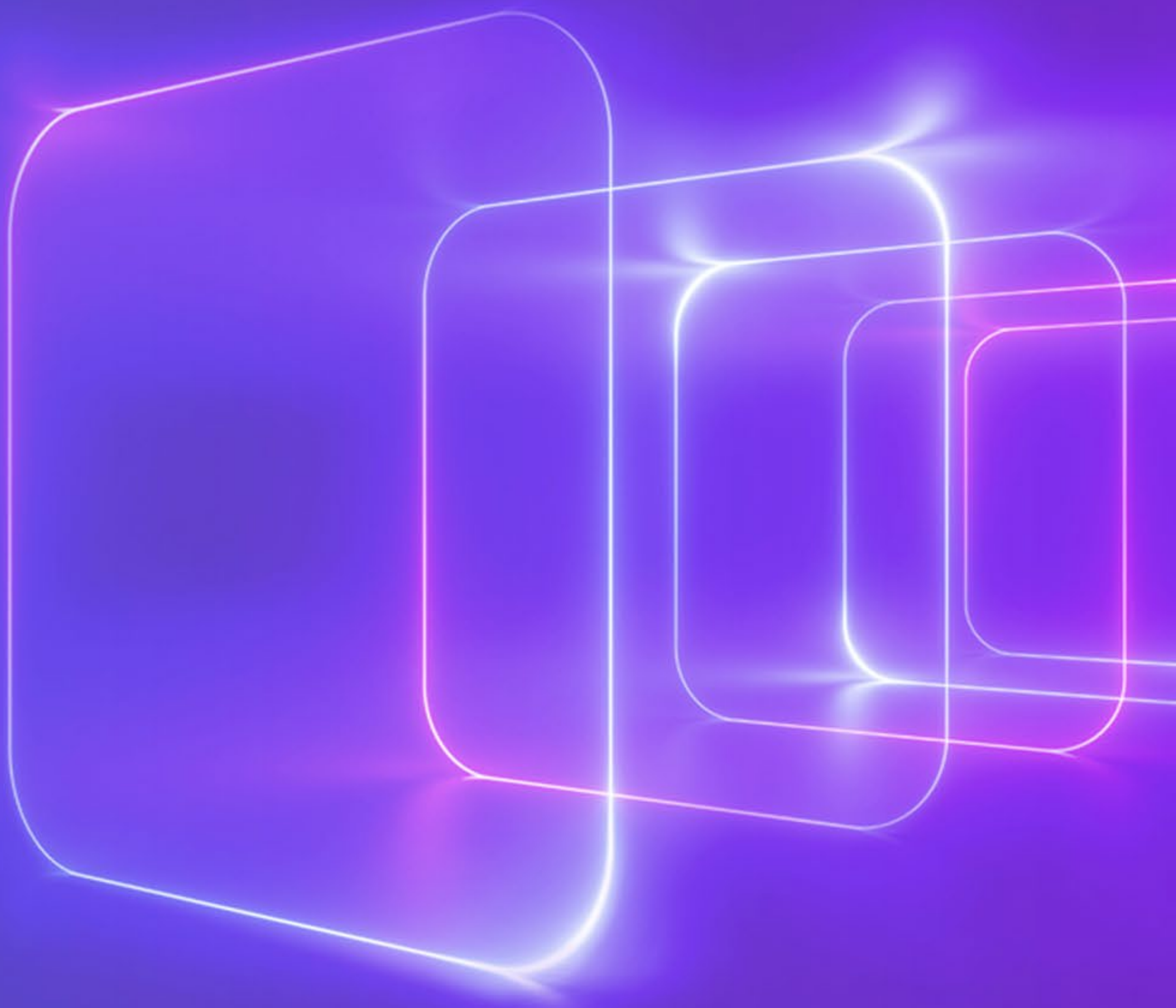
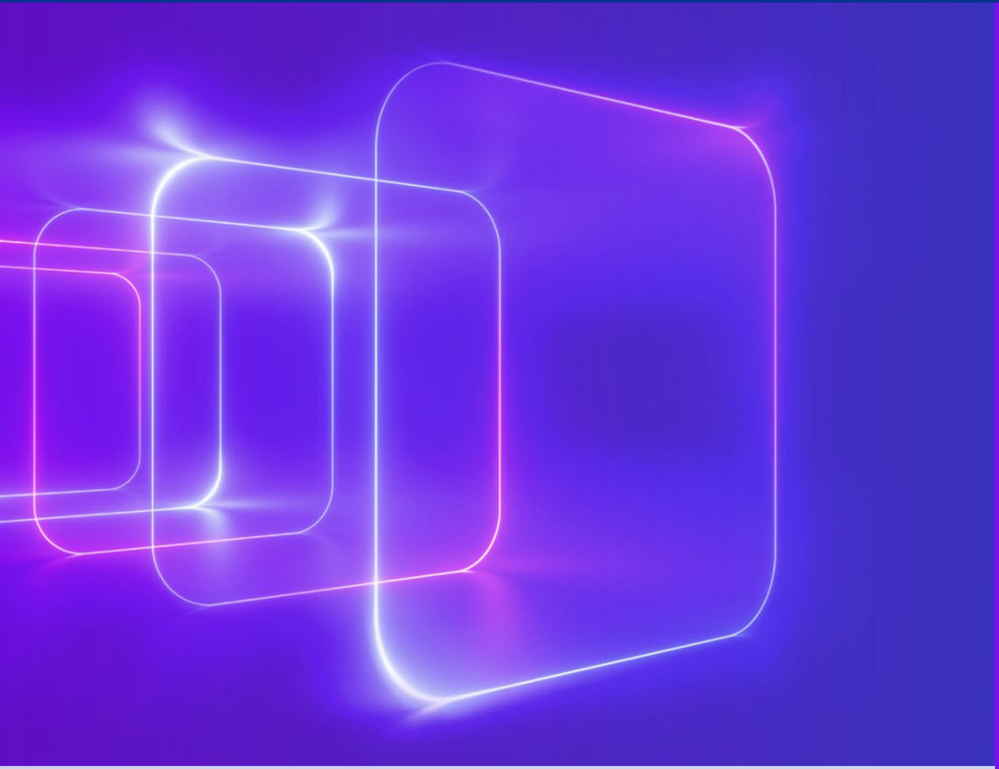
KPMG

