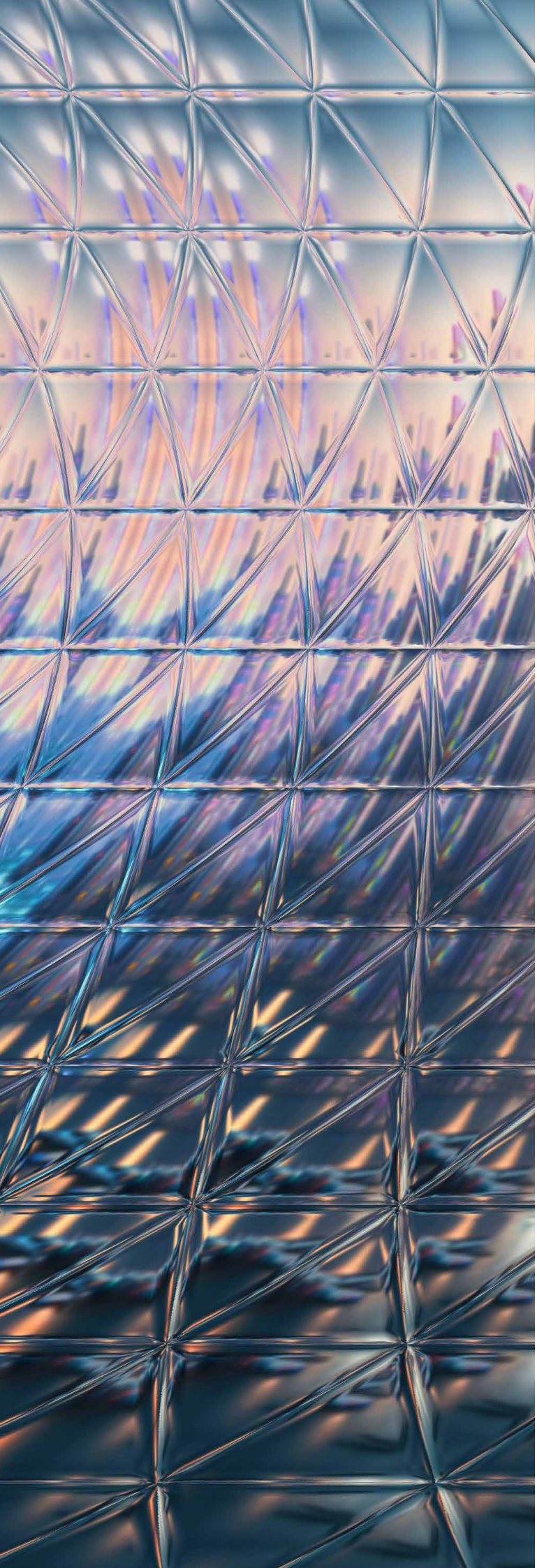
WHITE & CASE

2025 Global compliance risk benchmarking survey

Perspectives on AI, off-network messaging, incentivizing compliance and voluntary disclosure



Contents

Insights from the global compliance risk benchmarking survey 2025

In a world that moves at break-neck speed, corporate legal and compliance teams have never faced greater pressure to stay ahead of the game. The result is a function that is not just reactive to risk, but increasingly proactive in shaping corporate behavior and decision-making.

This year's Global Compliance Risk Benchmarking Survey offers a timely snapshot—based on insights from 265 senior compliance, legal and risk professionals worldwide—of how today's legal and compliance leaders are adapting to new technologies, regulatory expectations and cultural shifts in business conduct.

The themes explored in this year's survey reflect the changing nature of legal and compliance risk management. Artificial intelligence (AI) is becoming an operational reality within legal and compliance teams. Our findings show that while a growing number of organizations are deploying AI to drive efficiency and clarity in investigations and reporting, concerns about accuracy, governance and data privacy remain significant. As adoption increases, so does the need for guardrails to ensure that the use of AI enhances—rather than undermines—operational integrity.

We explore not only whether organizations are using AI, but also how long they have been doing so; the primary motivations driving adoption; the specific uses being prioritized; and the perceived advantages gained by users. Crucially, we also investigate the key concerns surrounding AI utilization; the prevalence of governance policies; the integration of AI risk into broader enterprise risk management (ERM) frameworks; and controls being implemented to ensure the trustworthiness and reliability of these tools.

Additionally, we examine the use of off-network messaging applications—tools that are convenient for employees, but often challenging for legal and compliance teams to monitor and access. The findings suggest that while many companies are implementing written policies, only a minority actively collect or audit off-network communications, raising questions about whether they do and, if so, how well these policies are being enforced and whether they are sufficiently comprehensive in scope, as well as emphasizing the importance of clear risk leadership and the right "tone from the top". Regulators are watching this space closely, and companies must consider whether their current approaches are sufficient in both spirit and substance.

The conversation around compliance incentivization shows promising signs of maturity. Many organizations are now integrating compliance metrics into compensation and performance frameworks. This finding suggests a shift from relying solely on punitive measures toward building a culture where ethical behavior is actively recognized and rewarded. Yet, the effectiveness of these programs depends not just on their existence, but on whether and, if so, how consistently they are implemented and whether they are aligned with broader business goals. The survey sheds light on the growing use of compliance-linked key performance indicators (KPIs) and how these are shaping both corporate culture and accountability.

In the final section, the report explores how companies are approaching voluntary self-disclosure to the United States Department of Justice (DOJ). While many companies now have formal processes to assess potential misconduct and to consider self-reporting, concerns about cost, reputational risk and the perceived benefits of disclosure continue to hold some organizations back. These concerns should be considered in the context of the global landscape. It remains to be seen, for example, the extent to which updated UK guidance on corporate self-reporting will factor into the equation for multinational organizations.

Together, these findings offer a nuanced view of how legal and compliance teams are navigating the demands of a digital, distributed and demanding business environment. From emerging technologies to traditional risk domains, the survey provides practical benchmarks and insights for organizations aiming to build resilient, forward-looking compliance programs.

We hope you find this year's report both informative and thought-provoking.

Key takeaways

Given the far-reaching nature of the survey and the findings within, as well as the changing nature of the compliance function, below are five takeaways that every legal and compliance leader should keep front of mind.

1

AI adoption is accelerating—and governance must keep pace

As more compliance teams deploy AI to streamline investigations and analyze risk, oversight frameworks need to evolve in parallel. Clear internal policies, strong ERM integration and proactive controls are essential to avoid over-reliance and ensure ethical, defensible use of these tools.

2

Managing off-network messaging is now a baseline expectation

Having a policy on off-network messaging is no longer a differentiator—it's a minimum requirement. Policy enforcement mechanisms, such as backup requirements and audit trails, are the next frontier, and organizations lagging here risk falling short of regulatory expectations.

3

Compliance incentives are working—but must go deeper

Tying compensation and recognition to compliance outcomes is gaining traction and positively shaping behavior. To be effective, however, these programs must apply across employee levels and extend to third parties. Selective or symbolic application risks undermining their impact.

4

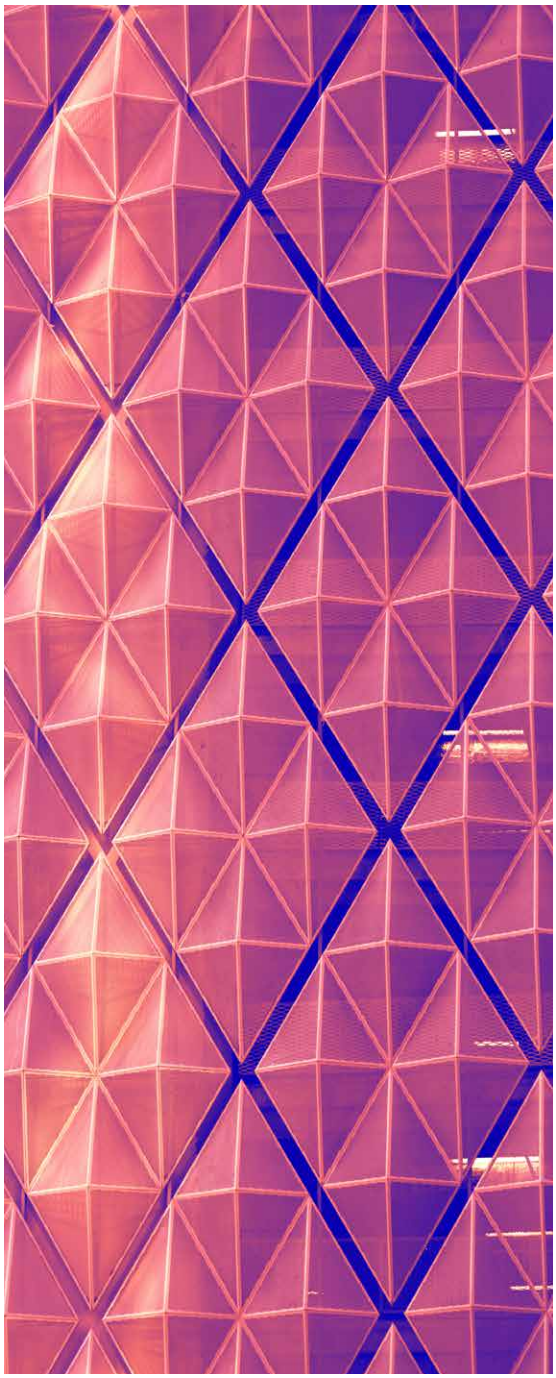
Voluntary disclosure is still a difficult choice; decision frameworks help

While concerns about cost, reputational harm and prolonged regulatory scrutiny persist, many organizations are still investigating and remediating misconduct—even when they opt not to self-disclose to the DOJ. The trade-offs are real: Voluntary self-disclosure may lead to reduced penalties and credit for cooperation, but it can also trigger intense external investigation, significant legal fees and public exposure. Building robust internal frameworks to assess these scenarios—and engaging regulators early where appropriate—can help organizations make more confident, consistent decisions.

5

Compliance is becoming a strategic function

As risks grow more complex and digitalized, the compliance function is evolving into a strategic advisor to the business. This shift not only requires more resources, but also a change of mindset—embedding compliance thinking into executive-level planning.



