NAVEX®

Navigator Series

Top 10 Trends in Risk and Compliance

2026

Contents

3 Executive summary

5 How AI will impact Compliance teams' work and staffing
BY MATT KELLY

8 Supply chain integrity in 2026: what does this mean?
BY PIERRE BERLIOZ

12 Compliance trends for Europe – what do you need to watch?
BY YUVAL GRAUER

16 The future of compliance and ethics: trends for the field into 2026
BY JOE MURPHY

19 Labor rules are changing – staying ahead with policy, training and more for a healthier culture and fewer incidents
BY CINDY RAZ AND ED MILLS

24 What's old is new again – 2026 presents new and enduring challenges in risk assessment
BY KYLE MARTIN

27 Signals show heightened stress on workplace cultures
BY SARAH JO LOVEDAY

31 The expanding role of the board of directors in compliance
BY REBECCA WALKER

35 Fundamentals that won't change amid 2026's regulatory headwinds
BY SIDNEY BASHAGO AND DANIEL KAHN

39 Looking back, moving forward: a 15-year journey in whistleblowing and incident management benchmarking – what's next?
BY CARRIE PENMAN

Executive summary

What are the top risk and compliance trends for 2026?

Echoing years past, experts contributing to this Top 10 Trends in Risk & Compliance publication described familiar forces that continue to impact our professions. Technology – namely, artificial intelligence – is reshaping the way organizations tackle misconduct. Supply chain ethics and integrity will matter more than ever. Risk-based strategic thinking is a difficult challenge, and signals of greater stress are growing in the workforce.

Many of these familiar themes come with corresponding guidance from our experts, learned from years of experience in the field. The way AI is empowering compliance is becoming clearer. Regulatory requirements and public expectations for ethical and resilient supply chains are becoming more consistent. The path forward in risk-based strategy may be resolving, and action to address recent cultural signals may be clearer.

The 2026 Top 10 Trends in Risk & Compliance serves as an indicator for the way forward in the months to come. Our experts have outlined not only challenges for compliance, but ways to address them.

We hope readers following these essays find ways to improve their compliance programs – to create more business value, improve cultures of ethics, positively impact their organizations' global reach – and much more.

Below is a summary of some of our predictions and considerations for 2026.

AI will play an important role for compliance programs, and teams will evolve in response

Artificial intelligence is becoming deeply integrated into compliance programs, and 2026 will see more clarity in questions about what the future will look like.

While the particulars differ for various organizations, a key question as this technology matures is around the expected role of compliance staff going forward. For example, integrating AI might mean that organizations will reorient their compliance teams to focus less on responding to inquiries about policies and more on considering policy soundness to support a self-service, AI-powered model for inquiries. Both processes are critical and only one element of compliance work, but this may represent the kind of clarification we'll see in 2026 as AI becomes more and more integrated in compliance programs.

It is exciting to see examples in practice for how these tools will enable Compliance to make a greater impact on their organizations. The nature of the work may change, but the goals of empowering individuals and ethical cultures will remain the same.

Organizations with ethical supply chains will win in 2026

Ethics and resilience in the supply chain has long been a critical value for organizations and consumers. The importance is only intensifying in respect to regulation, including the European Union's Digital Operational Resilience Act (DORA).

In 2026, our experts suggest organizations with ethical and resilient supply chains will have an advantage. Such flows of service and supplies are subject to change at a moment's notice, of course, but the fundamental considerations appear to be solidifying for 2026. Regulatory compliance, ethical considerations and resilient supply chains – these fundamentals are more solid than ever in 2026. This is particularly important as consumers increasingly expect these levels of supply chain due diligence regardless of regulatory requirements.

Sophistication of risk management and assessment will improve

NAVEX research and partnership with the industry have long signaled that the "language of risk" may not always share the same syntax as the language of compliance. Yet 2026 may be a time when that disconnect coalesces into a language that resonates across functional areas, enabling greater impact with boards of directors and others.

The language of "risk" is difficult to quantify and articulate across functional areas, but perhaps less so leading into 2026. Compliance is often seen as a risk-mitigating element of the organization, but where there is risk, there is also business opportunity. Tools and practices enabling conversations about Compliance's value to the organization are growing in importance – those who capitalize on those tools and strategies are likely to excel in 2026.