Implementing tech and data-driven compliance

Forward focus for ethics and compliance





How KPMG Can Help

Compliance Transformation Services

GRC Technology Services

Introduction

With rapidly evolving technology innovation and the adoption of digital capabilities such as Generative AI increasing across organizations, Compliance plays a critical role—to proactively anticipate and mitigate the new and emerging risks associated with this ongoing tech innovation, including in areas such as deceptive marketing, model bias, civil rights, and digital devices. At the same time, accelerating and implementing technology and data-driven processes within the Compliance function is no longer "nice to have" but rather a crucial capability to proactively and effectively position Compliance to meet the dynamic business needs and regulatory expectations in a continuously increasing technology-driven business environment.

CCOs' focus on technology

Chief ethics and compliance officers (CCOs) expect the focus on Compliance to increase based on rising regulatory expectations and scrutiny.

As a result, companies are focusing on enhancing technology and data analytics in their ethics and compliance in an effort to help create a dynamic and continuously improving Compliance program. In particular, they are implementing data-driven approaches, investing in strong data governance and controls, maintaining resources, establishing effective operational controls, and implementing automation.

Key elements in the implementation of an effective tech and data-driven compliance program entail:

1. Identifying areas of enhancement

Increasing technology budgets to enhance areas such as cybersecurity, process automation, and artificial intelligence (AI)/models.

2. Prioritizing processes for automation

Identifying and prioritizing opportunities for automation in accordance with evolving regulations aimed at mitigating risks associated with advanced technology innovations.

3. Investing for compliance returns

Demonstrating the business value of compliance and securing investment in ethics and compliance programs.

2023 KPMG CCO Survey

53%

look to enhance technology and data analytics

63%

anticipate increasing their technology budget

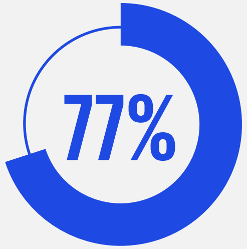
44%

are implementing enterprise technology solutions

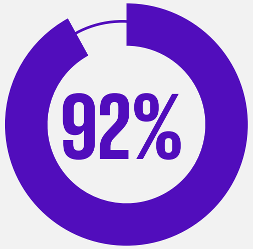
KPMG conducted the 2023 KPMG CCO Survey, Anticipating more scrutiny, in February 2023. The survey captures insights from 240 CCOs representative of the largest companies operating in six industry sectors on key areas of ethics and compliance, including regulatory complexity, operational challenges, ethics and firm culture, sustainability/ ESG, and evolving technology. Unless otherwise noted, the statistics in this report are findings from the 2023 CCO Survey.