Artificial intelligence in the compliance function

KEY FINDINGS

■ AI adoption in compliance and investigations is gaining traction, especially among larger and publicly listed companies ■ Current usage patterns suggest that most respondents using AI are still in the early stages of their journey ■ Efficiency and cost savings are the primary motivators for AI implementation ■ Current use cases center on document summarization and review and assisting with risk assessments and regulatory updates, with more advanced uses still emerging ■ Respondents that are larger organizations report higher satisfaction with AI tools, likely because they have used AI for a longer period of time and have achieved better integration ■ Formal policies and risk controls around AI use are more common in high-revenue and public companies

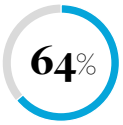
Corporate compliance is undergoing a seismic shift due to the transformative effect of digitalization and, in particular, AI. Once a futuristic concept, AI is rapidly becoming a mainstream, even business-critical, technology for legal and compliance functions globally. As organizations grapple with an increasingly complex regulatory environment, exponential data growth and relentless pressure to operate more efficiently and effectively, AI presents both unprecedented opportunities and novel challenges.

Our findings reveal a period of transition—one where early adopters are realizing tangible benefits, while also running up against growing pains such as implementation challenges, gaps in policy development and the inherent risks of deploying this transformative technology.

AI adoption trends

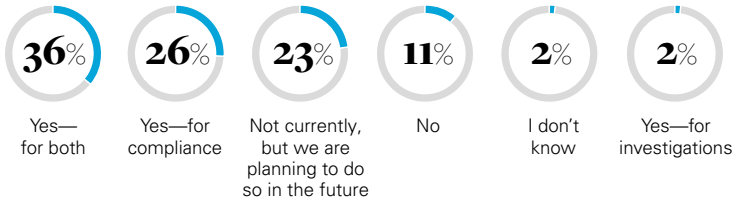
At the most fundamental level, AI is no longer a niche tool, but a technology gaining serious traction, albeit with adoption levels varying considerably across different organization types and sizes. Overall, 36 percent of respondents report using AI in both their compliance and investigations processes, with a further 26 percent using it for compliance tasks only.

This adoption is notably higher among certain segments.



Percentage of respondents using AI in their **compliance and/or investigations processes**

Does your organization utilize AI in its compliance and/or investigations processes?



Respondents that are publicly listed companies are almost twice as likely (44 percent) to use AI for both compliance and investigations compared with their private sector counterparts (23 percent). This disparity likely reflects the larger data volumes and potentially higher investment capacity often associated with public entities, and potentially the correspondingly greater expectations from regulators regarding use and deployment of data analytics in underlying compliance programs. Similarly, corporates show significantly higher adoption of AI (43 percent) compared with private equity firms (10 percent), suggesting differences in operational scale, risk appetite and/or the immediate perceived need for AI-driven compliance between these different types of businesses.

> **At the most fundamental level, AI is no longer a niche tool, but a technology gaining serious traction.**

Organizational size and revenue generation show a strong positive correlation with AI adoption. Nearly six out of every ten (59 percent) of the highest revenue-generating respondents already leverage AI for both compliance and investigations, a stark contrast to the 14 percent adoption rate among the lowest revenue-generating respondents. This finding highlights a resource gap, where larger organizations possess the financial means, technical expertise and the necessary data infrastructure to invest in and deploy AI more readily.

The tenure of AI usage reveals that while adoption is growing, it is still a relatively recent phenomenon for many organizations. Among respondents currently using AI, the largest cohort (36 percent) has been using it for one to two years, closely followed by those using it for a year or less (34 percent). A wave of adoption has occurred within the past two years, driven in part by pandemic-era digitalization trends, but even more so by the rapid mainstreaming of generative AI models and other scalable tools that have made the technology newly accessible and applicable to legal and compliance teams.

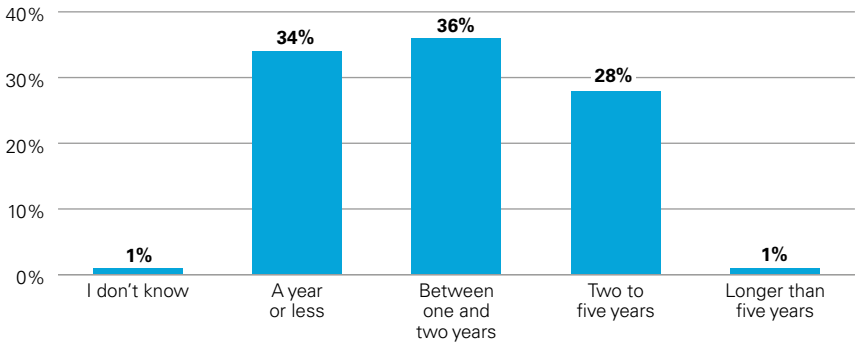
Again, respondents that are larger organizations demonstrate longer-term engagement with AI. Almost half (46 percent) of the highest revenue organization respondents have been using AI for two to five years, compared with just 11 percent of the lowest revenue organization respondents. As such, organizations that have used AI longer perceive the value of the technology as higher and have developed more sophisticated use cases.

Motivations driving AI adoption

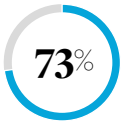
The rationale behind implementing AI for compliance and investigations is overwhelmingly pragmatic, focusing on efficiency and resource optimization. For respondents using these tools, the primary drivers are time savings (cited by 73 percent) and cost savings (71 percent). This finding underscores the increasing pressure on compliance functions to "do more with less"—managing escalating risks and data volumes without commensurate increases in headcount or budget. As one member of the ethics and compliance function of a US company said: "We use AI for compliance and investigations to lower the amount of manual work. Manual work has become time consuming due to the changing regulations and the complexity of the process. So, the use of AI became inevitable at a certain point."

AI is viewed as a critical tool to automate repetitive tasks, accelerate analysis and free up compliance professionals for higher-value strategic work.

How long has your organization been utilizing AI in its compliance and/or investigations processes?*



*Question only asked to the 168 respondents that previously stated their organization utilizes AI in its compliance and/or investigations processes



Percentage of respondents that cite **time savings** as a motivation for using AI

How AI is being applied

When examining the specific uses of AI among users in compliance and investigations, a clear focus emerges on the use of AI for tasks involving large-scale text analysis. The top use cases identified are summarizing documents (88 percent) and reviewing documents during investigations (85 percent). This aligns with the strengths of current Natural Language Processing (NLP) and Large Language Model (LLM) technologies, which excel at processing and extracting

What is your organization's motivation for using AI?* (Select all that apply)

Time savings	73%
Cost savings	71%
Allows compliance personnel to focus on other activities	64%
Regulator guidance	48%
Peer businesses are adopting AI for compliance	21%
I don't know	1%

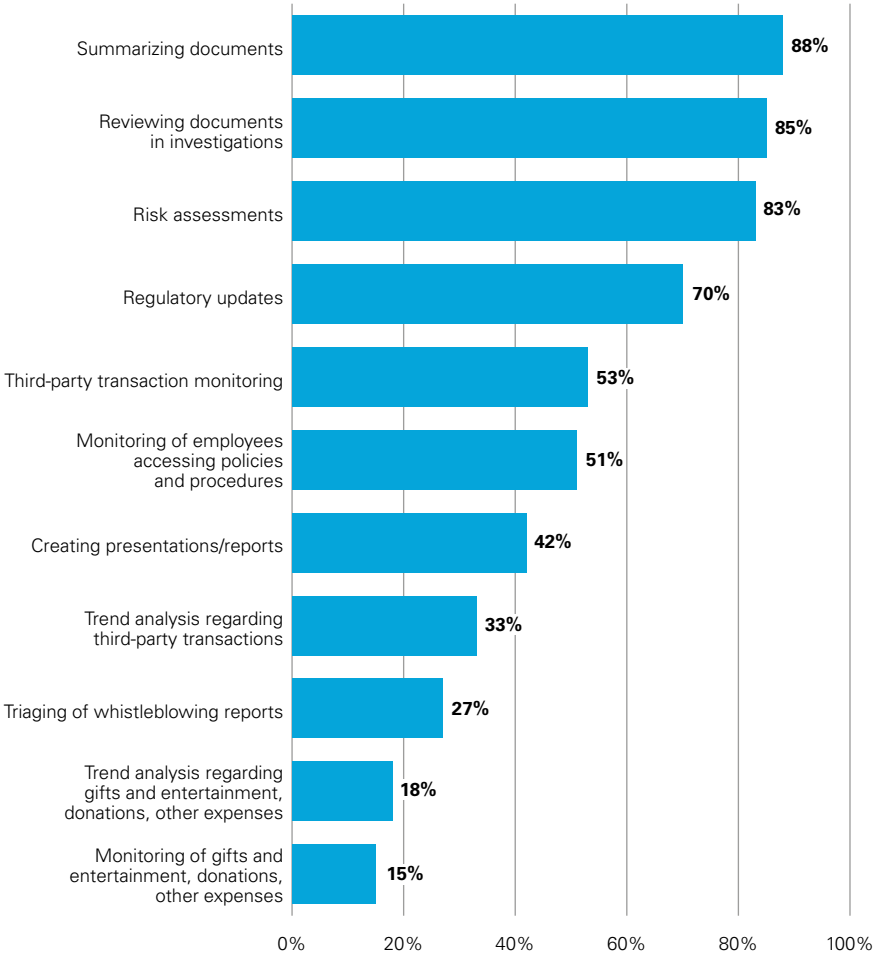
*Question only asked to the 168 respondents that previously stated their organization utilizes AI in its compliance and/or investigations processes

information from vast amounts of unstructured text data—a commonly shared challenge in compliance monitoring, due diligence and internal investigations.

In particular, the advent of generative AI marks a notable inflection point. Unlike earlier rule-based systems or machine learning algorithms designed for discrete tasks, generative models can summarize, compare, rephrase or even prepare first drafts of compliance documentation in a fraction of the time. This versatility, while powerful, also brings a new class of risks, including potentially opaque decision-making, unexpected outputs and uncertainty around the reliability of AI-generated content. Organizations are still grappling with where to draw the line between helpful automation and risky over-reliance and potential liability exposure.

While current uses of AI deliver on efficiency and cost savings, they represent a relatively narrow band of the technology's capabilities. More sophisticated applications, such as advanced anomaly detection in transactional data or intelligent training personalization, are less prevalent, based on the top responses, suggesting many organizations are still in the early stages of leveraging AI's full potential.

How is AI being used in your organization? (Select all that apply)*



*Question only asked to the 168 respondents that previously stated their organization utilizes AI in its compliance and/or investigations processes

Some organizations are already seeing benefits beyond basic review, however, as noted by a member of the legal function of a Mexico-based company: "We noticed how contextual information is captured and processed by utilizing AI, so we are using it for both compliance and investigations processes. There is a better understanding of everyday and uncommon risks in our activities."

User experience: High engagement and perceived value

Encouragingly, where AI is implemented, user engagement and satisfaction appear to be high. Among respondents in organizations using AI, almost all (96 percent) report personally using AI tools within their role. This level and use indicates that AI is not just running in the background, but is being integrated into the daily workflows of legal and compliance professionals.