Worrisome signals endure in the workplace

Higher levels of reporting about any issue in the workplace should represent a "good thing," showing that employees trust the internal reporting system and feel willing to raise concerns of misconduct. These reports also provide insights into the "mood" of workplaces, and should be used to inform leadership on cultural trends.

Namely, *Workplace Civility*, the recommended nomenclature for reports often regarding employee relations or misconduct that NAVEX uses in our benchmarking, deserves attention in 2026. This reporting category (or in our parlance, *"Risk Type"*) often invites nuanced assessment as a signal of cultural health and has continued to grow as a share of total reporting. We've observed a notable increase in Europe, perhaps related to the evolution of the public consciousness in what constitutes misconduct in light of maturing regulatory protections for whistleblowers in the region.

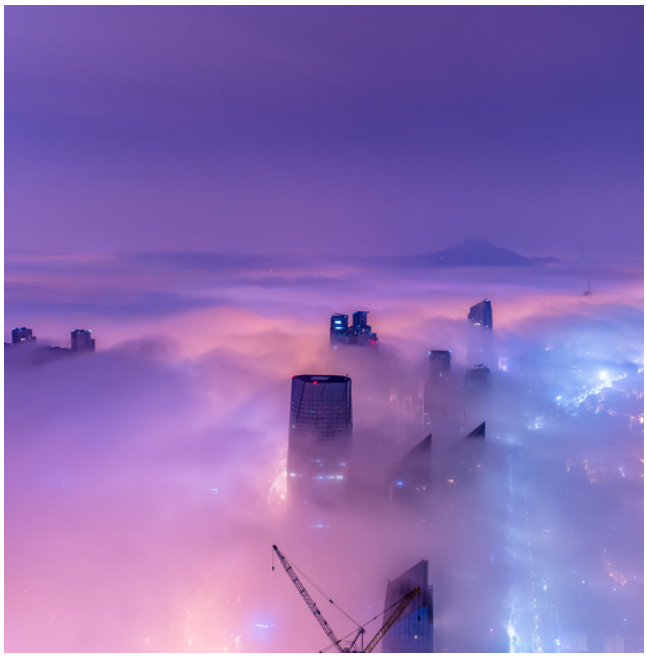
Unfortunately, this is not the only category in which we've seen an increase. *Imminent Threat to a Person, Animals or Property* has increased in the total global share as well. These shifts don't necessarily reflect more reporting in each category, but may invite consideration of the issues most important to reporters and where they are most willing to speak out.

These observations might suggest that 2026 presents a time when workers and other reporters are both better educated about cultural dynamics and reporting resources, but also, on edge. As *Workplace Civility* reports have been prominent in recent years, this is not necessarily something new. However, as our experts discuss, will 2026 be our opportunity to act and achieve the productive and ethical workplace dynamics that allow workers to flourish?

What does 2026 hold for Risk and Compliance?

The essays in this report represent a range of expert perspectives relevant to Compliance, Human Resources, Legal, Procurement and many other related professions.

It is thrilling to consider: by 2027, our industry may rest at a place of greater maturity and impact in line with the trends described in this publication. The path forward seems clearer. Yet challenges remain, and this guidance, along with other publications we provide freely to the public, is designed to help readers to navigate them.



How AI will impact Compliance teams' work and staffing

By Matt Kelly

Artificial intelligence was the dominant technology story of 2025, and will remain so in 2026. For better or worse – or, more likely, for both better and worse at the same time – AI is now seeping into every corner of corporate operations.

Compliance functions are no exception to that trend. Chief compliance officers will need to spend 2026 finding the right ways to integrate AI into their program and considering what an AI-enhanced program will mean for their team.

Brace yourselves. The final result might look quite different from what you imagine now.

We can break down the challenge ahead into several discrete tasks:

- Assessing the potential of AI to do compliance work
- Understanding how AI will transform the compliance processes you already run
- Identifying the new risk and technology questions that AI in a compliance program is going to raise

Chief compliance officers will need to spend 2026 finding the right ways to integrate AI into their program and considering what an AI-enhanced program will mean for their team.

Let's take each challenge in turn.