2023 KPMG Generative AI Survey

KPMG conducted the **2023 KPMG Generative AI Survey** of 300 global business executives to explore generative AI views and trends.



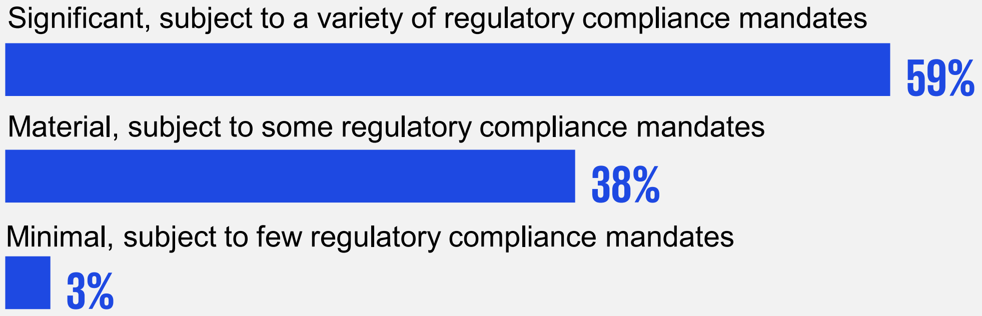
of respondents expect generative AI to have the largest impact on their businesses out of all emerging technologies.



think generative AI implementation introduces moderate to high-risk concerns.

2023 KPMG Cloud Transformation Survey

KPMG conducted the 2023 survey, **Building trust in cloud environments**, in 4th quarter 2022. More than 300 information security, IT, risk and compliance, technology, and internal audit professionals described their companies' regulatory exposure/commitments as:

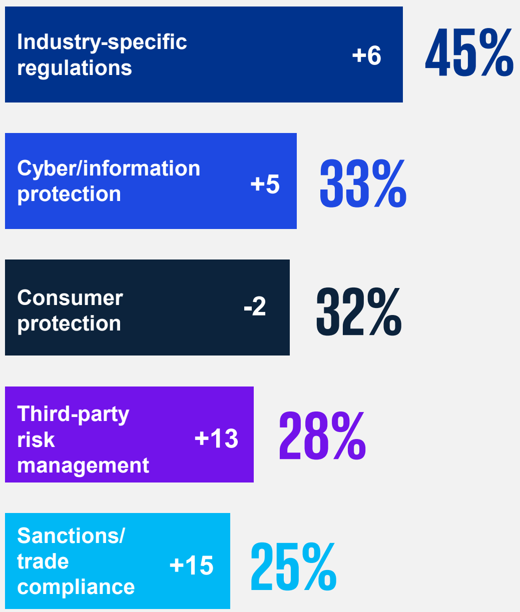


1. Identifying areas of enhancement (1/2)

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

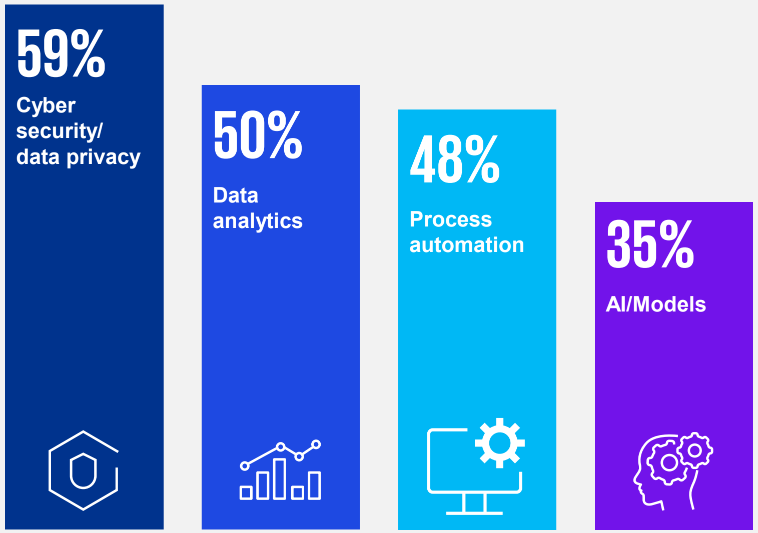
As the adoption of cloud, e-communication technologies and platforms, and digital tools grows along with the increasing use of service providers, regulators warn of potential risks, including information security incidents, cyberattacks, and misuse of consumer data.