Furthermore, the perceived utility is overwhelmingly positive. None of the respondents who personally use AI tools found them unhelpful. Instead, 48 percent rate them as "very helpful," while 43 percent find them "somewhat helpful." This strong endorsement suggests that once deployed, these tools are meeting user needs and delivering tangible benefits in their day-to-day tasks.

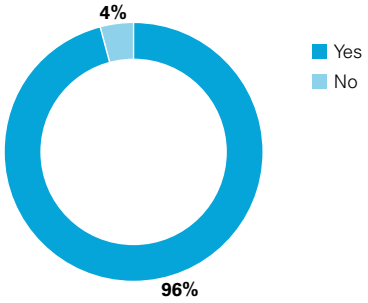
This perceived utility correlates strongly with organizational size and resources. Nearly three-quarters (73 percent) of users at the highest-revenue-generating respondents find AI tools "very helpful," compared with only 37 percent at the lowest-revenue-generating respondents. This disparity is likely attributed to the maturity of AI implementation in larger firms, better integration with existing systems, more comprehensive training, and/or access to more sophisticated, tailored tools, reinforcing the longer tenure findings.

AI challenges and concerns

Despite positive user experiences, significant concerns remain regarding the deployment of AI. The key concerns center on data security and reliability. Data protection emerges as the top concern (64 percent), reflecting

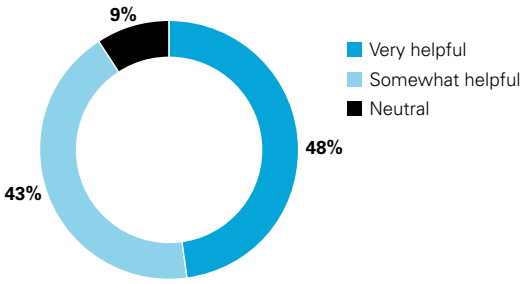
Among respondents in organizations using AI, almost all report **personally using AI tools** within their role

Do you personally use AI tools within your role?*



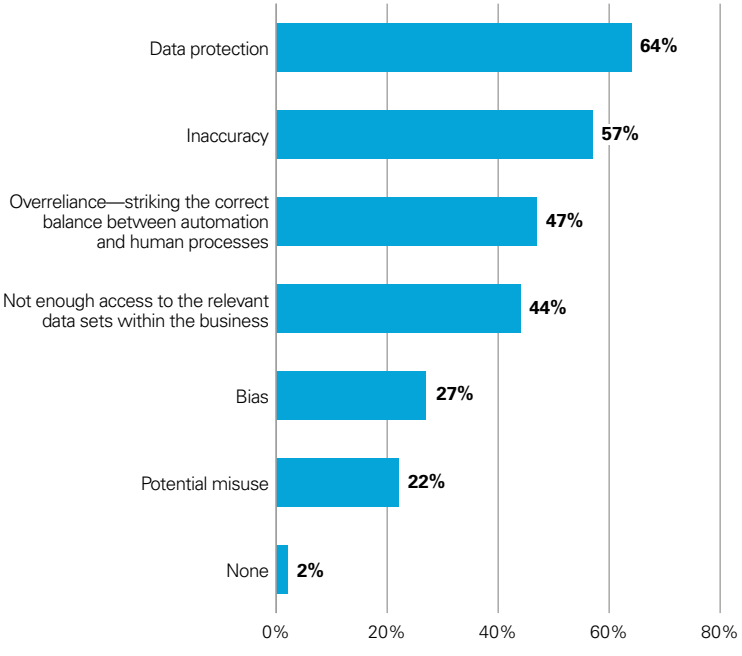
*Question only asked to the 168 respondents that previously stated their organization utilizes AI in its compliance and/or investigations processes

How helpful have AI tools been in your role?**



**Question only asked to the 162 respondents that previously stated they personally use AI within their role

What are your key concerns with the use of AI in compliance and investigations? (Select all that apply)



respondents' anxieties about handling sensitive personal or corporate data within AI systems, ensuring compliance with privacy regulations such as the European Union's General Data Protection Regulation (GDPR) and safeguarding against costly breaches. Inaccuracy (57 percent) is the second major concern, highlighting the risks associated with potential biases in algorithms, "hallucinations" in generative AI outputs, and the consequences of making legal and compliance decisions based on potentially flawed AI analysis.

Concerns about overreliance on AI are more pronounced in respondents that are publicly listed companies (55 percent) than in private organizations (35 percent). This finding may indicate a greater awareness in public companies of stricter governance expectations and a keener sense of the reputational and regulatory risks associated with inadequately supervised AI systems.

One often underestimated hurdle is cultural. Some legal and compliance teams remain skeptical of AI, fearing that automation could either dilute their influence or introduce errors for which they will be held responsible.

Others face institutional silos, where the data required for AI analysis is sequestered in legacy systems or resides in departments that do not coordinate effectively with legal and compliance teams. Without cross-functional alignment, even the most advanced AI models will struggle to reach their potential. Given this reality, it is perhaps not surprising that one of the questions that US DOJ prosecutors are encouraged to ask in the Evaluation of Corporate Compliance Programs (ECCP) guidance when assessing a company's compliance program is whether compliance teams have sufficient access to relevant data sources for timely testing and monitoring of a company's policies, controls and transactions.

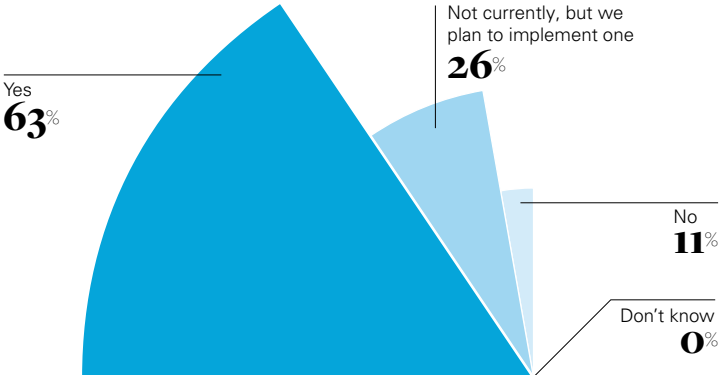
Policies and frameworks: Catching up to technology

As AI adoption grows, organizations are stepping up by developing governance frameworks, although progress varies. Almost two-thirds (63 percent) of respondents report having a policy governing employee use of AI. A significant gap remains, however, with 26 percent stating they do not currently have a policy but plan to implement one. Policy implementation shows disparities similar to adoption rates: 79 percent of the highest-revenue respondents have an AI use policy compared to only 34 percent of the lowest-revenue respondents. Likewise, publicly listed respondents (75 percent) and corporates (68 percent) are ahead of private companies (44 percent) and private equity firms (30 percent) in establishing these guidelines.

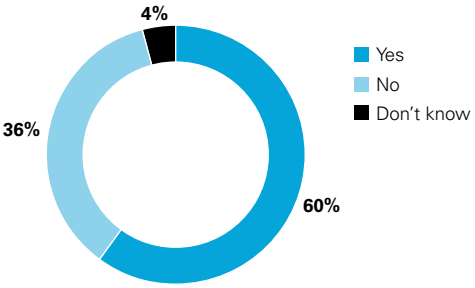
Beyond usage policies, integrating AI considerations into broader risk frameworks is crucial. Currently, 60 percent of respondents consider risks associated with the use of AI and other new technologies as part of their ERM process. AI is also proving to be valuable in navigating the complexities of the regulatory environment. "When there are regulatory updates, we need to make sure that we remain adaptive to these changes," explains a member of the ethics and compliance function of a US company. "AI has transformed the way we adapt to regulatory changes. Existing compliance procedures are altered without many issues. There is more confidence in our compliance management ability overall."

Integrating AI into ERM is again more prevalent among larger and public respondents compared with smaller and private

Does your organization have a policy governing employee use of AI?



Does your organization consider risks associated with use of AI and other new technologies as part of its enterprise risk management (ERM) process?



One often underestimated hurdle is cultural. Some legal and compliance teams remain skeptical of AI, fearing that automation could either dilute their influence or introduce errors for which they will be held responsible.

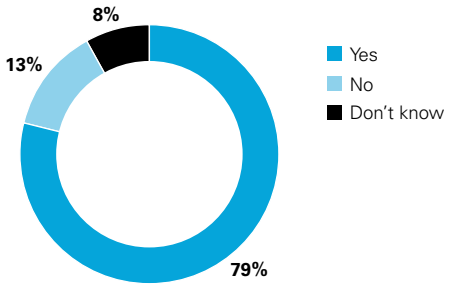
entities. For example, 71 percent of respondents that are public companies incorporate AI into ERM versus 44 percent of private companies, and 79 percent of the highest-revenue respondents do so compared with 30 percent of the lowest revenue ones.

Encouragingly, among the 60 percent of respondents that consider these risks in ERM, a strong majority (79 percent) state they have controls in place to monitor and ensure the trustworthiness and reliability of AI and its use in accordance with applicable law and company policy. This finding suggests that organizations formally addressing AI risks are also actively implementing mitigation measures.