Understanding AI's compliance capabilities

Yes, AI can do a wide range of compliance work, and do it quite well – but doing compliance work is not necessarily the same as executing compliance processes.

Large language models (LLMs) from OpenAI, Microsoft, Google and Anthropic – often called "frontier models" – power nearly every AI system compliance officers encounter. These models excel at tasks such as matching or mapping data, extracting information, and ranking elements based on risk or urgency. They are great at language translation and pattern analysis. They can summarize long documents and suggest next steps in a course of action.

Those tasks are all *work* that compliance teams must get done; if AI can help to do that work faster, that's great. On the other hand, if you ask compliance officers what they do every day, they'll rattle off a list of processes:

- "I review whistleblower reports to identify serious issues that need immediate attention."
- "I assess conflict of interest submissions from employees, and consider whether we need more detail before coming up with a mediation plan."
- "I assess employee training needs based on risks we have, and confirm that the training materials we provide reflect those issues and work well."

Every compliance process consists of multiple smaller steps, and many of those steps are the work that AI can do well. AI, however, still struggles to string all that work together into one self-contained process that it can execute as well as a person.

So yes, AI can categorize conflict of interest (COI) submissions by issue, region, and so forth; but it struggles to understand what additional detail might help to determine the true risk in a COI submission. It can take a written policy and cook up a training video; but it can't easily ponder internal hotline and training data to devise a new policy that better addresses employee behavior.

For now, AI is still very much a tool compliance teams can use to achieve your program objectives. It can't achieve your program objectives on its own – that still requires people.

Fitting AI into your compliance program

Even when used simply as a tool, AI unquestionably can help chief compliance officers to improve your program overall. The real question for 2026 is how to integrate AI into your compliance program.

First, consider the objectives you and senior management want to achieve. AI can help with all sorts of process improvements, but making those improvements does need careful planning.

For example, you could use AI to build a policy chatbot that answers employees' questions about compliance policies. Lots of companies are already experimenting with this exact idea. Early evidence suggests employees do engage with policy chatbots often, which is good.

AI systems will transform your compliance program, leaving it able to do more things more efficiently. That doesn't automatically mean AI will make your program more efficient or less complicated – the work of compliance teams will adjust to support these new capabilities.

At the same time, however, you may need to write longer policies, and update them more often, to assure the policy chatbot gives current and correct answers. You might also have more policy escalations to evaluate since employees are asking the bot more questions (sometimes, lots more).

In other words, policy chatbots can help you build a more engaging compliance program, but that effort might **rearrange** the work your compliance team does – eliminating some work here, creating new work there. Some of that work, AI will handle; other work, human employees will still need to manage.

That's the sort of analysis chief compliance officers will need to perform in 2026 and beyond: "If we introduce artificial intelligence into this compliance process, how will it change that process? And what will that change mean for my own team supporting that process, and what will it mean for others engaging with that process?"

The list of potential scenarios here is long. AI systems will transform your compliance program, leaving it able to do more things more efficiently. That doesn't automatically mean AI will make your program more efficient or less complicated – the work of compliance teams will adjust to support these new capabilities.

The other challenges AI introduces

Compliance officers also need to think about the larger strategic questions of how to "fit" AI into your compliance program and your organization's IT environment.

For example, most LLMs can now do most compliance work quite well – but no single LLM does **all** compliance work **consistently** well. So, would you want to use one LLM that is good at all your compliance tasks, but not necessarily great at the one or two compliance tasks that matter most to you? Or would you want to use multiple LLMs, each one focused on your most common or pressing needs?

Using only one LLM would save money and reduce security and operational risks, but may sacrifice performance. Using multiple LLMs may bring better performance, but may introduce more security and operational risk. So how would you, your CISO, your IT manager, and your CFO decide which choice is best?

The questions about using AI strategically in your compliance program are many. They'll need to be answered too.

Compliance's role for broader AI implementation

Compliance officers will also play a crucial role helping the rest of the enterprise as they integrate AI into **their** operations, too.

