

Compliance and Integrity: Challenging the status quo to navigate shifting tides

Forensic & Integrity Services

US edition of the 2024 Global Integrity Report



EY

Building a better
working world

CONTENTS

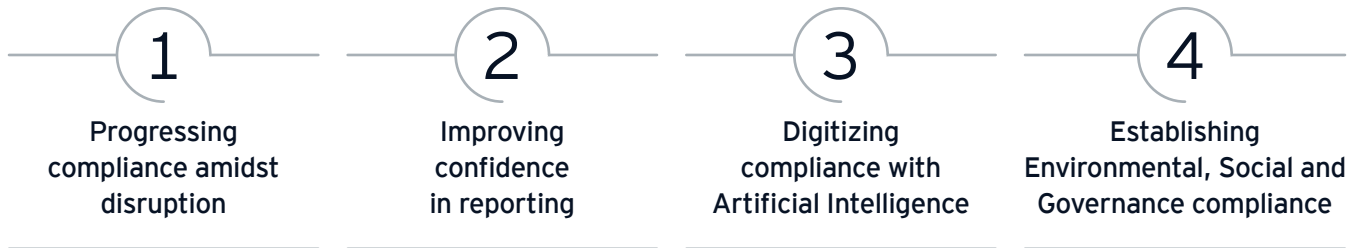
1	Forward	3
2	Key highlights	4
3	Progressing compliance amidst disruption	6
4	Improving confidence in reporting	14
5	Digitizing compliance through AI	19
6	Establishing ESG compliance	26
7	Methodology	32

1 Forward

Against a backdrop of strong macroeconomic forces and changing international regulations, global compliance leaders are navigating a difficult course of rapid developments as reflected by our recent survey of more than 5,000 board members, executives, managers and employees from public and private entities around the world.

We are providing this US edition to complement the [EY Global Integrity Report 2024](#). Our US edition focuses on global companies that have already made great progress in maturing their compliance function and desire to meet new challenges with advanced compliance practices and innovative technologies. For this reason, the US edition concentrates on survey respondents in global organizations with more than 10,000 employees.

Our research explores four key issues facing compliance professionals:



The content in this report is intended to help leaders entrusted with upholding compliance and integrity standards learn more about how multinational organizations are approaching compliance challenges and advancements. It includes our insights and key takeaways to manage the expanded compliance agenda and demonstrate the strategic value that compliance brings to the organization.



Liban Jama
EY Americas Forensic & Integrity Services Leader



Kris Curry
EY Americas Forensic & Integrity Services Deputy Leader

Key highlights

Our extensive research highlights critical insights across the four focal areas affecting compliance leaders today. The findings underscore the evolving challenges and opportunities within the dynamic landscape of compliance. Below, we present the key highlights from our survey.

1. The complex economic and regulatory environment places greater significance on the value that compliance must deliver to the organization.

External forces are exerting a significant impact on compliance risks, challenging and transforming conventional models of compliance. Our survey shows that external stakeholder expectations, a changing regulatory landscape and economic pressures are the top challenges for corporate compliance professionals to maintain business integrity. **Organizations need to maximize the impact of their compliance function, and they can do this by elevating the status of compliance in the organization to equal other strategic positions and enhancing its visibility among senior leaders and corporate boards.**

Nearly twenty-five percent of compliance and legal professionals surveyed have experienced a significant integrity incident, such as a major fraud, security breach or regulatory violation, in the past two years. It's critical for companies to learn from their wrongdoing and determine the root causes behind major and repeated violations. **Leading-class organizations leverage these insights and lessons to strengthen the compliance environment by fixing operational loopholes, reinforcing compliance weaknesses and improving detection methods in riskier business areas, while also considering the role of new technologies in these improvements.**

Organizations should align their compliance priorities with their most critical risks and areas needing enhancement. Compliance and legal professionals rank data privacy and security as the top risk, with fraud and corruption also posing significant concerns. They identified employee training and risk assessments as key compliance areas for improvement. **In shaping compliance priorities to address elevated risks and vulnerabilities, leaders should strategically incorporate advancements in technology and artificial intelligence (AI) into the areas of compliance with the greatest forecasted returns on investment, reducing efforts on existing compliance activities and freeing up limited resources.**

Today's business environment places greater strategic value on compliance to manage the risk of corporate misconduct and achieve statutory compliance. Compliance leaders, facing expanding responsibilities to navigate the ever-changing risk landscape, are pursuing agile compliance programs fueled by data-driven insights. They need to strategically incorporate technology and drive compliance priorities to manage dynamic risks and demonstrate business value. **To enhance these efforts further, leaders can measure the organizational benefits of compliance progress and quantify return on investment to show success.**

2. Employees need more than reassurance and encouragement to feel safe to report concerns.

Technology has advanced the state of whistle-blowing reporting and creation of a speak-up environment, including offering greater ease of reporting and better anonymity and flexibility in reporting. Despite this progress, one in five survey respondents admit to having a concern in the past two years that went unreported, which highlights the continued need to build employee trust in the whistle-blowing process.

Compliance leaders can take direct actions to improve confidence in reporting by addressing the main factors behind employee's reluctance to report misconduct: corporate accountability and whistle-blower safety. **Compliance leaders should consider strengthening accountability by demonstrating consistent disciplinary actions, objectivity of the investigation team and transparency in whistle-blower communications. Leaders can advance beyond simple policy statements by embedding specific confidentiality and anti-retaliation protocols to protect whistle-blowers into the report handling process. Finally, they should increase organizational awareness of these measures and their effectiveness through audits of the whistle-blower hotline, sharing audit findings and resulting improvement plans throughout the company.**

These tangible efforts go beyond simply encouraging a speak-up culture to actually creating an environment where employees feel secure to report issues, confident that their concerns will be taken seriously and appropriately acted on.

3. Emerging AI technologies are digitizing and modernizing compliance programs.

With the rapid acceleration of technology in business, compliance leaders are adopting modern solutions within everyday operations aligned to current business practices and regulatory expectations.

Our survey finds that nearly one in three large corporations are using at least one AI-enabled technology within their compliance environments, most frequently in continuous program improvement, third-party due diligence and ongoing monitoring. Survey respondents identify continuous improvement as the compliance activity that would most benefit from AI and the correlation of disparate data sets as the greatest AI use case. However, organizations struggle with how best to channel AI, citing lack of in-house expertise. **Companies overcome this challenge by establishing a cross-functional team responsible for guiding the use of emerging technologies, managing critical risks around privacy, security and transparency; and establishing guardrails aligned with responsible design principles and legal requirements.**

Guided by a team of experts and strong risk management, compliance leaders can confidently explore how AI technologies can uplift current compliance efforts and integrate with existing technology capabilities. By using this strategic approach, organizations are better positioned to find long-term success in using digital technologies to achieve overall compliance objectives.

4. The introduction of international regulations warrants the involvement of compliance within corporate ESG initiatives.

Corporations are challenged with managing evolving environmental, social and governance (ESG) standards of sustainable and responsible business practices. Our survey finds that complying with new and changing regulations is now the top ESG compliance issue. This prompts the need for evaluating and monitoring regulatory developments and obligations as part of a continuous ESG risk assessment.

In meeting ESG statutory reporting requirements, data integrity poses a significant disclosure risk, with concerns over data reliability, consistency and accuracy. **This underscores the need for technology-enabled ESG reporting mechanisms and safeguards, with strong monitoring and testing, and the importance of folding sustainability disclosures into the company's existing public disclosure controls and procedures. Companies should also be aware of greenwashing and include this fraud risk in the company's compliance program to prevent, detect and address misconduct.**

Compliance leaders can deliberately shape the role of compliance within corporate ESG initiatives while they are still developing. The scope of compliance's responsibilities and authority should center on the areas where it can provide the greatest impact: achieving statutory compliance, mitigating key risks and upholding ethical standards.