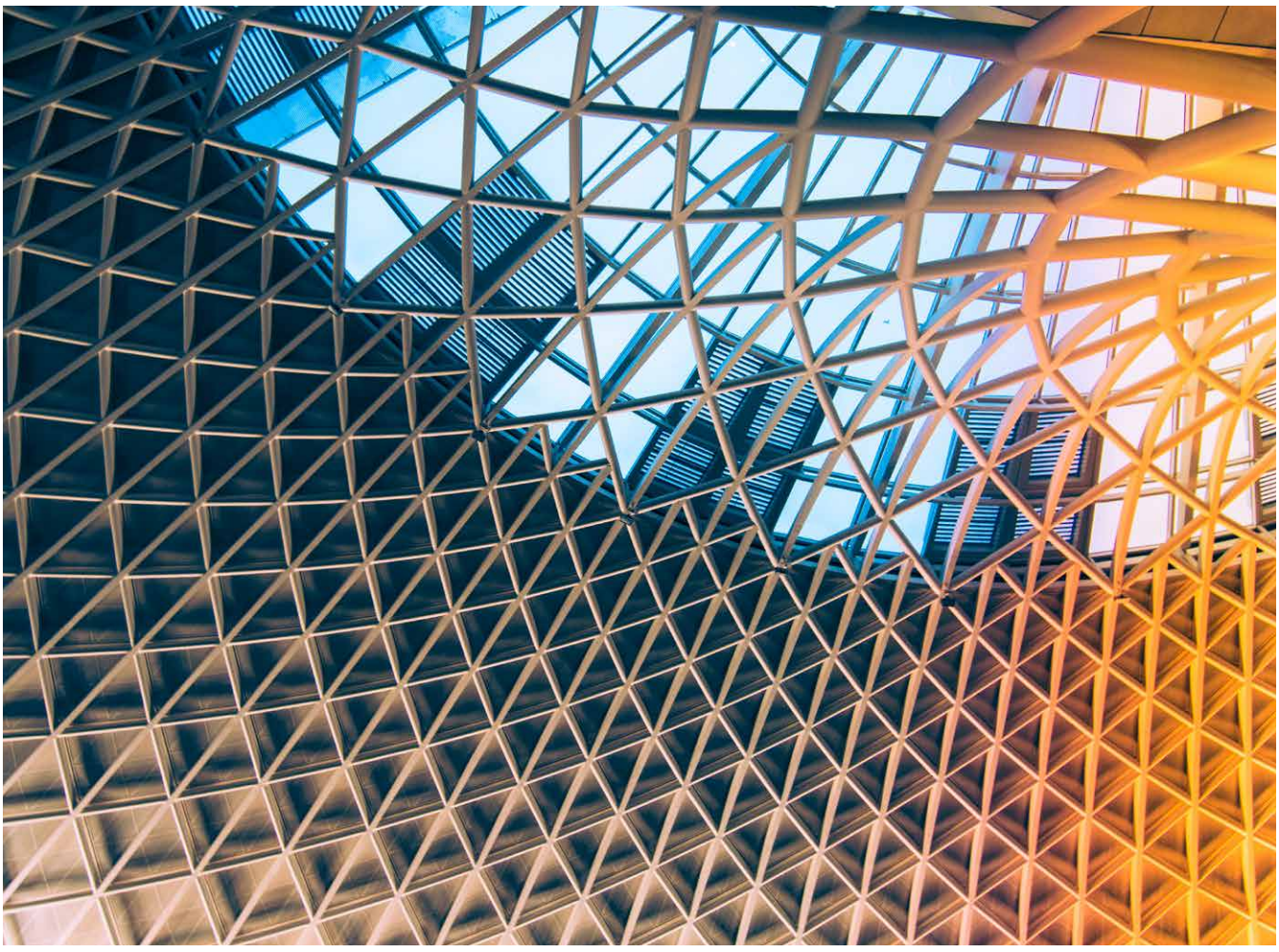
Looking ahead, several forces may accelerate AI integration in compliance. Regulatory bodies are starting to experiment with AI for enforcement and oversight, raising the stakes for regulated entities. At the same time, the emergence of AI-specific audit frameworks and ethical guidelines along with innovation programs run by governments and regulators may help hesitant organizations gain confidence. In the UK, the Financial Conduct Authority (FCA) publishes regular updates on the work it is doing to support the government's "pro-innovation strategy" on AI (this work has included co-authoring a discussion paper on how AI may affect regulatory objectives for the prudential and conduct supervision of financial institutions).

As tools evolve, we may also see a shift from task automation toward decision augmentation—where AI is not just doing the work but helping to shape how compliance professionals think about risk.

Does your organization have controls in place to monitor and ensure the trustworthiness and reliability of AI and its use in accordance with applicable law and company policy?*



*Question only asked to the 159 respondents that previously stated their organization considers risks associated with use of AI and other new technologies as part of its enterprise risk management (ERM) process



Off-network messaging and compliance

KEY FINDINGS

■ The use of off-network messaging apps for business communication is widespread, creating significant compliance and risk management hurdles ■ While many organizations have adopted formal rules around off-network messaging use, implementation often lags, with manual workarounds, unclear expectations and limited enforcement undermining effectiveness ■ Despite awareness of the risks, few organizations are equipped to reliably capture, monitor or retrieve business-related communications from personal or off-network platforms ■ Capturing and preserving communications from encrypted, third-party applications, especially on personal devices, presents significant technical, privacy and logistical difficulties ■ Features that cause messages to disappear automatically, i.e., ephemeral messaging, are fundamentally incompatible with recordkeeping duties and significantly increase compliance and legal risks, leading many organizations to ban their use entirely

The ubiquity of off-network messaging applications presents a major challenge for legal and compliance functions. While offering convenience and immediacy, these platforms operate largely outside traditional corporate IT infrastructure, creating substantial risks related to recordkeeping, regulatory supervision, data security, legal discovery and the potential for unmonitored misconduct. Regulatory and enforcement authorities globally, particularly those overseeing financial services, have intensified their scrutiny of off-network messaging use for business communications, highlighting the severe consequences of non-compliance.

The risks associated with unmonitored off-network communications are not theoretical, but have crystallized into significant financial and reputational consequences for numerous organizations. Since late 2021, US regulators, led by the United States Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), have launched sweeping enforcement initiatives targeting widespread failures by broker-dealers and investment advisors to preserve business-related communications conducted on personal devices and off-network messaging platforms. These enforcement actions have resulted in large penalties, exceeding US$2.5 billion in total fines levied against over 100 firms as of early 2025.

Individual penalties have often reached tens or even hundreds of millions of dollars. Investigations consistently revealed that employees, including senior managers and executives, routinely used text messages and apps for substantive business discussions, violating critical recordkeeping rules such as Rule 17a-4 of the Securities Exchange Act of 1934.

While self-reporting and cooperation have occasionally resulted in reduced penalties, the baseline fines remain substantial, underscoring the regulators' insistence on robust recordkeeping practices regardless of the communication channel used.

The UK's FCA has thus far adopted a less punitive approach, focusing on clarifying expectations under existing rules and issuing information requests to selected institutions rather than imposing SEC-scale fines. Nonetheless, a number of UK firms have taken their own actions against staff found to be using personal instant messaging systems.

It is clear that, globally, regulations are moving toward emphasizing heightened scrutiny of off-channel communications, putting pressure on firms everywhere to proactively address these gaps.

Individual penalties have often reached tens or even hundreds of millions of dollars.

Similarly, the US DOJ has made clear that prosecutors assessing corporate compliance programs should consider a company's policies and procedures governing the use of off-network messaging applications, which should be tailored to the company's business needs and ensure to the greatest extent possible that business communications are accessible and can be reviewed by the company. Recent DOJ enforcement actions also underscore the DOJ's expectations regarding companies' review and production of communications stored in off-network messaging applications; indeed, the companies that have maximized cooperation credit under the revised CEP reviewed and produced to the DOJ communications from off-network messaging applications.

Regulatory landscape and foundational device policies

Direct regulatory mandates governing the use of off-network messaging applications for all business types are not yet universal. Indeed, half of survey respondents indicate they do not work for organizations directly regulated by a governmental authority concerning off-network messaging usage specifically. This finding suggests that, while sectors such as finance face explicit rules, many other industries operate under broader recordkeeping guidelines or have regulations governing conduct that off-network messaging use might implicitly violate, rather than specific off-network messaging directives.

The foundation for controlling off-network messaging often starts with policies governing the devices that employees use. Formal "bring-your-own-device" (BYOD) policies are not consistently established, however, with 53 percent of respondents reporting they do not have such a policy. But there is a striking difference between business types: While only 34 percent of corporate respondents have a global BYOD policy, this figure jumps to 90 percent among private equity firms, likely reflecting divergent operational priorities, IT environments and workforce compositions.

Even without a formal BYOD policy, the question remains whether employees are permitted to use personal devices for work. More than half (54 percent) of respondents do not permit employees to use their personal devices for business purposes. This restriction is more common among larger organizations; a little over a quarter (26 percent) of the highest revenue-generating respondents allow personal device use for business, compared with 45 percent of the lowest revenue-generating respondents.

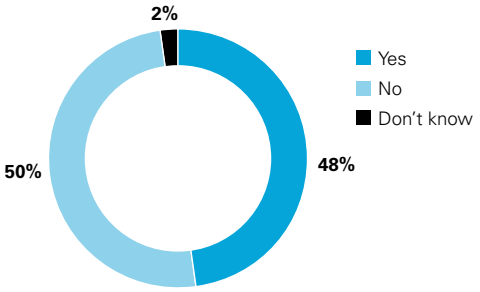
Again, a stark contrast exists between corporate respondents and private equity firm respondents, with only 35 percent of corporates allowing personal device use for business compared with 90 percent of private equity firms. This disparity suggests private equity firms operate with significantly different technology and communication norms compared with traditional corporate environments. Prohibiting personal device use entirely is one strategy to mitigate off-network messaging risks, as it theoretically keeps business communications contained within company-managed systems, although enforcing such prohibitions can be challenging and perhaps impractical.

Governing the use of off-network messaging applications

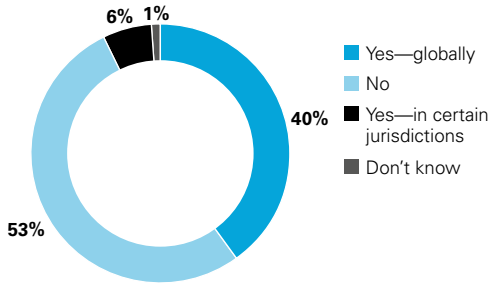
Recognizing the ubiquity of personal device usage with third-party communication apps installed, many organizations attempt to control off-network messaging use through specific policies, regardless of device ownership. A majority (63 percent) of respondents report having a written policy governing employee use of off-network messaging apps. Policy adoption is more prevalent among respondents facing greater public scrutiny or possessing more resources: 72 percent of publicly listed respondents have a policy compared with 50 percent of non-listed respondents and 79 percent of the highest-revenue-generating respondents have one versus 54 percent of the lowest.

Despite the prevalence of policies, the dominant approach by respondents is prohibition or significant restriction of off-network messaging use. A majority (58 percent) of respondents do not permit employees to use off-network messaging apps for business communications. Private company respondents are more likely to allow off-network messaging use for business globally (47 percent) compared with publicly listed company respondents (27 percent). Similarly, lower-revenue respondents

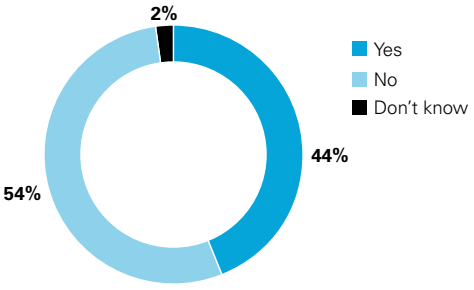
Is your organization regulated by a governmental authority regarding the use of off-network messaging applications?



Does your organization have a "bring-your-own-device" policy?



Does your organization permit employees to use their personal devices for business purposes?