CCOs target processes in these areas as the top areas to improve Compliance*
(+/- percentage point change from 2021):



CCOs are looking to increase their technology budgets due to increased focus on cybersecurity/data privacy, data analytics, process automation, and AI.*

Drivers of budget spend



Regulatory drivers compelling companies to expand compliance technological tools and data analytics include:

- 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., Interagency statement on monitoring the development and use of automated systems, SEC cyber risk management proposals, FTC data safeguards rule, CISA incident reporting).
- DOJ’s initiatives related to compensation, voluntary self-disclosure, and personal devices, including the “Monaco Memo” which revises its Corporate Criminal Enforcement Policy to enhance corporate ethics and compliance.
- 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.

** Respondents could choose one or more.*

1. Identifying areas of enhancement (2/2)

Investing in and adopting technological tools requires companies to be diligent in complying with evolving regulations and improving areas such as:

Technology risk management

Regulators are continuing to focus on the robustness of a company's modern technology risk management program. Specifically, heightened attention will be directed to significant operating changes that utilize new technology innovations such as AI/models, cloud, and digitization of risk management processes. Companies utilizing technologies such as AI should consider during the design, use, and deployment of such tools, the safety and effectiveness (e.g., protections against unintended or inappropriate use); protections against, and ongoing testing for, bias; data governance and privacy; transparency (including what and how information is being used and potential impacts to the business/ consumer); and accountability and oversight.

Data integrity and accuracy

This step is foundational. In order to target compliance processes where automation can most easily be incorporated, the underlying data must have integrity and be available and acquirable. Investigating this fully in the initial planning stage may reveal instances where certain data remediation exercises or normalization efforts are needed first, before a process can be automated, and may also redirect initial efforts to automate other Compliance processes or activities. Since many processes are not owned by the Compliance function alone, it is important to collaborate with the process owners and users to better evaluate needed data.

Data analytics

Measure multiple Compliance risk areas in a more dynamic way to look for potential compliance flags that may warrant additional review. As companies utilize technology to enhance their analytics, it allows Compliance to go from sampling reviews to full population reviews, and with newer technology it allows this in areas such as voice analytics (e.g., complaint analysis, potential illegal/illicit activity speech pattern), optical recognition and analysis (e.g., physical security reviews, marketing images to target demographics) and text analytics (e.g., contracts, disclosures, policies).

Attracting and retaining talent

Identify personnel with the appropriate skills, knowledge, and availability to undertake integration of Compliance technology tools and data analytics. Staffing needs are being shaped by the more data-driven Compliance function, which requires attracting data analytics-focused skill sets; allocating limited resources to the growing number of pressing/evolving risks; and incorporating forward-looking, innovative technologies into Compliance tasks to create efficiencies and expand Compliance workforce focus to value-added initiatives.

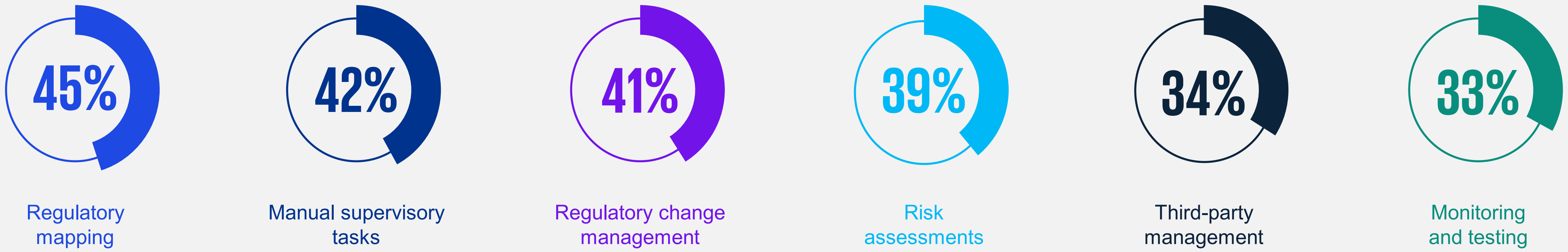
2. Prioritizing processes for automation

When determining which compliance processes to target for automation, organizations often start by inventorying their regulatory and compliance obligations and evaluating which process steps or activities are most labor-intensive and which are repeatable and consistently actioned. Automation today involves more than a large-scale application; it requires an in-depth process of selecting smart use cases and testing them to ascertain optimal value and required uplift.

To integrate automation into compliance and increase organizational awareness of compliance tools and technology, it is important that data analytics and predictive modelling tools are developed for compliance monitoring and risk management.