Progressing compliance amidst disruption



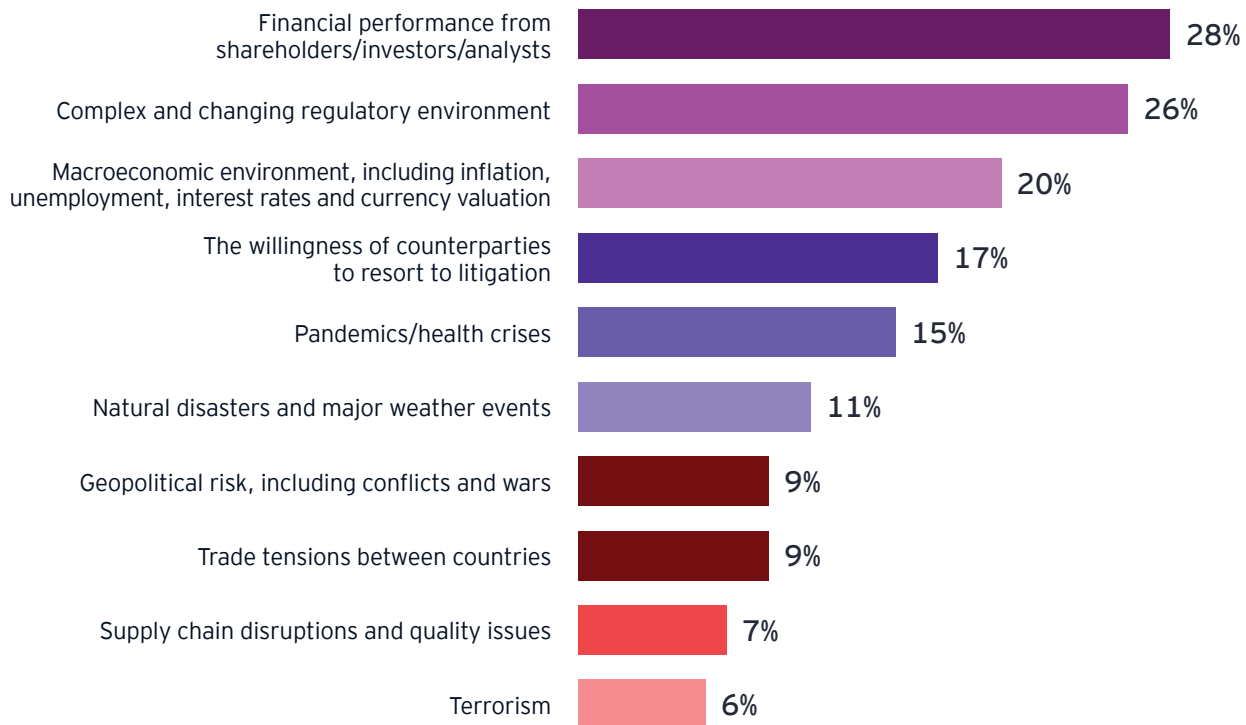
Corporate compliance leaders face considerable pressure from regulators, boards, management, investors and the public to continually improve and demonstrate business value. This responsibility becomes even more challenging in today's dynamic market. Increased macroeconomic and geopolitical uncertainty, growing international regulations, intensified regulatory scrutiny, technology advancements and financial pressures are transforming the landscape of compliance risks and disrupting traditional compliance models.

The current business climate highlights the importance of agile compliance programs fueled by data-driven insights. Compliance leaders pressing to implement sustainable and adaptive compliance solutions are exploring the strategic application of emerging technologies, such as advanced analytics, robotic process automation and AI. The survey results below highlight the key risks and issues on the minds of compliance leaders, as well as the actions that they are taking to deliver strategic value to their organizations.

Dynamic external conditions

Understanding both external and internal influences on corporate behavior is essential when tailoring compliance programs to address evolving business practices and regulatory expectations. According to our survey, the top three external forces identified by compliance and legal professionals creating the greatest difficulty to maintain compliance standards are: expectations from external stakeholders, the complex and changing regulatory environment, and economic pressures.

Which, if any, of the following external factors create the greatest pressure and/or opportunities for employees to violate your organization's standards of integrity?



Macroeconomic factors significantly impact business operations, supply chain management and customer buying power, jeopardizing a company's ability to meet its financial targets and stakeholder expectations. Global economies are experiencing major disruptive events at a high velocity, including elevated inflation and interest rates, exchange rate volatility, geopolitical risk involving conflicts and wars, natural disasters and major weather events, terrorism, trade tensions and sanctions, pandemics and health crises. These events often have a direct impact on a company's bottom line, creating pressure on executives to take aggressive action to meet the company's targets. Such actions, however, may not align with the company's ethical standards. The pressure on management is intensified by the connection between their personal financial incentives and the organization's performance. With ongoing global economic volatility, this elevated pressure on corporate earnings is likely to remain, leading to ongoing challenges in maintaining compliance and ethical conduct.

Fines and penalties fell slightly in 2023 but remain high

In 2023, enforcement actions by the Securities and Exchange Commission (SEC) rose by 3% to 784, with monetary relief of more than \$5 billion, down from 2022's \$6.4 billion. During the same time, the Department of Justice (DOJ) corporate cases closed rose 14% to 8, while monetary recoveries fell to \$690 million from \$2.14 billion. Both agencies noted a higher case count but a lower average monetary value per case.

In addition to these macroeconomic factors, the ever-changing international regulatory environment adds another layer of complexity to compliance efforts. Encompassing areas such as privacy, antitrust, trade sanctions and consumer rights, regulators continue to introduce new laws and regulations, placing significant requirements on multinational corporations. Businesses are finding it difficult to keep pace with the speed and scale of new regulatory developments, especially given the severe consequences associated with noncompliance. Looking ahead at regulatory agendas, the fast pace of international regulatory activity shows no signs of slowing down in the near term.

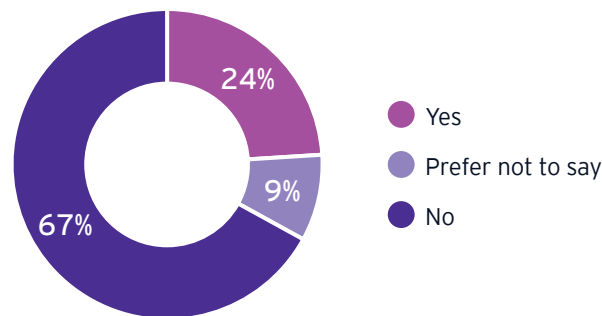
The dynamic economic and regulatory environment, as well as potential financial exposure from noncompliance, places greater strategic importance on the role of compliance within the organization to uphold business integrity and compliance standards. To achieve this, many leading-class corporations are elevating the prominence of their compliance function within the organization to maximize its impact. This includes rethinking corporate hierarchies to empower compliance with the same level of authority as other strategic positions within the company. Additionally, corporations are increasing the awareness and visibility of compliance matters among senior leadership by prioritizing and improving compliance reporting at board and executive updates.

Since 2017, the DOJ has refined its compliance program guidance, emphasizing the need for robust, adaptable corporate compliance functions. Key developments include:

February 2017	April 2019	June 2020	September 2022	March 2023
The Criminal Division of the DOJ introduces the Evaluation of Corporate Compliance Programs (ECCP), outlining essential compliance program criteria.	ECCP revisions expand its utility, introducing three evaluation questions on design, implementation and effectiveness.	Further ECCP refinement highlights data analytics and the integration of compliance controls in acquisitions.	The "Monaco Memo" directs new ECCP considerations, including compensation clawbacks and monitoring of personal devices.	An ECCP update adds a subsection on ephemeral messaging, focusing on policies, training and enforcement related to personal device use for corporate communications.

According to our survey,
nearly one in four organizations has had a significant integrity incident in the last two years.

Has your organization experienced a significant integrity incident, such as a major fraud or regulatory compliance violation, in the last two years?



Learning from past incidents

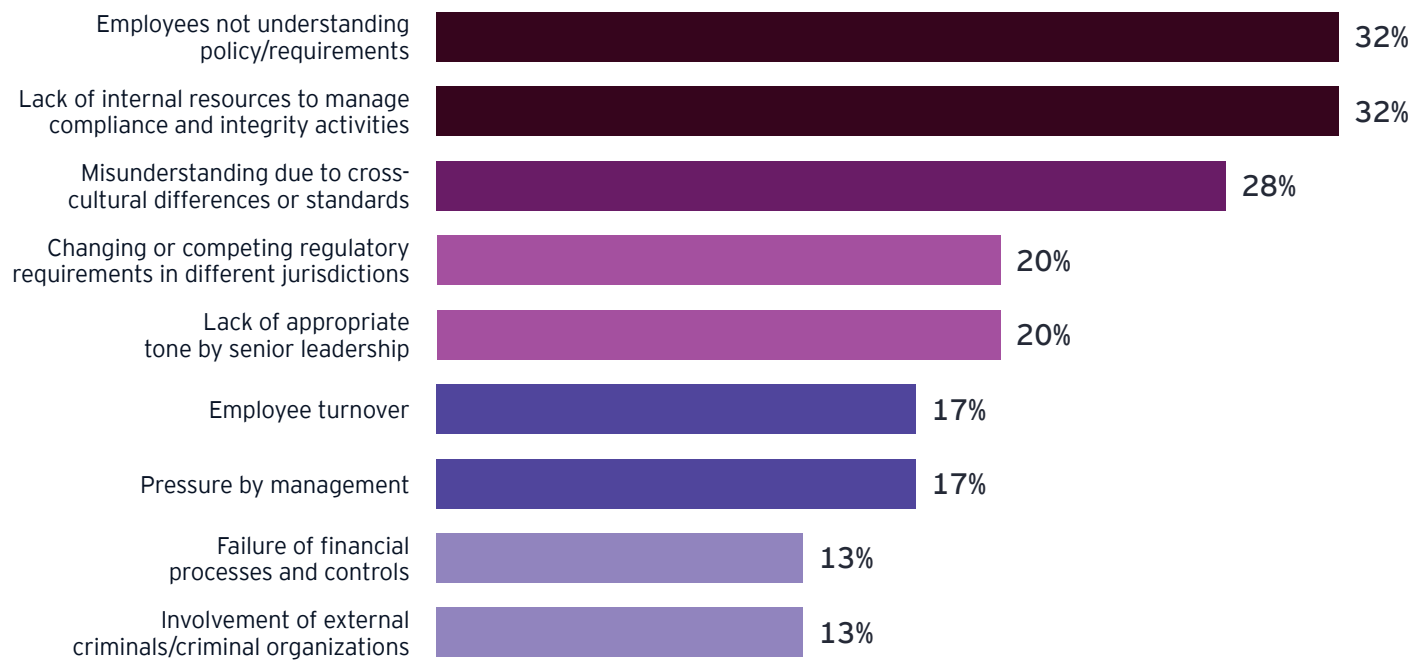
Even the most effective compliance programs are not immune to instances of noncompliance, which can be both costly and disruptive to the organization. In the wake of misconduct, it's imperative for a company to learn from its wrongdoing. By doing so, it can identify and correct systemic issues, prevent recurrence, maintain trust with stakeholders and foster a culture of integrity.