Recognizing the ubiquity of personal device usage with third-party communication apps installed, many organizations attempt to control off-network messaging use through specific policies, regardless of device ownership.

are far more permissive (45 percent allow) than the highest-revenue respondents, where only 9 percent permit off-network messaging use for business communications globally. The corporate versus private equity split is also pronounced, with 70 percent of private equity firm respondents allowing off-network messaging use for business compared with only 36 percent of corporates. This pattern suggests that larger, public corporations facing greater regulatory pressure and possessing more established communication infrastructure tend to adopt a much more conservative position toward off-network messaging risks.

Managing permitted use: Limitations, back-ups and tech hurdles

For the respondents (39 percent) that do permit off-network messaging use for business communications, restrictions are common. Over half (51 percent) of respondents that allow usage limit it strictly to non-substantive scheduling or logistical communications as an attempt to keep official business records off these platforms while acknowledging their convenience for quick coordination.

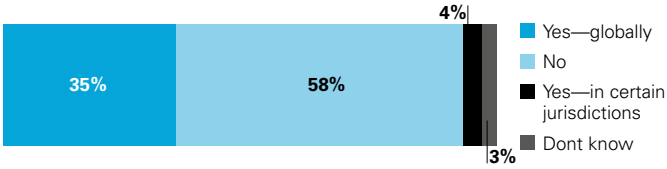
A critical challenge is record retention. Off-network messaging data typically resides outside corporate IT infrastructure, making preservation difficult. To address this reality, among respondents allowing off-network messaging usage, 72 percent require employees to actively back up or manually save any off-network business messages. This approach, however, relies heavily on employees to be diligent and may not meet regulatory and/or corporate expectations for completeness and reliability. Private equity firms appear to be more strict on off-network procedures, with 60 percent—compared with 28 percent of corporates—requiring employees to use an enterprise-wide off-network messaging application as well as backing up/manually saving any off-network messages.

Addressing the technical challenge of capturing off-network messaging data is also a major hurdle. While the

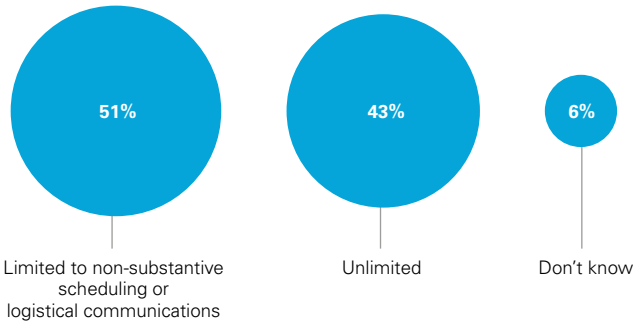
Percentage of respondents that **permit off-network messaging** use for business communications

Does your organization have a written policy governing employee use of off-network messaging applications?

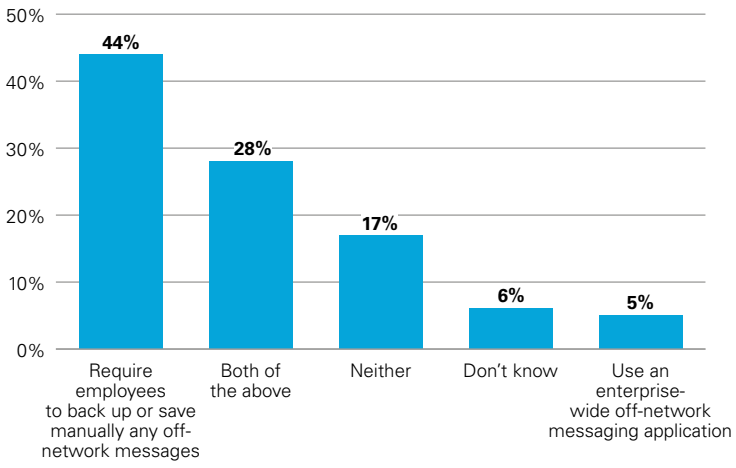
Does your organization permit employees to use off-network messaging applications for business communications?



How limited is the permitted use of off-network messaging applications?*



Which of these does your organization do with respect to off-network messages?*



*Question only asked to the 105 respondents that previously stated their organization permits employees to use off-network messaging applications for business communication either globally or in certain jurisdictions

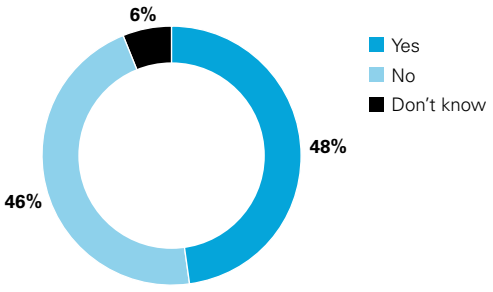
market offers potential solutions, none is without drawbacks. Some platforms provide enterprise versions with built-in archiving, but these solutions often do not cover popular external apps. Third-party archiving vendors offer specialized tools, but implementation can be complex and costly.

End-to-end encryption poses a significant barrier to access and preservation, often requiring capture on the device itself, which is difficult to achieve reliably, especially under BYOD scenarios, and requires employee cooperation that, depending on the circumstances, may not be forthcoming. Frequent app updates can break integrations, requiring constant maintenance. Employee privacy concerns are also paramount, particularly with personal devices. The manual alternative—requiring employee screenshots to track their activity—is fundamentally unreliable, lacks metadata, cannot be easily authenticated and fails to meet robust recordkeeping standards.

Ephemeral messaging dilemma

Ephemeral messaging features (causing messages to disappear after they are read) pose an even greater challenge. Recognizing this heightened risk, nearly half (48 percent) of all respondents expressly prohibit the use of ephemeral messaging applications for business purposes. This prohibition is significantly more common among organizations under greater regulatory scrutiny: 58 percent of publicly listed respondents ban ephemeral messaging compared with 33 percent of private organizations, and 67 percent of the highest-revenue-generating respondents impose a ban compared with 39 percent of the lowest. For financial firms, where communications can constitute trade instructions, client advice or other regulated activities, the inability to retain ephemeral messages creates unacceptable compliance gaps.

Does your organization expressly prohibit the use of ephemeral (disappearing) messaging applications?



End-to-end encryption poses a significant barrier to access and preservation.

Disappearing messages are generally incompatible with recordkeeping obligations and investigation needs. Furthermore, the intentional use of ephemeral messaging after a duty to preserve legal or regulatory information arises can lead to severe consequences, including allegations of obstruction or evidence tampering—risks that financial institutions and others are keen to avoid given the potential for substantial fines and reputational damage.

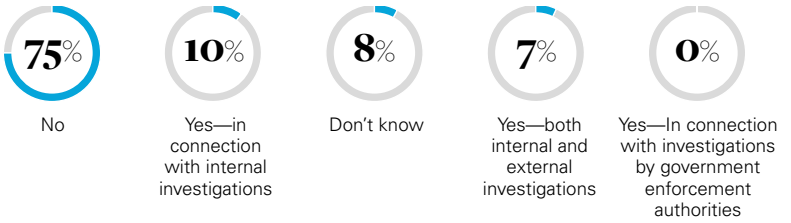
Investigations and data collection: A significant gap

The true test of off-network messaging controls often arises during internal investigations or inquiries by enforcement authorities. Three quarters of respondents report, however, that they did not collect any business communications from off-network messaging apps in connection with investigations over the past 12 months. This finding points to significant technical and practical hurdles, including privacy concerns and the need for employee cooperation. The disparity between high-revenue respondents (39 percent collected off-network messaging data) and low-revenue respondents (5 percent collected) suggests resources and regulatory impetus influence collection efforts.

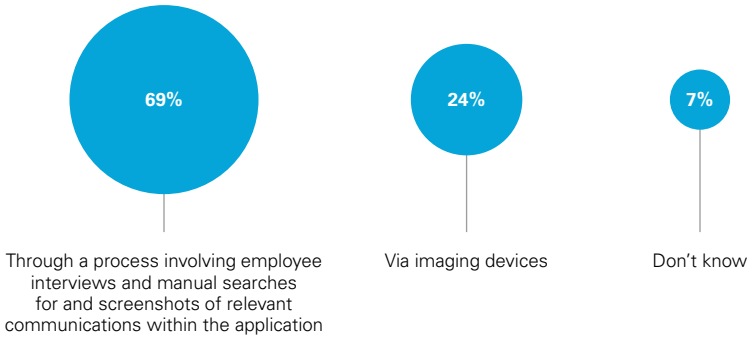
For 17 percent of respondents that did collect off-network messaging data, the methods employed highlight the lack of sophisticated strategies. The dominant approach, used by 69 percent of collectors, involved manual processes: employee interviews combined with manual searches and screenshots on the employee's device. This method is labor-intensive, prone to incompleteness, difficult to authenticate forensically and highly dependent on employee cooperation.

This inability to capture effectively and produce off-network messaging data carries significant legal risks beyond regulatory fines. In litigation, the failure to preserve relevant electronically stored information (ESI) may constitute spoliation, potentially leading to court sanctions, adverse inference instructions (telling a jury to assume missing evidence was harmful), or even dismissal of claims.

In the past twelve months, has your organization collected business communications from off-network messaging applications in connection with investigations?



How has your organization collected business communications from off-network messaging applications?*



*Question only asked to the 45 respondents that previously stated they collect business communications from off-network messaging applications

Collecting data forensically from personal devices is also far more complex than from corporate systems, potentially impacting admissibility. The inability to produce relevant communications from these off-channel sources can critically undermine an organization's legal defense or its ability to respond comprehensively to external inquiries.

Making policies stick

The widespread use of off-network messaging apps continues to present a major compliance challenge. While a majority of respondents have implemented written policies, the prevailing approach leans toward prohibition or severe restriction on off-network messaging use, especially in larger, public corporations. Ensuring adequate recordkeeping remains a challenge, often relying on imperfect manual employee backups, while ephemeral messaging is frequently banned outright.

Perhaps most critically, the gap between the reality of off-network messaging usage and the ability of most organizations to effectively monitor, retain and retrieve relevant business communications persists. This gap poses significant ongoing compliance risks. Addressing this challenge requires more than written policies. Effective implementation demands clear communication of expectations and consequences, regular tailored training, consistent enforcement applied at all levels (including senior management, whose conduct was frequently cited in enforcement actions) and providing viable approved communication alternatives.

Fostering a culture where employees understand the risks and prioritize approved channels for substantive business is a must. While technology solutions are evolving, they present challenges related to encryption, privacy and cost. Until these challenges are addressed, mitigating off-network messaging risk requires a multi-pronged approach that combines policy, training, technology where feasible and strong cultural reinforcement.