Although many companies have begun automating processes over the past few years, CCOs are building on this effort and prioritizing automating processes that will enable them to mitigate emerging risks and keep up with changing regulations.

CCOs prioritized these areas for automation over the next two years*



* Respondents could choose one or more.

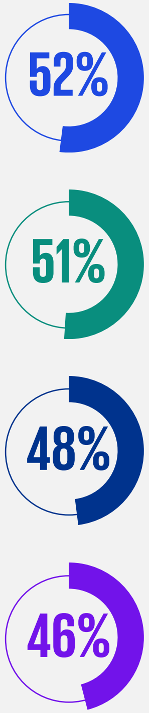
3. Investing for compliance returns

Companies must change their mindset from seeing the “cost of compliance” or “policing for compliance” to seeing the benefits of embedding compliance up front and ongoing; the advantages of early self-identification, mitigation, and remediation of risks; and the value of an investment in ethics and compliance as an investment in the business.

Viewing Compliance as an investment can help measure its return during ongoing compliance improvements while propelling the organization toward greater effectiveness, sustainability, and efficiencies in its compliance efforts. Implementing a data-driven approach, investing in strong data governance and controls, maintaining resources, establishing effective controls, and implementing automation will help to create a dynamic and continuously improving Compliance program.

To the extent possible, having quantitative data to support the overall benefits can help demonstrate the return on investment to stakeholders and leadership.

CCOs cite plans to demonstrate the “business value” of Compliance in the next two years via the following methods: *



52% Promoting compliance culture as an enterprise-wide strategy

51% Increasing the use of technology and/or AI

48% Improving digital trust and safety

46% Encouraging business unit accountability

* Respondents could choose one or more.

Bringing it all together: Opportunities to automate

Regulatory mapping and change management

Automation can accelerate the inventorying of regulations, laws, and obligations from global regulatory sources; provide real-time notification of new rules, proposed rule changes, and guidance; track regulation lifecycles; and enable a quicker impact analysis when such obligations change (through a mapping of the regulations to applicable controls).

Manual supervisory tasks

Automation of repetitive manual supervisory tasks enables CCOs and their teams to continue business-as-usual (BAU) processes and also focus more time on initiatives that require greater attention and subject matter expertise; current workforce challenges of attracting talent and allocating resources to areas of evolving regulatory scrutiny (e.g., sanctions and trade compliance, ESG, cybersecurity, data privacy) add to the impetus to automate these tasks.

Monitoring and testing

Automation can be used to extract textual information from non-machine-readable documents to review transaction activity, analyze source documentation, aggregate test results for a more holistic view of risks, and assist with proactive identification and escalation of compliance failures. Automation can provide greater risk coverage and consistency and help identify more meaningful patterns in transactional data, ultimately providing stakeholders with improved insight into the organization's compliance practices.

Policy management

As policies and procedures have proliferated, it has become increasingly difficult to identify changes and to develop a clear understanding of what policies and procedures are current. Automation can be used to track policies, procedures, communications, and changes to protocols as well as to provide a workflow for approval and certification processes and an audit trail.

Risk assessments

Organizations can use automation to assign ratings to inherent risks or mitigating controls as part of the quantitative analysis process. Automation can also be used to analyze structured and unstructured data contained in documentation and to prepopulate the information into risk assessment templates and for overall document retention. Automation of risk assessments can be quite useful for organizations that are seeking a single view of risks across their enterprise.

Third party management

Automation is driving down the costs of completing due diligence, particularly on third-party vendors, suppliers, contractors, and customers, which often must be updated, or refreshed, on a recurring basis, potentially in real time. For example, automation can slim down due diligence results, limiting duplication of similar records or topical matters and applying a rating of relevancy to the records to enable quicker identification of negative information that is impactful to the organization.

Contact us

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

Lisa Rawls
Principal and
GRC Technology Leader
lisarawls@kpmg.com

Travis Canova
Energy CT
lcanova@kpmg.com

Brent McDaniel
Consumer/Retail CT
bmcdaniel@kpmg.com

Jaime Pego
Healthcare CT
jpego@kpmg.com

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

Anthony Monaco
Government CT
amonaco@kpmg.com

Todd Semanco
Financial Services CT
tsemanco@kpmg.com

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

Mike Lamberth
Insurance CT
mlamberth@kpmg.com

Jennifer Shimek
Healthcare & Life Sciences CT
jshimek@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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.