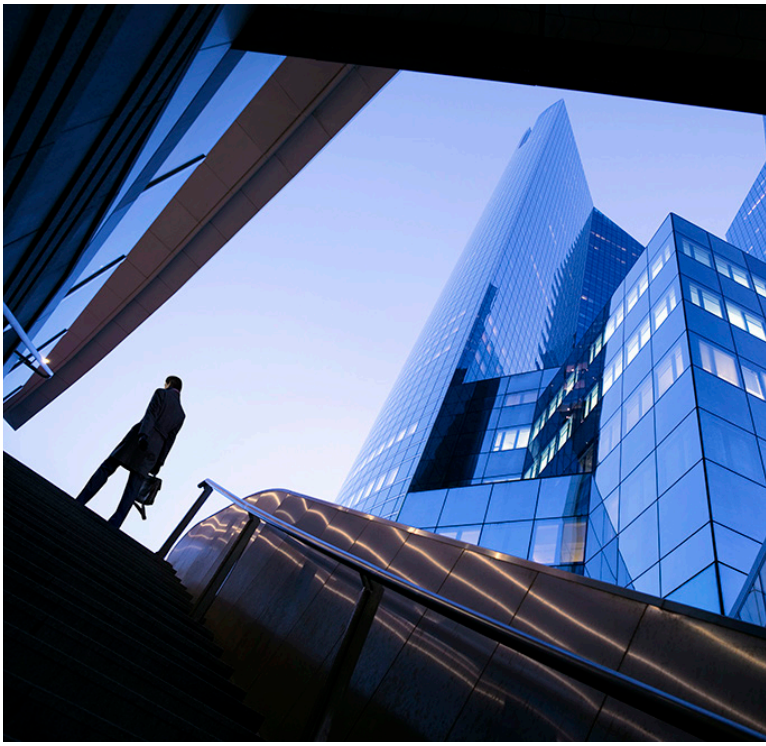
First, business units will need help identifying and assessing the compliance risks that might arise from weaving AI into their processes. Then they'll need help developing and implementing new controls to make sure their AI-enhanced business processes avoid privacy, security and compliance risks.

What does that mean in practice? Consider a few steps.

Develop an AI governance model. That is, a structured approach for senior executives (ideally, a team including heads of Legal, IT Security, HR, Finance, and of course Compliance) to review and approve AI implementation across the enterprise, so those use-cases properly handle the company's compliance obligations. Good news: according to the NAVEX 2025 State of Risk & Compliance Report, two-thirds of compliance officers are either "very" or "somewhat" involved in deciding how AI is used within your organization.

Use frameworks to guide your AI implementation. Frameworks can help you identify new regulatory risks, gaps in your existing controls, and new controls that might plug those holes. Two leading frameworks today are the ISO 42001 standard for AI management systems, popular in Europe; and the NIST AI Risk Management Framework in the United States. Australia, Singapore, and other countries are rapidly developing their own regulatory frameworks too, so keep your eyes open globally.

Prepare to help. As your organization rolls out new policies or controls for AI, you'll need new training and communication materials to help employees understand AI risks and behavior. You'll need policy management capabilities to identify new AI regulations as they arrive to see whether your policies need updating. You'll need testing, auditing and data analytics capabilities geared for AI risks, too.



2026 prediction

Concerns about an "AI bubble" will become more pointed – primarily for the LLMs spending billions on data center infrastructure, but even for other AI businesses too. Executives will want to see clear and specific ROI for proposed AI investments, so team leaders trying to integrate AI into their operations will need good answers for productivity gains, risk management requirements and data management challenges.

About the author

Matt Kelly
Matt Kelly is editor and CEO of Radical Compliance, a blog and newsletter that follows corporate governance, risk, and compliance issues at large organizations. He speaks and writes on compliance, governance, and risk topics frequently. Follow him on LinkedIn or get in touch with him via email.

Supply chain integrity in 2026: what does this mean?

By Pierre Berlioz

"Resilience" is clearly the keyword for 2026 – the mantra that must guide every company to face the ongoing turbulence, which, regrettably, we fear will extend beyond December 31, 2026.

"Resilience" rather than "sustainability," because sustainability has been experiencing an unprecedented backlash since its emergence, unfortunately associated with the idea of a bureaucratic burden. This perception is fuelled by regulations whose extreme sophistication and unreasonable haste have undermined their foundations.

"Resilience" rather than "competitiveness," because competitiveness has been weaponized to conceal attempts to maintain outdated models through deregulation. Ultimately, this approach will only weaken the global economies and their players against competitors who understand the power of law to impose new perspectives.