Incentivizing compliance and disincentivizing non-compliance

KEY FINDINGS

■ A strong majority of organizations have compensation clawback or withholding policies in place, but actual use is limited ■ The mere status of individuals being under investigation can influence compensation and recognition decisions, particularly in public and higher-revenue companies ■ Compliance-related incentives are widely used, with an overwhelming majority incorporating them into compensation structures ■ The most common incentives are KPIs and formal recognition programs, signaling that organizations increasingly view ethical conduct as part of performance management

The relationship between employee compensation, recognition, and an organization's culture of compliance is increasingly under scrutiny. Regulators, stakeholders and boards are recognizing that how employees are paid, rewarded and potentially penalized can significantly influence behavior.

Effectively integrating compliance considerations into compensation structures requires an integrated approach, encompassing mechanisms to penalize wrongdoing and strategies to proactively incentivize ethical behavior and adherence to compliance norms.

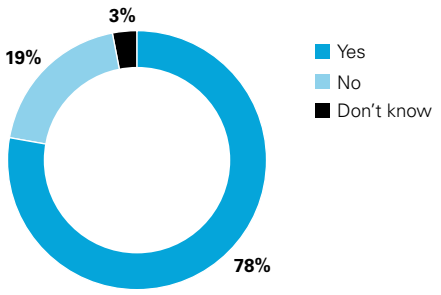
Withholding and recouping compensation

One of the most direct ways organizations can signal accountability for misconduct is through policies allowing for the withholding or recoupment of compensation from employees involved in wrongdoing, or those who fail to comply with their supervisory duties. These policies act as a deterrent and demonstrate a commitment to ensuring that individuals do not profit from unethical behavior or significant compliance failures occurring under their watch. Regulatory authorities, particularly in the financial services sector, have mandated these policies while other authorities have encouraged their use. For example, the ECCP underscores that "the design and implementation of compensation schemes play an important role in fostering a compliance culture." Prosecutors examining corporate compliance programs are therefore directed to assess the use of compensation structures, including clawbacks, to incentivize compliance and punish non-compliance. To incentivize companies to use clawback rights, in 2023 the DOJ adopted a Compensation Incentives and Clawbacks Pilot Program whereby companies can receive reductions in otherwise applicable fine amounts by compensation withheld from culpable individuals.

Our findings indicate widespread adoption of such policies. A significant majority (78 percent) of respondents report having a policy in place that allows them to withhold or "claw back" compensation from employees who engage in misconduct or who fail to adequately supervise others involved in misconduct. This high prevalence suggests that companies recognize the importance of having this mechanism available to them, likely driven by regulatory expectations and a desire to establish clear consequences for serious compliance breaches.

Adopting a policy is not, however, the same as enforcing it. Despite the prevalence of these policies, they appear not to be applied frequently. Among those respondents with clawback policies, a notable 55 percent stated they

Does your organization have a policy to withhold or recoup compensation from employees who engage in misconduct or who fail to supervise others who engage in misconduct?



Effectively integrating compliance considerations into compensation structures requires an integrated approach, encompassing mechanisms to penalize wrongdoing and strategies to proactively incentivize ethical behavior and adherence to compliance norms.

had not actually withheld or sought to recoup compensation within the past 24 months from employees meeting the criteria. This finding indicates a potential gap between policy intent and practical execution.

Several factors might contribute to this state of affairs, including the legal challenges in enforcing clawbacks (which can vary significantly by jurisdiction and depend on employment contract specifics), potential negative impacts on employee morale, difficulty in definitively assigning responsibility, or a lack of sufficiently severe incidents triggering the policy during the period. Consistency of application of such policies therefore requires close attention, particularly when it comes to holding senior executives and potentially third parties to the same standard as employees.

Even when clawbacks are used, they are not always triggered by external scrutiny. Of those (40 percent) that do have a clawback policy, 32 percent utilized them in the past 24 months based on internal findings, independent of any investigation initiated by enforcement authorities.

While this finding demonstrates internal accountability, the relatively low overall usage rate raises questions about whether these policies are serving as the potent deterrent regulators envision, or if implementation challenges are limiting their effectiveness in practice.

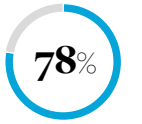
The shadow of investigation: Impact on compensation and recognition

Clawbacks aside, simply being under an internal investigation can also cast a shadow over an employee's or even a third party's standing within an organization, potentially impacting decisions related to compensation, bonuses, promotions or other forms of recognition. Organizations must navigate a delicate balance: protecting the integrity of their compensation systems and avoiding rewarding individuals possibly involved in wrongdoing, while also respecting due process and avoiding premature judgment before an investigation concludes.

Current practices show a divided approach. Overall, 42 percent of respondents consider both an employee's and a third party's status as the subject of an internal investigation when making decisions regarding compensation and other forms of recognition such as awards. This finding indicates that a significant portion of companies are proactively factoring investigation status into these decisions for both internal and external stakeholders. A slightly smaller, but still substantial, number of respondents (31 percent), however, limits this consideration to employees only, suggesting less willingness or less of a perceived need to apply the same scrutiny to third parties.

This consideration is not applied uniformly across all types of respondent organizations. Publicly listed respondents, often subject to greater external scrutiny and shareholders' governance expectations, are significantly more likely to factor investigation status into compensation decisions. Over half (51 percent) of public company respondents consider investigation status in making compensation decisions for both employees and third parties, compared with only 29 percent of private company respondents. It seems that due to public accountability pressures, public companies are apt to take a more cautious approach to rewarding individuals or entities potentially implicated in ongoing investigations.

Similarly, organizational size and resources, reflected by revenue, play a significant role in a company's decision to consider investigation status in making compensation decisions. Nearly two-thirds (64 percent) of the highest revenue-generating respondents take investigation status into account for compensation and recognition decisions concerning employees and third parties, which contrasts sharply with lower revenue respondents, where only 27 percent do so. Larger organizations may have more sophisticated internal investigation processes, dedicated resources to track investigation statuses, and potentially more formalized connections between human

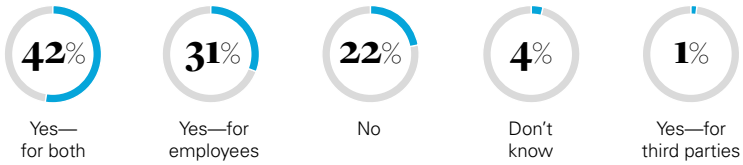


of respondents report having a **"claw back"** policy in place

In the past 24 months, has your organization withheld or sought to recoup compensation from employees who engage in misconduct or who fail to supervise others who engage in misconduct?*

*Question only asked to the 206 respondents that previously stated their organization has a policy to withhold or recoup compensation from employees who engage in misconduct or who fail to supervise others who engage in misconduct

Does your organization consider an employee's or third party's status as the subject of an internal investigation in making decisions regarding compensation and/or other recognition (e.g., awards)?



resources, compliance and legal functions to ensure this information is considered appropriately during compensation cycles.

Incentivizing compliance: Rewarding the right behaviors

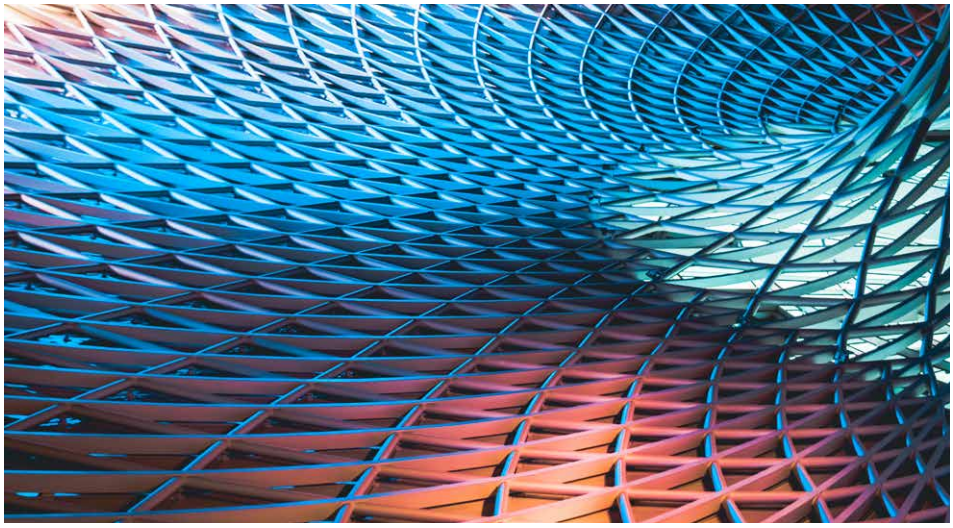
While penalties and clawbacks address negative behavior, a comprehensive approach also involves proactively encouraging and rewarding positive compliance conduct. Using the compensation structures to incentivize compliance signals that ethical behavior and commitment to the organization's compliance program are valued and contribute to success. An overwhelming majority of respondents recognize this connection, with 83 percent reporting that they use their compensation structure in some way to incentivize compliance.

The most common methods of implementing this incentive approach involve targeted performance indicators and formal recognition programs. Among the respondents who use their compensation structure to incentivize compliance, the vast majority (89 percent) incorporate compliance-related KPIs for designated employees. These individuals might include compliance officers, internal auditors, managers in high-risk functions, or designated "Compliance Champions" embedded within business units.

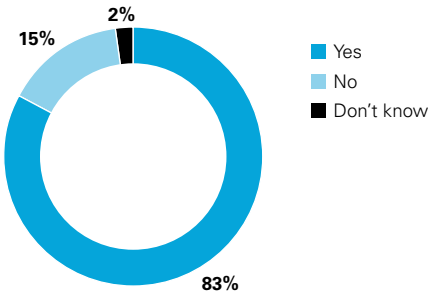
Tying specific, measurable compliance objectives to performance evaluations and, consequently, compensation helps ensure that compliance responsibilities are taken seriously and prioritized alongside business objectives. As one member of the compliance and ethics function of a US corporate notes: "Compliance-related KPIs are present for designated employees who are responsible for managing compliance and audit activities. Recently, we decided to offer awards for compliance-related achievements, and it's driven positive results for us."

Beyond direct KPIs, formal recognition is equally important. Nearly four in five (79 percent) of respondents using compensation to incentivize compliance use employee recognition or award programs specifically for compliance-related achievements. These awards can highlight individuals or teams who demonstrate exemplary ethical leadership, implement innovative compliance approaches, champion a culture where people are empowered to raise concerns, and report wrongdoing, or successfully embed compliance practices into business operations. Such recognition not only rewards individuals but also serves to promote positive role models and reinforce desired behaviors across the organization.