Nearly twenty five percent of survey respondents in compliance and legal roles faced a significant integrity incident, such as a major fraud, security breach or regulatory violation, in the last two years. Respondents report that almost half of these incidents relate to corruption and bribery issues, with the remainder mostly distributed among data privacy and security, fair trade, fraud and theft, labor laws and international trade issues.

Corporations should carefully evaluate the nature of past incidents and determine the root cause of major and repeated violations. Understanding these issues helps to identify common drivers and lessons learned to guide the remediation of internal controls and compliance measures, which is crucial for preventing and detecting similar misconduct moving forward. This type of root cause analysis also aids in uncovering systemic operational issues requiring more broad remediation across the organization.

According to survey responses from legal and compliance professionals, employees not understanding corporate policies or misinterpreting them due to cultural differences ranks among the top internal causes surrounding compliance violations. Recognizing this, we regularly see compliance leaders advocate for the simplification and consolidation of policies as a strategic initiative to enhance organizational understanding and adherence to corporate and regulatory requirements.

Which, if any, of the following internal factors create the largest pressure and/or opportunities for your employees to violate your organization's standards of integrity?



Traditional compliance strategies, such as increased communication and training, aim to boost employee awareness of compliance policies and requirements. Organizations are enhancing these efforts with specialized educational campaigns and on-demand communication channels, hoping to see better outcomes. However, leading-class corporations are going a step further with innovative approaches to make compliance easier for employees to follow and to prevent wrongdoing in the first place. They are leveraging learnings from reported misconduct, as well as ongoing compliance efforts, such as employee inquiries, risk assessments, auditing and remediation activities, to proactively identify and remove operational loopholes and weaknesses used to circumvent compliance requirements. This approach is even more effective when compliance requirements transition into business requirements by embedding compliance conditions and preventative controls directly into underlying business systems, workflows and processes.

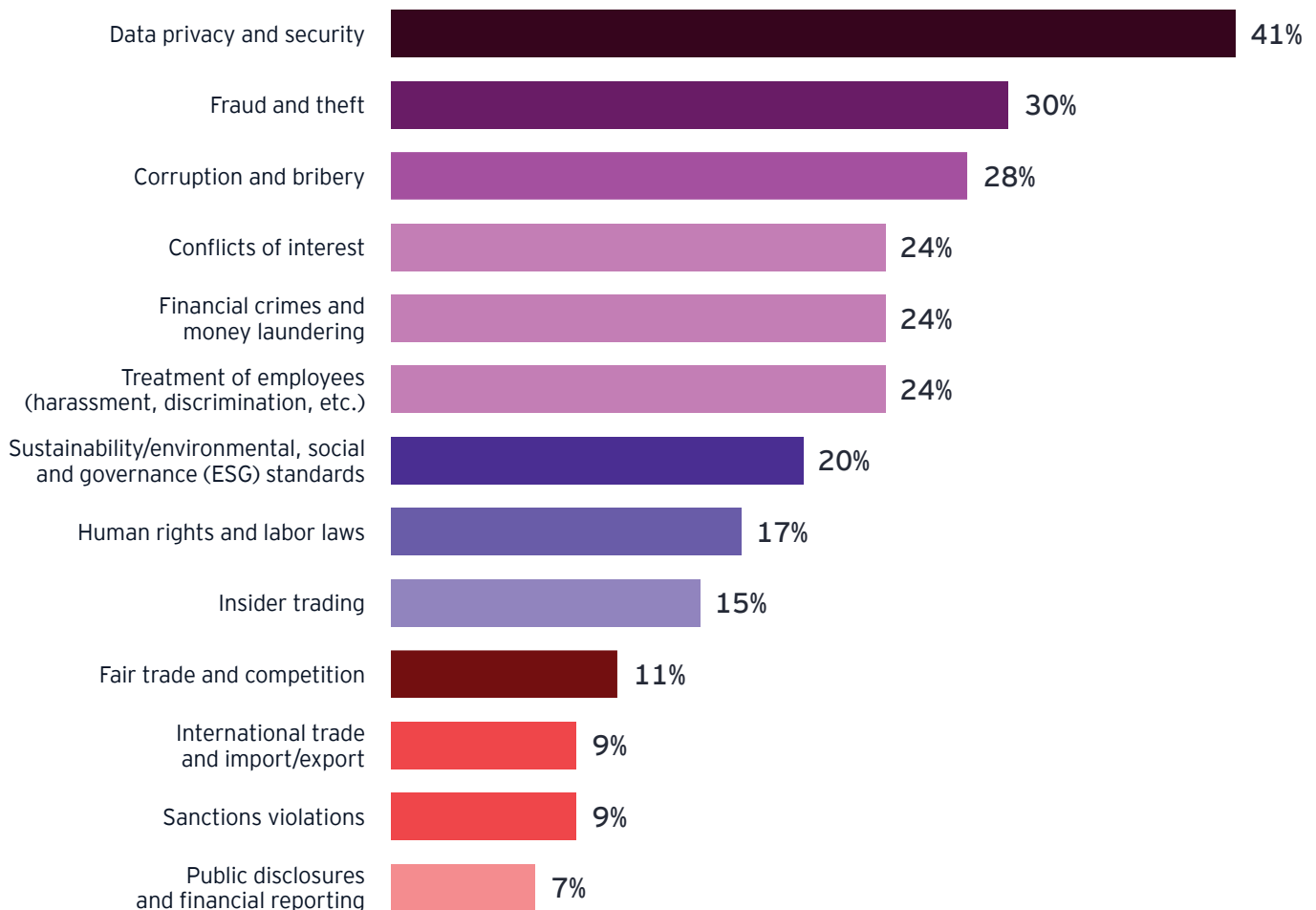
Another key insight from past incidents is the importance of not only preventing them but also detecting them. In business areas or regions where compliance issues are more prevalent, especially those with substantial cultural differences and low whistle-blower activity, companies are recognizing the limitations of employee training alone. As a response, they are exploring stronger detection techniques to identify misconduct at an earlier stage. Survey participants highlight Eastern Europe, China, the Middle East and North Africa as the regions with the most significant compliance risks. In response, leading companies are stepping up detection methods in these regions through targeted monitoring and enhanced audit procedures, aided by technologies such as advanced data analytics, robotic process automation and AI. Earlier detection of misconduct minimizes its impact by allowing organizations to promptly intervene, thereby limiting damage and monetary losses. Moreover, findings from monitoring and auditing can be embedded back into local training programs as a further deterrent measure.

Balancing compliance risks and priorities

An organization’s compliance priorities should be strategically shaped by a thorough assessment of its greatest vulnerabilities: (1) the organization’s most significant compliance risks and (2) the compliance measures requiring the most improvement. This tailored approach ensures that resources are allocated effectively, focusing on mitigating the highest risks that could potentially lead to legal penalties, financial loss or reputational damage. Simultaneously, by identifying and addressing the weakest links in their compliance framework, organizations can strengthen their overall compliance value. This dual focus on risk magnitude and areas for improvement allows for a proactive and comprehensive compliance strategy that not only protects the organization but also promotes a culture of integrity and ethical conduct.