Resilience for sustainability and competitiveness, instead, because sustainability and competitiveness are truly effects, not causes. A company can only be sustainable **and** competitive – one doesn't happen without the other – if it rests on a **resilient** foundation, enabling it to develop despite geopolitical, economic or regulatory hazards and obstacles.

From this perspective, the supply chain is a significant stake. It can be a pillar of strength or the company's Achilles' heel, depending on the company's ability to ensure its integrity. Integrity, in this context, means ensuring every link in the chain is sufficiently robust. The fragility of any single link can indeed compromise the proper functioning of the entire chain and, consequently, the long-term viability of the company whose activity relies on it.

A company can only be sustainable and competitive – one doesn't happen without the other – if it rests on a resilient foundation, enabling it to develop despite geopolitical, economic or regulatory hazards and obstacles.

The difficulty lies in identifying these fragilities. In this regard, lines can be considerably blurred by issuing directives that are sometimes contradictory and adopted within short intervals. In this context of permanent shifts – in this uncertain landscape that will, at best, only partially clear up during 2026 – companies can legitimately feel lost.

They can also see this as an opportunity for a genuine, strategic groundwork effort, moving past the minor vicissitudes of the literal text of the regulations and the confusion they create. Instead, they can focus on the spirit of the regulations, which possesses a genuine rationality: the company must know and understand its supply chain to both control it, and thus ensure its integrity.

Knowing your supply chain

The banking sector, as well as certain service providers (e.g., accounting or legal professionals), have an obligation to Know Your Customer (KYC), notably to avoid being unwitting accomplices in illicit operations. Knowing your customer requires tracing the chain of financial flows to identify the ultimate beneficial owner of the transaction.

Increasingly, due to the risks they face, companies have a similar obligation to know their suppliers and subcontractors, not only Tier 1 but also those below, right up to the initial source of supply.

This obligation is one of the significant issues associated with adopting the Corporate Sustainability Due Diligence Directive (CSDDD) and determining its final content following the 2024 reform of its initial text in the "omnibus" draft directive.

However, other texts impose a similar obligation and are scheduled to come into effect progressively starting in 2026. This is particularly the case with regulations aimed at combating deforestation and forced labor.

The first requires that palm oil, soy, wood, cocoa, coffee, cattle and rubber, as well as products derived from these commodities, entering, circulating within, or being exported from the European market, must be "deforestation-free" and have complete traceability ensured. Consequently, this means the different links in the supply chain must be known, and each link must possess this information.

The second regulation prohibits the placing on the European market, circulation within it, and export from it of products resulting from forced labor. This text indicates that it "does not create additional due diligence obligations for economic operators other than those already provided for by Union or national law." In other words, the issue of forced labor is a subject that companies subject to due diligence obligations under their national or European law must integrate into their implementation. The regulation is thus intended to fit within the framework established by the CSDDD and be applied in accordance with its provisions.

The regulation applies to all companies, regardless of their legal nature, form or size. However, not all companies are legally obligated to undergo due diligence. Therefore, while the regulation does not formally create any obligation for companies to exercise due diligence regarding forced labor, it indirectly creates such an obligation, nonetheless.

This is also the case with the CSDDD. Article 8 of the directive requires subject companies to carry out mapping of their own activities, those of their subsidiaries, and, when linked to their chains of activities (value chain), those of their business partners. Although the text does not explicitly state it, this implies the company must know its suppliers and subcontractors at various tiers.

The current discussions on the omnibus draft directive demonstrate this. As the objective of this text is to simplify the mechanism, the proposals aim to clarify specific provisions of the CSDDD, particularly Articles 8 through 11. Specifically, the text adopted by the Council of the European Union for trilogue negotiations includes a provision in Article 8 stating that the company must map its chain of activities to identify its indirect business partners.

Admittedly, this mapping must be carried out using reasonably accessible information. The directive only establishes best-effort obligations, but it clearly states an obligation to know your supply chain.

Given that a company can only know this chain by tracing it upward, this obligation will indirectly fall on every company member of a supply chain. Each company must be able to communicate to its higher-ups in the chain – particularly the one directly above it – which links are situated below it.