The overall sentiment is that integrating compliance into the compensation and reward framework adds tangible value. "All these measures are included in the compensation structure. It does add value to compliance management. It influences our employees positively, and they know that complying with the rules and regulations is an added advantage for them," says one member of the compliance and ethics function at a US company.



Does your organization use its compensation structure to incentivize compliance?



How does your organization use its compensation structure to incentivize compliance?* (Select all that apply)

89%
Compliance-related KPIs for designated employees (e.g., "Compliance Champions")

79%
Employee recognition/awards for compliance-related achievement(s)

76%
Compliance-related KPIs for executives (e.g., percent completion of compliance training in relevant department or business unit, clean/green internal audit results, satisfactory results on culture surveys)

*Question only asked to the 220 respondents who previously stated their organization uses its compensation structure to incentivize compliance

Voluntary self-disclosure

KEY FINDINGS

■ Most companies now have formal processes in place to assess potential misconduct for DOJ disclosure, highlighting a shift toward more structured and intentional compliance protocols ■ Almost half of the organizations have considered self-disclosure under the DOJ's 2023 revised CEP, showing significant engagement with the updated incentives. It remains to be seen whether the DOJ's 2025 revisions to the CEP, which postdated the data-gathering for this survey, will reinforce this trend ■ Public companies and those with higher revenues are more likely to consider self-disclosure, suggesting that resource availability and external scrutiny play a major role ■ Internal remediation remains a top priority even when companies opt not to disclose, with larger organizations showing a greater tendency to investigate and correct issues ■ Concerns around costs, duration and reputational risk continue to deter many from self-disclosing, despite DOJ incentives and potential leniency. These concerns are likely to remain despite the most recent policy changes to encourage voluntary disclosure

Whether to voluntarily self-disclose potential corporate misconduct to the DOJ presents one of the most challenging and complex decisions a company facing compliance issues can encounter. Multinational organizations will also need to consider self-disclosure regimes in other jurisdictions, notably the UK.

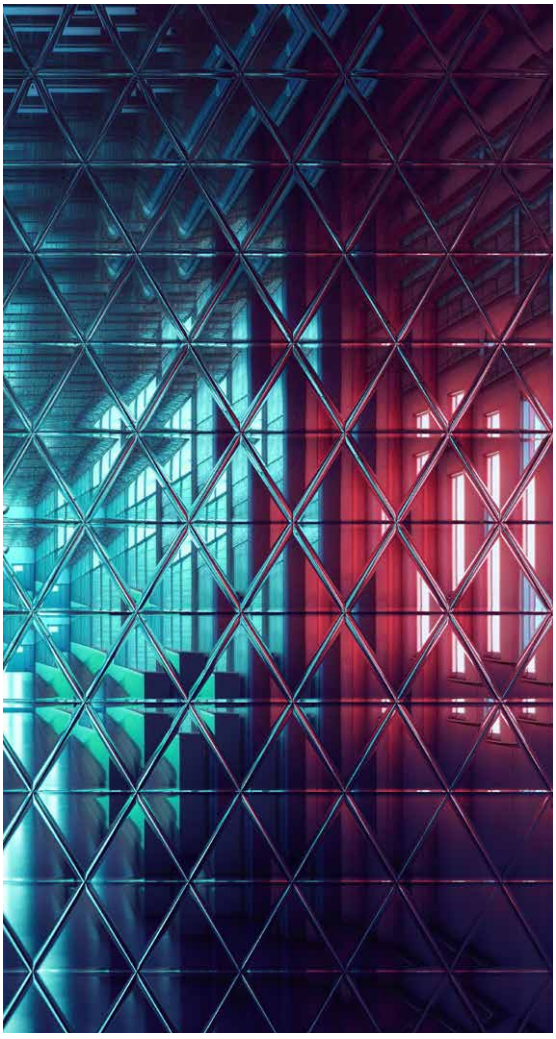
Voluntary self-disclosure offers a potential pathway to leniency, including possible declinations or significantly reduced penalties, under the CEP. The January 2023 revisions to the CEP sought to further incentivize prompt and comprehensive disclosure, cooperation and remediation, and underscore the DOJ's emphasis on corporate accountability and proactive compliance. More recent revisions announced in May 2025 are designed to provide even greater certainty and transparency to companies that voluntarily self-disclose, fully cooperate and timely and appropriately remediate. Most notably, the latest revisions to the CEP provide that companies meeting these criteria are entitled to a declination of prosecution—absent aggravating circumstances underlying the misconduct—whereas the previous version of the CEP provided that such companies were entitled to a presumption of a declination.

The 2025 revisions to the CEP also create a new category for "near miss" voluntary self-disclosures, where a company self-reports in good faith but falls short of full voluntary self-disclosure criteria, among other scenarios. In such "near miss" voluntary self-disclosures, the form of resolution is a non-prosecution agreement (absent particularly egregious conduct or multiple aggravating factors) with a term of less than three years, a reduction of 75 percent off of the low end of the applicable fine range and no independent compliance monitor.

The path of self-disclosure, however, is fraught with perceived risks and uncertainties, demanding a careful calculus of potential benefits versus substantial costs that often lead companies to refrain from stepping forward.

Formalizing the disclosure assessment process

Given the high stakes involved, a structured approach to identifying and evaluating potential misconduct for self-disclosure is highly desirable. Recognizing a potential issue is only the first step; determining its severity, scope and implications under DOJ policy requires a robust internal process involving legal and compliance personnel and usually external counsel.



Encouragingly, a majority of organizations appear equipped, at least procedurally, for this task. Our findings show that 69 percent of respondents have established a formal process specifically designed to identify and assess compliance escalations involving potential corporate misconduct for the express purpose of evaluating potential voluntary self-disclosure to the DOJ.

This finding suggests that most organizations understand the need for a systematic framework to handle these critical decisions, ensuring that potential disclosures are considered deliberately and consistently, rather than on an ad-hoc basis. The existence of such processes allows for timely internal investigations, thorough analysis of the facts against the DOJ's criteria and informed recommendations to senior management and the board.

Engagement with the 2023 revised DOJ policy

The DOJ's revisions to its CEP in January 2023 aimed to provide greater transparency and stronger incentives for companies to come forward promptly upon discovering misconduct. These changes clarified the benefits available for companies meeting specific standards of disclosure, cooperation and remediation, even where aggravating circumstances exist. As noted above, the CEP was further revised in May 2025 following the completion of this survey.

Since the 2023 CEP revisions, nearly half (49 percent) of surveyed organizations have actively considered voluntarily self-disclosing potential corporate misconduct to the DOJ. This indicates a significant level of engagement with this topic, perhaps motivated by the DOJ's efforts at greater certainty and transparency in this context.

Publicly listed companies, which generally face heightened regulatory oversight and shareholder expectations, have been more inclined to consider voluntary self-disclosure. A 57 percent majority of public company respondents considered self-disclosure under the revised policy, compared with only 37 percent of private company respondents. Similarly, scale is important, with 56 percent of the highest-revenue-generating respondents having contemplated self-disclosure, compared with just 33 percent of the lowest-revenue-generating respondents.

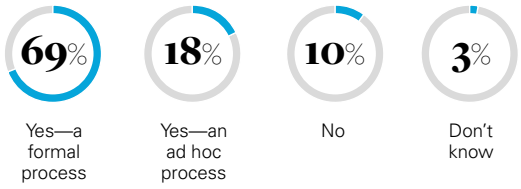
This disparity likely reflects factors similar to those seen in the adoption of AI and other compliance practices: larger, public companies may have more sophisticated monitoring systems that detect potential issues sooner; greater resources dedicated to legal and compliance functions enabling thorough evaluation against DOJ policy; and perhaps a greater sensitivity to the potential reputational and financial consequences of not disclosing if the misconduct were later discovered by authorities.

Internal remediation: A priority regardless of disclosure

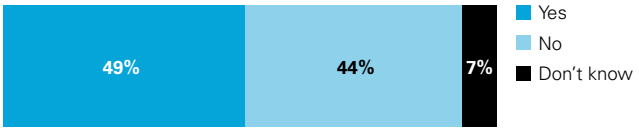
Crucially, the decision not to self-disclose does not necessarily mean inaction. Effective compliance programs emphasize not only detection but also thorough investigation and remediation of identified issues, regardless of external reporting decisions. Among organizations that considered voluntary self-disclosure but decided not to disclose, nearly half (48 percent) nonetheless proceeded to conduct an internal investigation

Percentage of public company respondents who **considered self-disclosure under the revised policy**, compared with only 37 percent of private company respondents

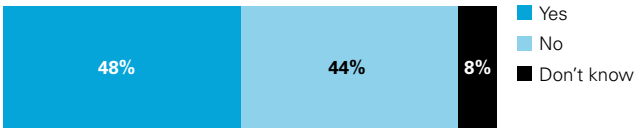
Does your organization have a process to identify and assess compliance escalations involving potential corporate misconduct for potential voluntary self-disclosure to the U.S. Department of Justice ("DOJ")?



Has your organization considered voluntarily self-disclosing potential corporate misconduct to the Department of Justice (DOJ) since the DOJ revised its Corporate Enforcement and Voluntary Self Disclosure Policy in January 2023?



If you considered voluntary self-disclosure but decided not to disclose, did your organization nonetheless investigate and appropriately remediate any misconduct?*



*Question only asked to the 129 respondents that stated their organization considered voluntarily self-disclosing potential corporate misconduct to the Department of Justice (DOJ)

and appropriately remediate any confirmed misconduct. This outcome underscores a commitment within many organizations to address compliance failures internally, fixing processes, implementing stronger controls, and potentially disciplining employees, even when choosing not to involve the DOJ.

Once again, larger organizations demonstrate a stronger tendency toward internal resolutions. A substantial 80 percent of the highest revenue-generating organizations investigated and remediated misconduct even when not disclosing, compared with only 32 percent of the lowest revenue-generating companies. This gap may reflect differences in internal investigation capabilities, resources dedicated to remediation efforts, or potentially a higher baseline level of compliance program maturity in larger firms.

Barriers to disclosure: Cost, duration, and uncertainty

Despite the DOJ's incentives, there remain hurdles to self-disclosure that dissuade companies from coming forward.

The most cited barrier is a pragmatic concern that the potential costs would ultimately outweigh the potential benefits (49 percent). This cost-benefit analysis is complex. While self-disclosure might lead to reduced fines, the costs of conducting the necessary rigorous internal investigation to the DOJ's expectations and of cooperating fully, which can involve extensive document production and employee interviews and, in extreme cases, paying for an independent compliance monitor, can be substantial. In assessing whether to self-report, companies typically also consider the likelihood of the government discovering the misconduct absent a self-report, and the potential benefits that can be obtained from cooperation and remediation alone should the government later come knocking. As one member of the legal function of a US private equity firm says, "Our concern has always been about the potential costs of voluntary self-disclosure. There should be a balance between the costs and the potential benefits. If the company is eventually at a loss due to this voluntary disclosure, it does not justify the step."