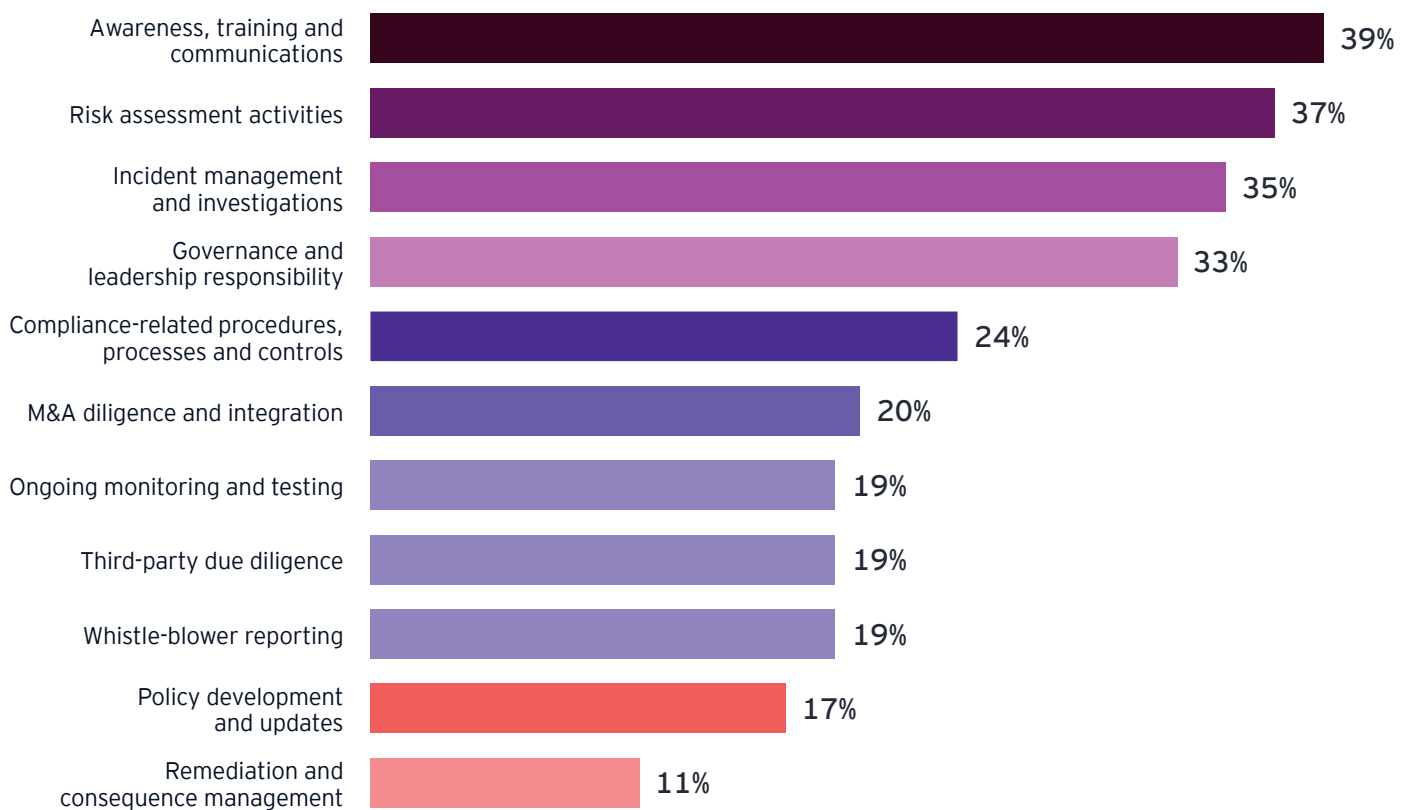
Survey respondents in compliance and legal positions identified data privacy and security as the foremost compliance risk facing their organizations, followed by risks of fraud and corruption. The acute focus on data privacy and security suggests that many organizations will focus on strengthening internal infrastructure and operations in cybersecurity, data governance and privacy regulations in the short term. Many effective leaders are taking a “security by design” approach, integrating security measures into the deployment of new technologies to defend against cyber and data privacy threats.

Which, if any, of the following pose the greatest integrity risks, including compliance and fraud risks, for the organization over the next two years?



An effective compliance program is one that continuously improves and evolves by addressing potential weaknesses in the compliance environment. According to our survey, legal and compliance respondents identified employee awareness and training and risk assessment activities as the top two compliance areas in need of improvement. Both of these compliance areas lend themselves to technology enablement. Leading organizations are augmenting traditional training programs with on-demand employee support and adding compliance messaging functionality through technology platforms, such as user-friendly AI chatbots. They are also standardizing and streamlining their risk assessment methodology, using a data-driven approach featuring risk scoring capabilities and technology automation within data gathering and dashboard reporting.

When it comes to your organization's integrity standards, which areas do you feel need the most improvement over the next two years?



Compliance leaders are seeing their roles and responsibilities expand as they navigate an ever-changing risk environment, adding pressure to an already long list of demands and priorities. They must evaluate these competing priorities to determine the right investment of resources and capital. More and more, leading corporations are strategically incorporating advanced technology and AI in the compliance areas promising the highest investment returns, such as cost savings from quicker detection, saved resource time, avoidance or reduction of penalties, and improvements in compliance metrics. This enables better resource allocation toward higher-value activities.

There is a practical balance in every organization between compliance progress and capital investment. Progress does require investment but not necessarily all at once. For large investment projects, companies can develop an incremental approach that divides the project into distinct phases aligned to the overall compliance strategy. Each phase is characterized by defined metrics and targets. Using a milestone approach helps to ensure long-term success while clearly demonstrating value along the way.

Key takeaways to progress compliance amidst disruption

- 1 Elevate the position of compliance within the organization by empowering compliance with the same level of authority as other strategic roles and improving visibility to senior leadership and boards.
- 2 Use lessons learned from past incidents and root cause analysis to identify operational loopholes, compliance weaknesses and business areas in need of stronger detection techniques.
- 3 To determine compliance priorities, conduct comprehensive assessments to identify the organization's most significant compliance risks coupled with the compliance measures requiring the most improvement.
- 4 Strategically incorporate advanced technologies and AI into the compliance areas with the greatest potential returns on investment, factoring in benefits such as cost savings and better resource allocation.
- 5 Measure the impact that compliance advancements have in terms of value for the organization and track the return on investment. For larger investments, develop a phased approach with distinct milestones to demonstrate incremental value and success.

4 Improving confidence in reporting

The real test of a compliance program lies not in its capacity to prevent or detect misconduct, but in the organization's handling of such situations. The company's response to misconduct establishes the culture of integrity and accountability and greatly affects the willingness of employees to report problems and raise concerns.

An organization's commitment to ethics and compliance goes well beyond having a reporting mechanism to capture employee and third-party concerns. When US regulators evaluate the strength and maturity of a company's compliance program, they consider the degree to which an organization fostered a speak-up culture that encourages open communication to identify potential misconduct. To create this environment, it is essential that employees feel safe to report issues and trust their concerns will be taken seriously and appropriately acted upon. While advances in reporting have improved this trust, continued efforts are necessary to strengthen employee trust even further.

Advances in reporting

Companies have made significant investments in a speak-up culture, encouraging employees to report issues without fear of retaliation. Our survey reveals that large corporations see general improvement in their whistle-blowing environment within the last two years, stemming from greater ease of reporting concerns, greater anonymity and flexibility in reporting, and greater protection from retaliation. There is also a notable trend where younger employees prefer to report concerns through digital channels, contributing to an increase in the total volume of reported issues in recent years. This change provides deeper insights into compliance risks within company operations and facilitates identification of areas needing improvement.

Organizations are eager to understand if their efforts to create a speak-up culture are working; many leading-class corporations are evaluating confidence in the whistle-blowing process through employee surveys and culture assessments. Others are incorporating measurements into their current compliance risk assessments. These approaches provide valuable input, enabling companies to target improvement areas and measure their progress over time.

Corporations are increasingly leveraging technology to streamline and enhance whistle-blowing channels and reporting tools. Third-party technology platforms, which feature whistle-blower anonymity, web-based reporting and consistent intake, now seamlessly integrate with internal Governance, Risk Management and Compliance (GRC) systems. Internal investigation teams are using structured dashboards to monitor whistle-blower metrics and perform benchmarking. Case management tools transcend simple document repositories – they characterize issues, manage case workflows, track progress, facilitate collaboration and streamline communications. These advancements not only elevate the whistle-blowing environment but also underscore the company's commitment to effectively address misconduct.

Improving reporting with AI

Corporations are using innovative applications of AI to enhance their whistle-blowing processes, such as:

Chatbots - Offer a user-friendly alternative for report intake, allowing individuals to submit concerns in writing with the ability to ask immediate follow-up questions for clarification.

Data intake - AI-driven generative models create dynamic data entry forms that adjust in real time based on the reporter's input. This streamlines the intake process by bypassing irrelevant questions and ensures reports are automatically routed to appropriate personnel.