The adjustment of thresholds currently being discussed by the European legislator will not alter this fundamental principle: all companies must be aware of their supply chain.

Controlling your supply chain

Why is it necessary to know your supply chain? It is not a bureaucratic requirement. It is an indispensable precaution that allows for discerning strengths and weaknesses, thus enabling the necessary measures to be taken to control it. This ensures it is managed as efficiently as possible while preventing the risks it may generate.

This highly strategic knowledge constitutes a trade secret for many companies, protected as such by the European Directive of June 8, 2016, and the implementing laws of the member states. The company is therefore not required to make it public; only the results of risk analyses performed based on this data may be published. This point is affirmed by the CSRD (Corporate Sustainability Reporting Directive) and is expected to be even clearer in the revised version of the omnibus directive.

However, this protection is conditional on the existence of measures intended to maintain the secrecy of this information. The company's information system must therefore ensure that access to this data is limited to those who need to know and that these individuals are subject to confidentiality obligations.

Similarly, when a company communicates this information to other links in the supply chain, either in execution of a legal obligation or to comply with contractual obligations, it is imperative that it expressly state its confidential nature and impose its preservation through adapted clauses.

This necessary control over the supply chain, which pertains to the company's strategy, is not explicitly mandated by the texts. The CSDDD, the regulations on deforestation or forced labor, or similar texts only require risk prevention. Control of the value chain is a means of this prevention, the content and methods of which are left to the company's discretion.

Nevertheless, the regulation provides companies with legal avenues to ensure this control. This is notably the case with the CSDDD, specifically Articles 10 and 11, which mention obtaining contractual guarantees as possible measures.

The contract is indeed the principal instrument for managing the supply chain, as the chain itself consists of a series of agreements between multiple companies that link them within the same productive and/or commercial process. Control of the chain thus necessarily involves inserting clauses into these various contracts, either to prohibit certain activities or behaviors, or to impose certain practices or the communication of information. These clauses can also help ensure a certain homogeneity within the chain by requiring the dissemination of prohibitions or obligations to the different links.

The CSDDD favors the use of these contractual tools, as stated in Articles 10 and 11, which stipulate that "Member States shall provide for the possibility to temporarily suspend the commercial relationship or terminate it in contracts governed by their law, except for contracts which the parties are legally required to conclude."

This provision opens an interesting avenue for companies to insert stipulations into contracts that allow them to manage the value chain, as it legalizes a leverage tool that might otherwise be considered abusive under general contract law. The directive expressly provides for the possibility of the company using or increasing its leverage by temporarily suspending commercial relations, which, without this provision, could be considered abusive conduct.

This possibility can be an effective way to integrate a code of conduct into the supply chain. The difficulty with the supply chain lies in the potential disparity in the contracts that comprise it. Referencing a single code of conduct in each of these contracts helps prevent this disparity. However, the clauses referencing the code must stipulate not only adherence to the code but also the renewal of this adherence when the code is updated, to avoid different versions applying to other links in the chain.

In periods of legal uncertainty, such as the one we are currently experiencing, the contract serves as an effective and convenient tool for establishing a stable and harmonized framework that can compensate for the fragmentation and variability of legislation.

2026 prediction

In conclusion, supply chain integrity appears to be essential for businesses to remain resilient in the face of growing risks. By equipping themselves with the means to understand and control their supply chain, organizations can transform a constraint into a strategic lever, capable of securing their operations and strengthening their long-term competitiveness. This approach should not be seen as a sterile compliance exercise. It is an essential investment for facing 2026 and the years to come.

About the author

Pierre Berlioz

Specialized in corporate and digital law, Pierre Berlioz served as adviser to the French Minister of Justice during the drafting of the Sapin II law, the due diligence (Devoir de Vigilance) law, and the Digital Republic law (loi pour une République numérique). He then served as chief of staff to the president of the French National Institute of Statutory Auditors (CNCC) during the CSRD negotiations. He subsequently held the position of director of European and international affairs at the Union des Industries et Métiers de la Métallurgie (UIMM). Today, he teaches business law, compliance, and CSR at Paris Cité University and co-chairs the Medef's sustainable finance and ESG reporting committee.

Compliance trends for Europe – what do you need to watch?