Closely related is the concern about the resulting duration and cost of the ensuing DOJ investigation itself (47 percent of those that do not voluntarily disclose). Initiating a voluntary self-disclosure invites government scrutiny, and companies worry about protracted, resource-intensive investigations that can disrupt business operations, consume significant management time and incur substantial legal fees, even if the ultimate penalty is reduced. The lack of certainty around timelines is a key deterrent. "Concern about the resulting duration of a DOJ investigation was the most troubling," says the general counsel of a Japanese company. "We cannot predict these timelines. It may involve a lot of negative publicity as well. I'm not sure that a voluntary disclosure was in the best interest of the business at the time." Further, a member of the compliance and ethics function of a US company echoed this sentiment, saying: "A full-fledged DOJ investigation was not something we were prepared for. Apart from the uncertain time and cost of the DOJ investigation, we were also concerned with the possible effects on the reputation of the company. There were a few positives to back the decision about going in for a voluntary self-disclosure."

The fear of a lengthy, costly and potentially reputation-damaging process, even when initiated voluntarily, clearly weighs heavily on the decision-making process. The emphasis on promoting efficiency in DOJ investigations in the most recent Department policy announcements are alone unlikely to assuage these concerns.

Adding to the complexity for multinational organizations are the disclosure regimes found in other jurisdictions. In the UK, the Serious Fraud Office (SFO) has recently updated its guidance with the aim of incentivizing corporate self-reporting by offering a clearer and quicker pathway to a deferred prosecution agreement for those who come forward voluntarily. It remains to be seen to what extent this new guidance will affect decision-making within multinational organizations.

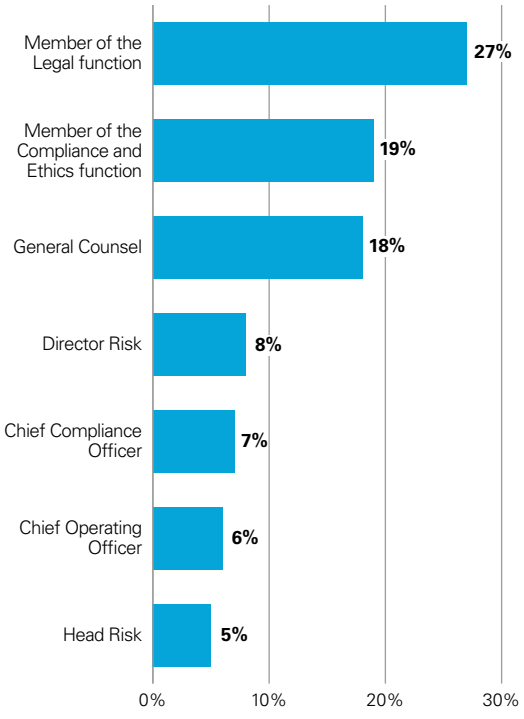
Why did your organization decide not to voluntarily self-disclose? (Select all that apply)

Survey methodology and demographics

Methodology

The survey was conducted in two tranches: Phone interviews were conducted by Mergermarket with a complementary online survey by White & Case LLP, totaling 265 responses.

What is your role within your organization?*

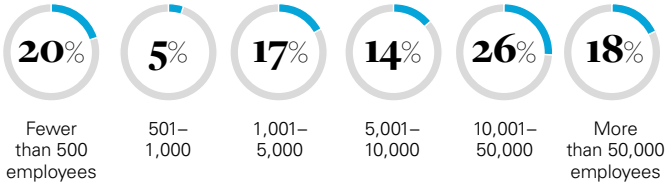


*Top seven responses shown only

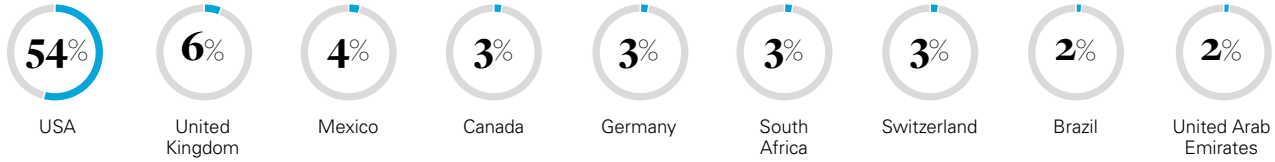
Key findings

- 26 percent of companies surveyed employ between 10,001 and 50,000 employees. 20 percent employ fewer than 500 employees
- 27 percent of respondents are members of the legal function. 19 percent are members of the compliance and ethics function
- 54 percent of respondents work for organizations headquartered in the US. 60 percent of respondents interviewed over the phone were headquartered in the US compared with 35 percent of online respondents
- 60 percent of the organizations surveyed are publicly listed
- 92 percent of respondents are not listed in multiple countries
- Sectors are relatively evenly split. Top three: 12 percent of the businesses surveyed operate primarily in technology, 12 percent in financial institutions and 11 percent in manufacturing
- 29 percent of the businesses surveyed have an annual revenue of US$1.1 billion to US$10 billion
- 98 percent have a compliance and ethics function or the equivalent
- Excluding internal audit, 35 percent of organizations have between 21-50 people within the compliance and ethics function. 33 percent employ between 11-20 people

Approximately how many people are employed by your organization?



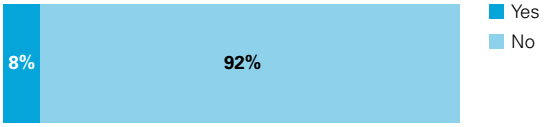
Where is your organization's corporate headquarters located?*



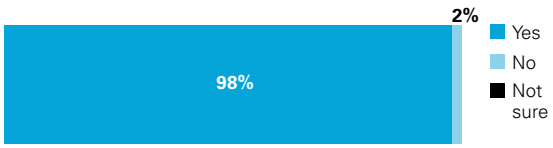
*Top nine responses shown only

Is your organization publicly listed?

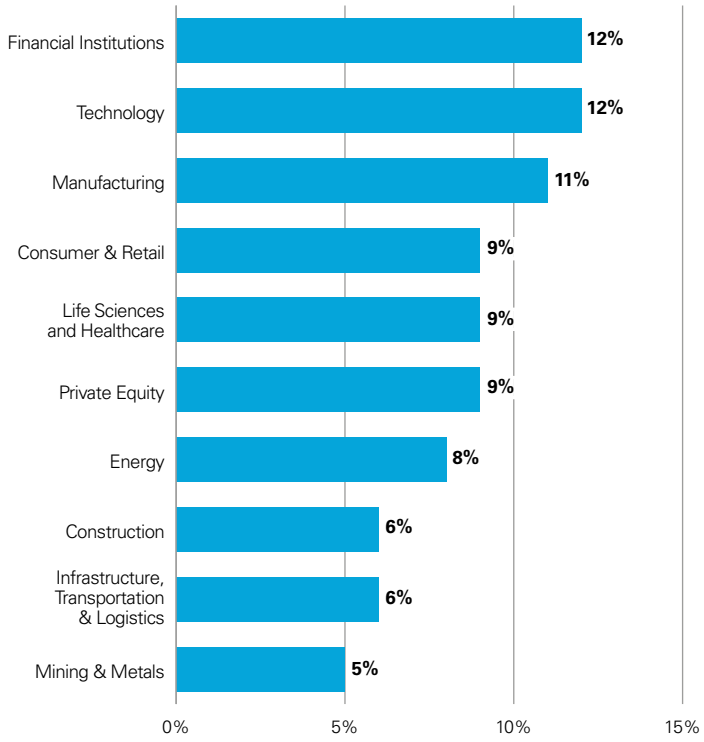
Is your organization listed in multiple countries?



Does your organization have a Compliance and Ethics function or equivalent?

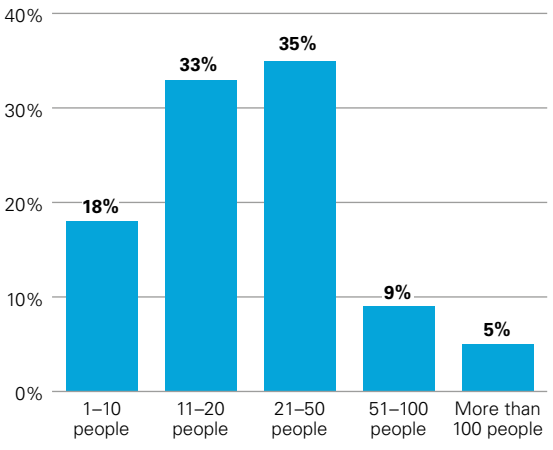


In what industry sector does your business primarily operate?**

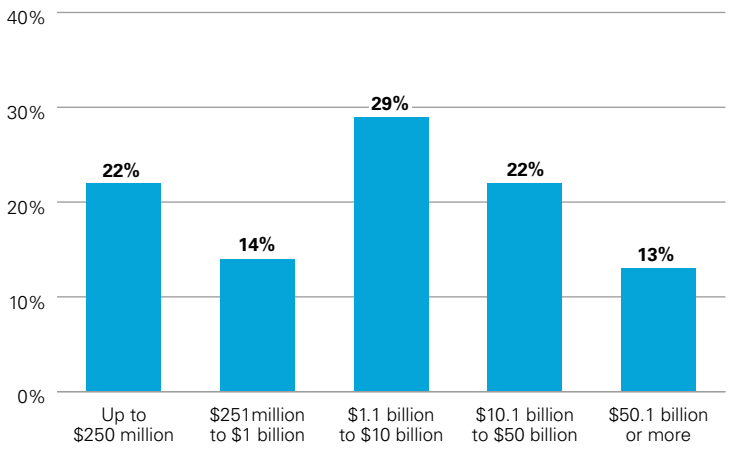


**Top ten responses shown only

Excluding internal audit, how many people in your company are responsible for carrying out the Compliance and Ethics function?



What is your organization's approximate annual revenue in U.S. dollars?



WHITE & CASE

whitecase.com

Darryl Lew
Partner, White & Case LLP
T +1 202 626 3674
E dlew@whitecase.com

Courtney Hague Andrews
Partner, White & Case LLP
T +1 213 620 7721
E courtney.andrews@whitecase.com

Anneka Randhawa
Partner, White & Case LLP
T +44 20 7532 1521
E anneka.randhawa@whitecase.com