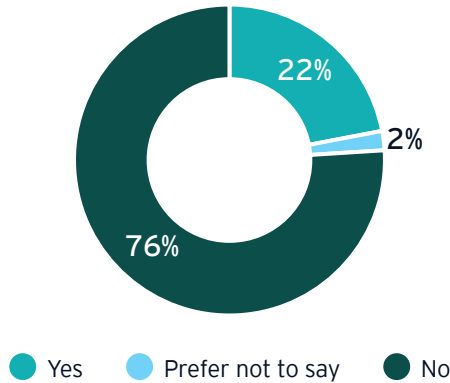
Transcription - AI technology is used to transcribe audio reports and convert free text narratives into structured data formats.

Translation - AI-powered tools translate reports across multiple languages and can summarize allegations across matters to facilitate executive reporting.

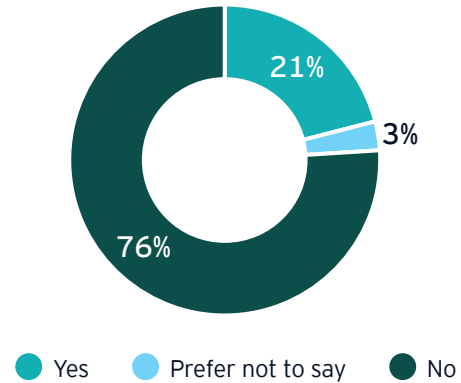
Employee trust in reporting

A persistent challenge within the whistle-blowing channel is continued improvement of employees' willingness to use it. According to our survey, about one in five respondents (22%) at large corporations reported concerns of misconduct in the last two years. Alarming, an almost equal number of respondents (21%) admit to having a concern in the same time period but not reporting it. This represents a significant volume of potential misconduct that remains unreported, highlighting the critical need to foster a strong speak-up culture.

Have you personally reported issues of misconduct, for example, to management or to a whistle-blowing hotline, in the last two years?



Have you had concerns about misconduct that you have not reported in the last two years?



Survey participants indicate that corporate accountability and negative consequences are

the two biggest factors behind their reluctance to report misconduct,

fears that are amplified if leadership is involved in the wrongdoing.

1

Lack of accountability

When asked why they did not report, the No. 1 reason provided by our respondents (46%) was the belief that their concerns would not be acted upon. Additionally, 30% report that unethical behavior is often tolerated when it involves senior executives or high performers.

2

Adverse consequences

Twenty percent of employees acknowledge experiencing or witnessing retaliation against a whistleblower, and 37% express reluctance to report issues due to concerns of future career progression. Moreover, when employees did report concerns, over half (52%) felt pressure not to report the misconduct at all.

Many companies have general policies that prohibit retaliation, provide whistle-blower confidentiality and describe penalties for violations. However, these policies are often not actively implemented with strong and transparent protocols in the report handling process. Enhancing corporate accountability and whistle-blower protection – beyond policy statements – is key in cultivating employee trust.

Corporations can improve accountability by demonstrating clear, consistent and objective actions in response to reported concerns. Practical examples include:

Assigning and enforcing disciplinary measures consistently across the organization at every level. Developing and publishing disciplinary guidelines to provide a basis for fair and consistent disciplinary actions, regardless of an individual's position, status or seniority.

Offering whistle-blowers greater transparency into the investigation actions and outcomes by providing them periodic updates on the status and resolution of their reported complaints.

Affirming that those charged with investigating and resolving reports are truly independent and impartial. In cases involving senior leadership, this may require formation of a special committee and use of external advisors to investigate allegations and determine disciplinary actions.

Corporations can reduce perceptions of adverse consequences by demonstrating robust whistle-blower safety and protection. Practical examples include:

Developing specific privacy protocols and controls to offer greater confidentiality protections, while maintaining strict adherence to these standards throughout the report handling process. Confidentiality protocols include restricting access to sensitive information, encrypting and redacting sensitive information, using pseudonyms or aliases, and securely handling and storing whistle-blower information.

Implementing retaliation prevention measures and raising awareness of retaliatory behavior through employee training and communications.

Proactively detecting signs of retaliation by monitoring factors that may lead to such behavior, both directly and indirectly. Promptly addressing suspected and reported instances of retaliation with appropriate intervention and disciplinary measures.

Corporations can also build trust in reporting by subjecting the whistle-blower hotline to periodic audits. In addition to testing the effectiveness of hotline controls, such audits evaluate the consistency of disciplinary actions, transparency in whistle-blower communications, objectivity of the investigation team, maintenance of whistle-blower confidentiality and effectiveness of anti-retaliation measures. Audit results are then used to develop targeted improvements. One leading practice is to publish summary findings from the hotline audit throughout the organization to reinforce employee confidence in the reporting process.

Employee reluctance to raise concerns is a serious deficiency in the compliance culture of an organization. Our research indicates that organizations should thoroughly assess if a speak-up culture is truly reflected throughout the company. If it is not, stronger efforts around corporate accountability and whistle-blower protection are necessary to improve confidence in how the company handles reports.



DOJ's new corporate whistle-blower reward program

Internal whistle-blower channels face increasing avenues of competition through external whistle-blower programs, both in the US and globally, that offer attractive financial incentives to individuals who come forward. The DOJ recently announced the introduction of a whistle-blower pilot program expected to be formally implemented later this year. The new program promises financial rewards to those who provide information leading to the discovery of significant corporate or financial wrongdoing. The program will accept tips on any federal law violations, making it wider in scope than other US agency whistle-blower programs.

The DOJ's program joins a list of existing agency programs, including the SEC's whistle-blower program. This program received a record number of tips in fiscal year 2023 and issued nearly \$600 million in whistle-blower awards, the highest amount in the program's history. The presence of these external whistle-blowing alternatives makes it even more important for organizations to focus on securing trust in their reporting processes and encouraging employees and third parties to report any misconduct through internal corporate channels.

Key takeaways to improve confidence in reporting

- 1 Measure employee confidence in the whistle-blower channel through employee surveys and culture assessments and use results to pinpoint areas of improvement.
- 2 Explore how technology tools can improve reporting mechanisms, streamline the whistle-blowing process and enhance a speak-up culture.
- 3 Strengthen corporate accountability by ensuring consistent disciplinary actions, objectivity of the investigation team and transparency in whistle-blower communications.
- 4 Curb the perception of adverse consequences by embedding confidentiality protocols and anti-retaliation measures into the report handling process.
- 5 Perform periodic audits of the whistle-blower hotline to test the operating effectiveness of hotline controls and protocols and share audit findings with employees.



Digitizing compliance through AI

Multinational organizations are placing digital transformation at the forefront of their corporate agendas, adopting innovative technologies and methodologies to reach business goals, gain competitive advantages and improve their bottom lines. Relative to other business functions, compliance departments have been slower to apply new technologies, despite pressure from regulatory bodies such as the DOJ. With the rapid acceleration of technology in business, compliance leaders are at a crossroads: adopt modern solutions to digitize compliance or risk maintaining an obsolete program that increasingly fails to align with current business practices and regulatory standards.

The move to digitized compliance

Leading-class companies seek to transform and modernize their compliance activities to better achieve compliance objectives by embedding advanced technology tools and enablers within everyday operations.

This digital transformation includes:

1

Integrating digital technology into existing processes or using technology to reinvent or replace such processes altogether

2

Managing new compliance risks or complying with new regulatory standards through the use of advanced technologies

3

Using technology to produce data-driven insights and generate better and faster decision-making

The DOJ and other regulators have continually underscored the value of integrating technology into compliance, with the DOJ specifically emphasizing the use of data analytics to evaluate the adequacy and effectiveness of compliance programs. However, many companies have found it challenging to aggregate and interpret data from various parts of the organization to measure compliance, especially with the growing amount and complexity of data generated and the disparate systems where this data resides. Leading-class companies have overcome this challenge and developed data-driven risk assessment methodologies using increasingly sophisticated data analytics to merge compliance-related data (such as information from investigations, training and helplines) with operational data (including financial, vendor, customer relations and human resources information).

Reference to EY article:

▶ [New DOJ guidance stresses importance of data analytics](#)

Some innovative companies are reinventing compliance risk management altogether by utilizing a powerful digital solution: a digital compliance scorecard. This approach uses specific metrics to unify different compliance areas under a universal framework, condensing a wide range of risk factors into an understandable, integrated view of compliance. This holistic view enhances transparency into the overall performance of compliance organization-wide, offering practical and meaningful applications. Compliance executives can leverage data-driven scorecards to deliver actionable insights and drive improvements in compliance, facilitate better communications with business partners and clearly demonstrate the value of proactive compliance to senior leadership and board members. The scorecards can be seamlessly integrated into a company's current technology environment, thereby achieving greater benefits from its technology investments.

For more information on the innovative digital scorecard, visit

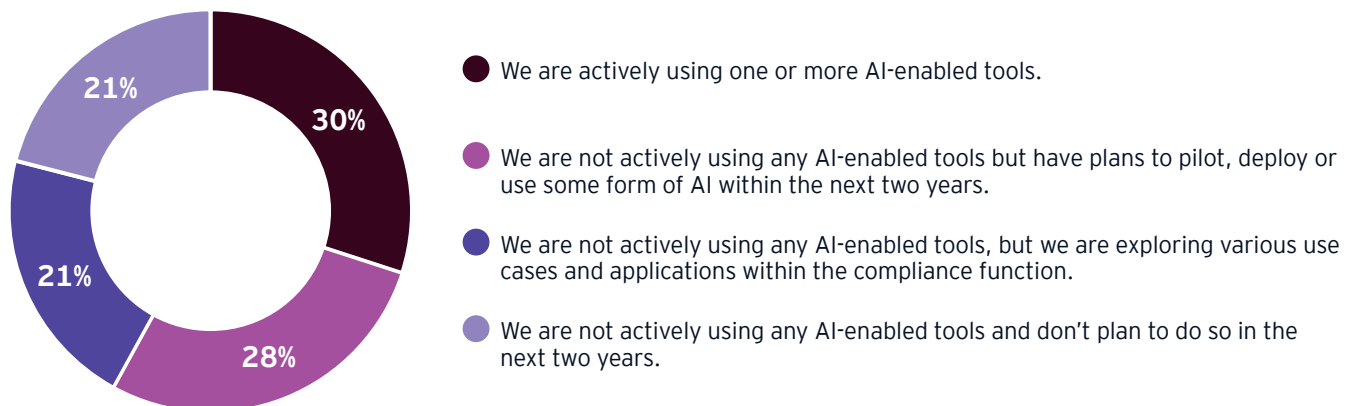
[!\[\]\(666e09182d4cd268646ea700ea60dcdf_img.jpg\) **Honeywell and EY Digital Compliance case study**](#)

In addition to other impressive advancements in compliance technologies, like digital third-party risk management and real-time transaction monitoring, compliance departments are turning their attention to the next chapter in technology – digitizing compliance through AI – and the potential value it can unlock in shaping compliance objectives, initiatives and strategies.

The rise of AI in compliance

Our survey indicates that more than a quarter of large organizations are already incorporating at least one AI-powered tool in their compliance settings. Additionally, nearly 50% are in the process of exploring AI applications or intend to implement them in the next few years. The areas where respondents most frequently reported the use and exploration of AI include continuous program improvement, third-party due diligence and ongoing monitoring.

Are you deploying AI within your compliance function presently?



These responses demonstrate that compliance leaders clearly recognize the strategic importance of emerging technology and the benefits it can provide. The real challenge is in unlocking that potential value; many compliance departments struggle with how to best channel AI within their operations. As reflected in our survey, one of the main barriers is the lack of in-house expertise. Additionally, leaders often face other hurdles in terms of securing executive support and understanding the value proposition, gaining access to relevant data and, of course, obtaining necessary funding.

What are your top challenges in deploying AI within your compliance function?



The successful incorporation of AI first requires a diverse team of professionals with expertise across multiple disciplines who can:

Form the strategic vision to guide the use of technology and data – and establish key performance indicators (KPIs) to measure success.

Establish guardrails with strong data governance to address concerns around security, privacy, cross-border transfers and transparency.

Build and train AI models using responsible design principles.

Develop strong testing mechanisms, including ongoing monitoring and auditing procedures, to verify that AI models produce unbiased output and accurate results.

Monitor the compliant use of AI-enabled tools in accordance with in-house guidelines, jurisdictional regulations and/or legal requirements.

These capabilities come together in a cross-functional team that draws on the diverse expertise within the organization, typically including compliance, legal, IT, data privacy, information security, finance and internal audit. This team is often complemented by external experts, either as an extension of the team or as on-call advisors. The collective insights from each of these stakeholder perspectives serve to address the practical risks associated with AI and set the foundation for long-term value creation.

Applications of AI within compliance

Even with the reported challenges, organizations have successfully deployed AI within compliance settings. Repetitive manual processes lend themselves well to digitization and are generally where companies first introduce AI. Examples include document review and compliance monitoring, which are frequently combined with automation technologies. Such advancements can dramatically impact workforce productivity by streamlining operations and increasing efficiency, presenting a compelling value proposition for compliance departments that may be understaffed.

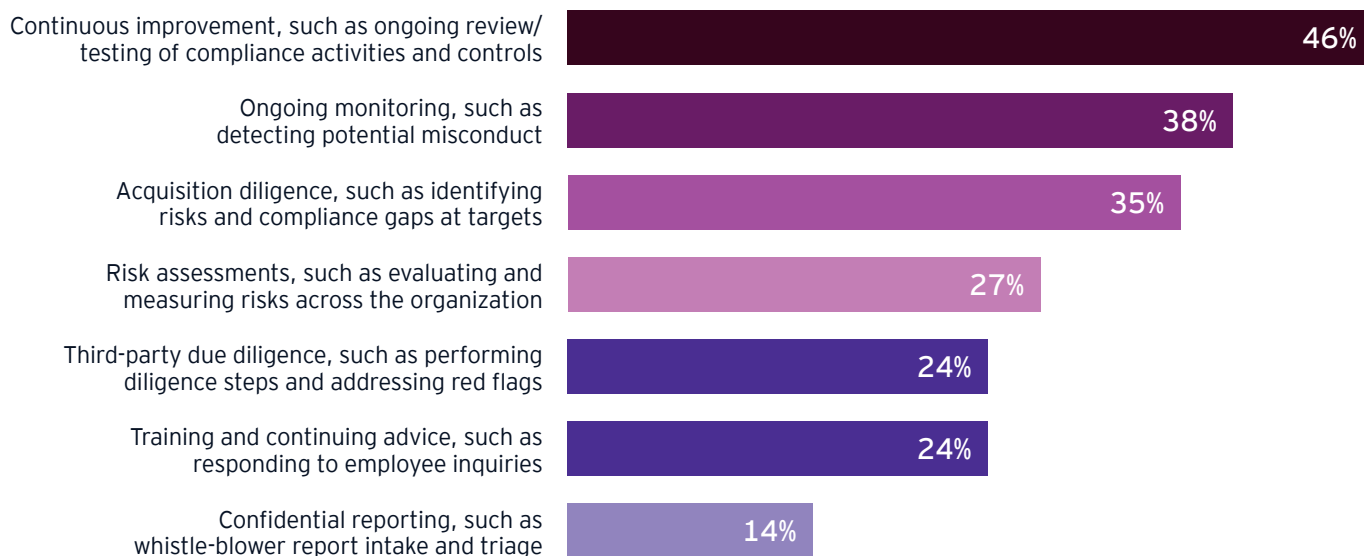
More progressive applications of AI in compliance focus on content generation. For instance, generative AI (GenAI) tools are capable of quickly researching and summarizing substantial amounts of information, drafting policy updates and performing certain e-discovery review procedures. AI is also proving to be a powerful complement to technologies already in use. For example, AI can interpret outputs from data analytics and recommend corrective measures. We recommend exploring use cases where AI can be layered with existing technologies to develop new insights and enable better decisions. This approach can lead to substantial cost savings compared to the investment required to implement an entirely new AI tool or platform to achieve comparable results.

For more information, refer to

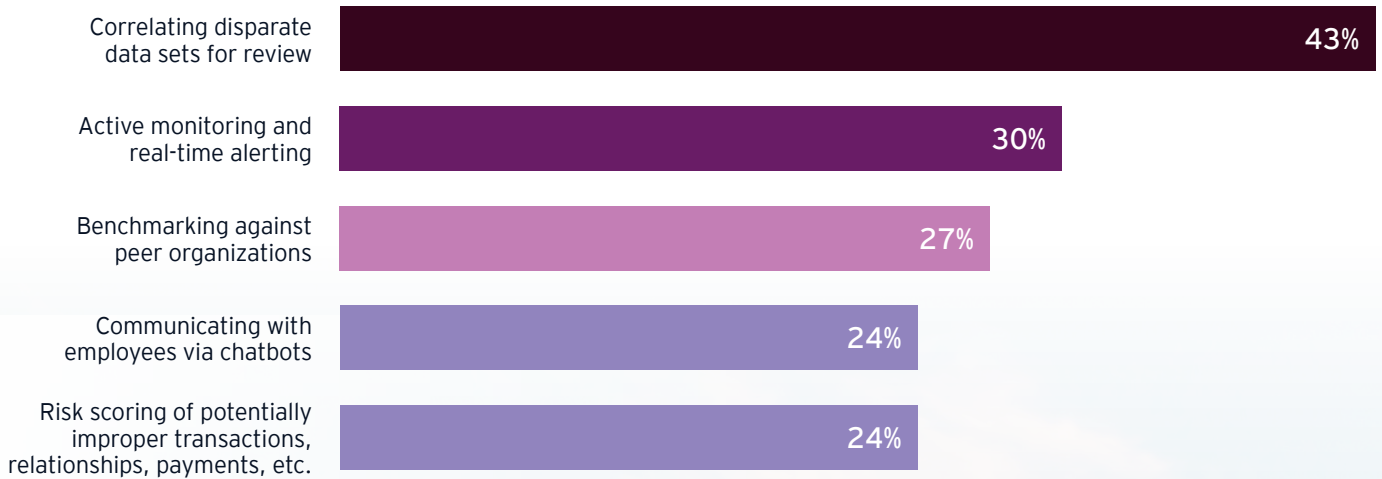
 [EY-Teva TPRM case study](#)

Survey respondents from large organizations ranked the compliance activities that could most benefit from AI, identifying continuous program improvement as the area best suited to AI and the correlation of disparate data sets as the top use case.

Which routine compliance activities do you think are best suited to incorporate AI?



What are the use cases in which AI can have the greatest impact within the compliance function?



Companies are finding greater success by

**taking a thoughtful,
strategic approach to AI,**

one that explores how technology can uplift current compliance efforts and integrate within the existing technology stack to create sustainable value.

Examples of practical, high-value compliance applications include:

- Providing on-demand answers to employees' compliance inquiries, referencing corporate policies and giving intelligent how-to instructions through an AI-enabled chatbot interface
- Streamlining the due diligence process of third-party background checks to synthesize screening documentation and detect reputational red flags
- Improving risk assessments by analyzing financial transactions, communications and other data points to detect weaknesses and recommend enhancements
- Monitoring ongoing regulatory and legislative updates and analyzing internal business data to highlight potential compliance gaps
- Generating real-time alerts of red flag activity within transaction monitoring and triaging instances of potential misconduct
- Mining large data sets with predictive models to perform email and document review in response to regulatory inquiries, subpoena and litigation
- Automatically identifying and extracting or redacting sensitive personal information across whole data sets

Key takeaways to digitize compliance through AI

- 1 Form a cross-functional team to work together in prioritizing specific technology use cases and associated risks with appropriate guardrails.
- 2 Investigate how other departments and peers are using or exploring emerging technologies, such as AI; apply these insights and leverage available technologies when making the business case for compliance.
- 3 Evaluate existing compliance efforts that could significantly benefit from digitization; start by considering areas where resources are spending valuable time performing repetitive, labor-intensive tasks that could be supported by automation and AI technologies.
- 4 Embed strong risk management practices over new technologies to address data privacy, cybersecurity, legal and regulatory concerns. Consider using ongoing monitoring and audit procedures to validate the accuracy of system outputs and to check for biases and hallucinations within AI models.
- 5 Take a strategic and incremental approach and continually measure progress through defined milestones and KPIs that demonstrate the return on investment.



Establishing ESG compliance

Discussions within corporations about aspirational ESG values and voluntary commitments are giving way to practical discussions about the actual execution of ESG initiatives. Attention is shifting toward integrating a variety of ESG issues – including social responsibility, equitable labor practices, ethical governance, carbon footprint reduction and environmental sustainability – into a cohesive ESG framework. This shift occurs against the backdrop of a changing global regulatory environment, where new and proposed sustainability legislation is introducing the element of regulatory compliance to the complexity of corporate ESG.

Companies are facing the challenge of integrating and managing the emerging global standards for sustainable and responsible business practices. Despite this, many compliance leaders have been reluctant to embrace a broad role in ESG compliance due to the dynamic nature of the regulatory environment and uncertainties regarding the level of effort required, especially when compliance departments are already stretched thin and under pressure to manage costs. Nevertheless, with ESG still taking shape within organizations, this is a critical moment for compliance to determine its role. Compliance executives have the opportunity to strategically define and control their responsibilities in ESG compliance and proactively set additional budgetary and resource requirements. If they do not take the initiative to navigate their ESG path now, they may find these decisions made for them as corporate ESG initiatives advance, potentially leading to unplanned resource and financial strains on the compliance function.



Determining the role of compliance within ESG

A key starting point is to first understand why compliance should be involved in ESG. To date, ESG initiatives have been defined by voluntary sustainability practices and self-imposed targets. However, with the swift enactment of ESG-related legislation globally, companies are losing their discretion to set their own goals and ambitions. Since compliance teams are tasked with ensuring that a business adheres to applicable laws, regulations and industry standards, it is appropriate for them to be involved in the development of policies and programs that address ESG regulatory compliance.

So the question is: What distinct role should compliance assume within the organization's ESG framework? Compliance may not assume responsibility for all ESG-related compliance efforts; in fact, our survey finds that accountability for ESG compliance differs significantly among larger organizations. The functions most often assigned to manage ESG responsibility include compliance, human resources, legal, operations, risk management and sustainability. While procurement, finance and investor relations also contribute to ESG efforts, they are less commonly charged with overall responsibility.

Which of the below functions in your organization have responsibility for ESG compliance?



The different governance models stem from the fact that ESG permeates all aspects of an organization, covering a wide array of issues, such as supply chain management, data privacy, product and packaging sustainability, diversity and inclusion, workplace safety and social justice. This often results in a fragmented strategy where different functions and business units pursue their individual objectives. A robust ESG governance framework, directed by senior leadership, is crucial for steering the company's ESG initiatives and strategic priorities. By setting precise roles and responsibilities with defined accountability for all stakeholders, organizations can ensure cohesive alignment with these ESG priorities.

Regardless of a company's ESG structure, the role of compliance within ESG should be clearly defined and center on the areas where it can provide the greatest impact: adherence to statutory requirements, management of critical risks and promotion of ethical behavior. For instance, compliance teams possess the specialized expertise required to conduct an extensive risk assessment focused on the company's key ESG goals and evolving regulatory landscape, evaluating regulatory, legal and reputational risks. Furthermore, with its institutional knowledge and established infrastructure spanning across functions and business units, compliance is ideally positioned to create and manage the necessary framework to identify, address and monitor the organization's key ESG risks and compliance with statutory obligations. Compliance leaders have the opportunity to proactively and deliberately shape these responsibilities while ESG structures are still developing.

Achieving statutory compliance with new and developing ESG regulations

We find that most organizations are in the early stages of developing their ESG compliance programs and are struggling to keep up with the rapid development of international standards. Compliance with new and changing regulations is the top challenge in ESG compliance for larger corporations, surpassing issues related to data integrity.

Which, if any, of the following are the greatest challenges for your organization to meet its ESG regulatory requirements?



ESG matters have progressed from nice-to-have priorities for global policymakers into strategic imperatives, resulting in the rapid development of new regulations and corporate reporting requirements. This has created a complex and growing landscape of competing sustainability legislation.

Current laws

US: Standardized climate-related disclosures: new rule that requires SEC registrants to disclose sustainability-related details, such as climate-related risks, likely to have a material impact on the business; information on the registrant's climate-related targets or goals; and, for certain registrants, information related to greenhouse gas emissions

EU: Sustainable Finance Disclosure Regulation (SFDR): applies to EU-based financial institutions as well as foreign-domiciled financial institutions that operate within the EU; requires entity-level disclosure of how firms and financial advisors consider sustainability

EU: Corporate Sustainability Reporting Directive (CSRD): standardizes nonfinancial measures on ESG reporting by requiring all companies doing business in the EU to report on their environmental and social impacts

EU: Carbon Border Adjustment Mechanism (CBAM): encourages cleaner production in non-EU countries through fees charged by importers for the emissions embedded in their imports

Germany: Supply Chain Due Diligence Act (SCDDA): requires German companies and those with significant operations in Germany to disclose measures taken to prevent and mitigate the risks of human rights violations and environmental damage within their operations

India: Business Responsibility and Sustainability Reporting (BRSR): requires reporting by Indian registrants on governance of the organization and nine key principles that demonstrate responsible business conduct

Proposed laws

Australia: Climate-Related Financial Disclosure (proposed). In December 2022, the Australian Commonwealth Government Treasury released a Climate-Related Financial Disclosure Consultation Paper. The paper outlines the climate disclosures that certain Australian companies may have to make in the near future related to climate-related risks and opportunities.

Canada: Disclosure of Climate-Related Matters: While not yet finalized for all companies operating in Canada, federally regulated financial institutions will be required to provide ESG disclosures on management and board oversight of climate-related risks and opportunities for reporting periods beginning as early as January 1, 2025.

Multinational organizations require a thorough legal analysis of sustainability regulations across all jurisdictions in which they operate to identify existing and anticipated regulatory obligations and reporting requirements. This legal analysis is a key element of an agile ESG risk management strategy and should be folded into a comprehensive ESG risk assessment to enable corporations to promptly respond and adapt to emerging ESG issues and evolving international and industry standards.

For more on developing an effective risk management strategy, refer to

▶ [ESG risk strategy for C-suites and boards](#)

Managing data integrity risks within ESG reporting

Companies are increasingly publishing their ESG initiatives, goals and metrics. The growing public interest in these disclosures has attracted regulatory attention. In the United States, the SEC finalized rules on March 6, 2024, aiming to “... respond to investors’ demand for more consistent, comparable, and reliable information about financial effects of climate-related risks,”¹ underscoring the importance of transparency and accuracy in public reporting. Major corporations are already defining and gathering necessary data sets for ESG reporting, although concerns about data reliability, consistency and accuracy remain among the top challenges in meeting ESG requirements.

The SEC brought multiple civil actions in 2023 against public registrants related to ESG issues, resulting in nearly

\$60 million in penalties.²

Data integrity poses a significant challenge in the context of ESG because of the diverse formats and decentralized systems in which information is stored throughout an organization and because it is gathered independently of the company’s financial reporting process. This issue is exacerbated by the country-specific nature of ESG reporting standards, increasing the inherent risk of manual errors and omissions. Inaccurate reporting can result in reputational harm, customer attrition and increased regulatory scrutiny. To avoid costly mistakes, businesses should prioritize technology-based reporting systems and automation. Industry-leading companies are developing robust technology strategies that include automated data feeds, structured workflows, standardized outputs and embedded safeguards. These measures aim to automate the assembly of ESG data and metrics in a consistent and trusted manner.

In addition, ESG-related public disclosures should be integrated into the company’s established controls and procedures for both financial and nonfinancial reporting. These processes are generally subject to internal controls testing and records retention policies. For US SEC registrants, such required disclosure processes provide assurance in the quality and integrity of publicly reported information.

ESG data risks also extend to intentional data manipulation, false statements and misrepresentations. This misconduct, sometimes referred to as “greenwashing,” often takes the form of misleading or exaggerated sustainability benefits related to the company’s products and services or misstatements in the company’s filing or public statements related to ESG metrics and sustainability practices.

1. <https://www.sec.gov/news/press-release/2024-31>

2. <https://www.sec.gov/news/press-release/2023-234#:~:text=The%20SEC%20brought%20several%20enforcement,its%20controls%20concerning%20ESG%20products>



Examples of greenwashing include:

- Promoting products or services as being environmentally conscious when there is no or insufficient underlying data to substantiate such claims
- Knowingly promoting a product or service as being “green” or “ethically sourced” while withholding information that clearly demonstrates this not to be the case
- Misrepresenting the strength of an organization’s ESG commitment, such as setting carbon-neutral goals that are known to be unattainable
- Making materially misleading or false statements about the company’s controls or policies concerning ESG
- Applying different measurement inputs or methodologies to overstate results or progress toward ESG goals

Given the mounting pressures to meet ambitious ESG targets, coupled with developing reporting obligations, greenwashing presents a significant fraud risk that can easily go unchecked. As regulators increase their scrutiny, this is becoming a significant litigation and regulatory risk for global organizations. Leading-class companies are taking steps to manage this risk by: (1) implementing robust reporting processes and controls, enabled by technology and subjected to strong monitoring and testing; (2) incorporating the risks of greenwashing into the company’s existing compliance structure to prevent, detect and address misconduct; and (3) integrating greenwashing risks into their broader enterprise risk management activities.

▶ [How good governance can keep corporates clean from greenwashing](#)

Key takeaways to establish ESG compliance

- 1 Proactively set the role of compliance in ESG by determining where compliance can make the most significant impact within a company’s ESG regulatory profile, such as navigating regulatory requirements, mitigating critical risks and maintaining ethical conduct.
- 2 Monitor regulatory developments and align procedures to statutory obligations as part of a continuous ESG risk assessment.
- 3 Invest in technology-driven ESG reporting mechanisms and safeguards, with strong monitoring and verification processes.
- 4 Integrate sustainability disclosures into the company’s existing disclosure controls and procedures for financial and nonfinancial disclosures related to public reporting.
- 5 Incorporate the risks of greenwashing into the company’s existing compliance structure to prevent, detect and address misconduct.

Methodology

The EY Global Integrity Report 2024 is based on a survey of 5,464 board members, senior managers, managers and employees in a sample of large organizations and public bodies in 53 countries and territories across the Americas, Asia-Pacific and Europe, the Middle East, India and Africa. Interviews were conducted by the global research agency Ipsos through online panels between October 2023 to January 2024.

Job title

Board director or member	445	8%
Senior management	1,625	30%
Other management	2,134	39%
Other employee	1,260	23%

Employees

250-499 employees	10	>1%
500-999 employees	1,085	20%
1,000-4,999 employees	1,980	36%
5,000-9,999 employees	879	16%
10,000 employees +	1,510	28%

Industry summary

Advanced manufacturing and mobility	1,069	20%
Consumer products, retail and wholesale	954	17%
Energy and resources	300	5%
Financial services	794	15%
Government and public sector	530	10%
Health sciences and wellness	424	8%
Professional firms and services	241	4%
Real estate, hospitality and construction	667	12%
Technology, communications and entertainment	979	18%
Other	626	11%
Total	6,584	120%

Note: Respondents could choose more than one sector so the number does not add up to 100%.

Number of interviews in each region

North America		Western Europe	
Canada	100	Austria	100
United States	500	Belgium	80
Total	600	Denmark	50
South America		Finland	100
Argentina	90	France	100
Brazil	107	Germany	100
Chile	70	Great Britain	150
Colombia	90	Greece	100
Ecuador	100	Ireland	50
Mexico	100	Italy	100
Peru	45	Netherlands	100
Total	602	Norway	60
Oceania		Portugal	100
Australia	100	Spain	100
New Zealand	50	Sweden	100
Total	150	Switzerland	60
Far East Asia		Total	1,450
China	506	Middle East, India and Africa	
Hong Kong	80	India	100
Indonesia	100	Israel	50
Malaysia	100	Kenya	45
South Korea	100	Nigeria	60
Taiwan	50	Saudi Arabia	75
Thailand	100	South Africa	100
Vietnam	100	Turkey	50
Total	1,136	United Arab Emirates	100
Eastern Europe		Total	580
Bulgaria	50	Eastern Europe	
Czech Republic	100	Bulgaria	50
Hungary	100	Czech Republic	100
Poland	100	Hungary	100
Romania	100	Poland	100
Serbia	100	Romania	100
Slovakia	100	Serbia	100
Slovenia	96	Slovakia	100
Ukraine	100	Slovenia	96
Total	846	Ukraine	100
Japan		Total	100
Japan	100	Japan	
Total	100	Japan	100

For the purposes of the US edition of the EY Global Integrity Report 2024, we filtered responses for large corporations, which are defined as those entities that reported 10,000 or more employees globally. Unless otherwise noted, statistics referenced in this report relate to organizations with more than 10,000 employees.



Progressing compliance amidst disruption



Katie Kyle
Partner
Ernst & Young LLP
+1 732 516 4091
katie.kyle@ey.com



Kiley Smith Kelly
Principal
Ernst & Young LLP
+1 215 448 5943
kileysmith.kelly@ey.com

Improving confidence in reporting



Amanda Massucci
Principal
Ernst & Young LLP
+1 213 977 8380
amanda.massucci@ey.com



JD Minotti
Partner
Ernst & Young LLP
+1 312 879 3478
jd.minotti@ey.com

Digitizing compliance through AI



Jeremy Osinski
Principal
Ernst & Young LLP
+1 617 585 1855
jeremy.osinski@ey.com



Arpit Bothra
Managing Director
Ernst & Young LLP
+1 415 984 7068
arpit.bothra@ey.com

Establishing ESG compliance



Chandan Sarkar
Principal
Ernst & Young LLP
+1 201 872 2077
chandan.sarkar@ey.com



Katharina Wegmann
Partner
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
+1 212 773 3802
katharina.wegmann1@ey.com

Sector leaders

Consumer & Health



Kip Ebel
Principal
Ernst & Young LLP
+1 732 516 4331
kip.ebel@ey.com

Industrials & Energy



Allen Melton
Principal
Ernst & Young LLP
+1 214 969 8839
allen.melton@ey.com

Financial Services



Walid Raad
Partner
Ernst & Young LLP
+1 212 773 0956
walid.raad@ey.com

Private Equity



Chris Sercy
Principal
Ernst & Young LLP
+1 212 773 3916
chris.sercy@ey.com

Government & Public Sector



BJ Nichols
Principal
Ernst & Young LLP
+1 202 327 8719
bradley.nichols@ey.com

Technology, Media & Telecommunications



Miles Ripley
Principal
Ernst & Young LLP
+1 415 984 7332
miles.ripley@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY Forensic & Integrity Services

Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 5,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider a client's distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team. We strive to bring clients the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

© 2024 Ernst & Young LLP. All Rights Reserved.
US SCORE no. 24083-241US

2403-4482479 | ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/usforensics/2024integrityreport