By Yuval Grauer

Companies face severe fines, increased regulatory scrutiny and significant compliance obligations under a raft of European Union (EU) and national legislation that has either recently come into force or which will take effect in 2026. Chief among these are duties to check the cyber resilience of third-party IT providers, improve supply chain due diligence and identify, prevent and remediate any actual or potential harm, and provide better protections for whistleblowers.

Through its Digital Operational Resilience Act (DORA), the EU is trying to push financial services firms to take greater control of – and accountability for – IT risks to protect the sector as a whole from potential cyberattacks. Previously, financial institutions were mandated to manage the main categories of operational risk primarily through the allocation of capital rather than through any other kind of operational resilience, such as the level of technology preparedness.

Companies face severe fines, increased regulatory scrutiny and significant compliance obligations under a raft of European Union (EU) and national legislation that has either recently come into force or which will take effect in 2026.

The rules, which came into effect on January 17, 2025, set strict requirements on information and communication technology (ICT) risk-management, incident reporting, operational resilience testing, and information and intelligence sharing with regulators. Crucially, the legislation also makes financial services firms responsible for the risk monitoring of "critical" third-party IT suppliers.

But because the rules have significant financial penalties attached, rather than creating a push for better compliance, firms have instead tried to push responsibility back onto third-party IT vendors by tightening up contract terms if they want to retain business. And for those financial firms with muscle, the signs are that tech services suppliers are buckling under the pressure. As a result, DORA may put tech providers under enormous regulatory scrutiny.

The implications of DORA

Industry experts have suggested that many firms in the financial sector were slow to meet DORA's requirements before the legislation took effect, which may have also prompted them to try to offload as much of the compliance work as possible – as well as the costs – onto the IT firms they work with. The main way they have done this is by renegotiating contracts with IT outsourcers so that the tech services they provide are categorized as "critical or important", even if they are not, thereby passing some of the compliance "burden" onto their third parties who are then obligated to provide more assurance. Firms are also using DORA as an opportunity to renegotiate vendor relationships more broadly, demanding enhanced transparency, data-sharing capabilities, and resilience reporting.

While tightening contractual clauses may appear to enhance compliance, it does not absolve firms of their responsibility: under DORA, boards ultimately remain accountable for their level of IT resilience and capability to report incidents

within the necessary timeframe. Furthermore, pushing DORA's compliance requirements back on to IT services providers could backfire. Not only could such a heavy-handed approach lead to strained relationships, but it could inadvertently put financial firms at greater risk of non-compliance because they will be even more reliant on the suppliers for assurance, while their lack of in-house expertise also gives them reduced internal preparedness.

DORA's scope is broad and almost all financial entities operating inside the EU are in scope, including banks, lenders, fintechs, trading venues, crowdfunders, crypto entities, investment firms, insurers, credit rating agencies and payments providers. Non-compliance can result in financial penalties up to 2% of their total annual worldwide turnover, or 1% of daily global turnover, as well as the removal of authorizations to conduct regulated business. For individuals, penalties can reach up to €1 million. Critical third-party ICT providers face even higher fines of up to €5 million (or €500,000 for individuals) if they fail to meet DORA's standards.

Supply chain due diligence comes to the forefront

Supply chain due diligence is also set to become a bigger issue in 2026 as both national and EU-wide rules become increasingly embedded in operations and regulators take a keener interest in enforcing them.

The German Supply Chain Due Diligence Act entered force January 1, 2023 and allows prosecutors to impose fines of up to 2% of a firms' global turnover if they fail to identify and prevent human rights and environmental impacts in their supply chains. It applies to companies with a registered office or principal place of business in Germany, as well as foreign companies with a branch office there. It applies to companies with 1,000 workers or more.

Although the act does not give rise to any new liability under civil law, it is expected to prompt non-governmental organizations to more readily file lawsuits for alleged human rights violations in German courts. During 2023, in its first year, just 30 complaints were brought under the legislation (and 22 of these were dismissed). In 2025, 75 cases were brought forward.

Contrast this with France's similar Duty of Vigilance Law, which came into effect in 2019. As of May 2025, just 16 claims have been filed, irrespective of whether either piece of legislation has sanctioned many companies, both have compelled large corporations to prioritize human rights and environmental considerations within their supply chains in a way they had not done so before.

Supply chain due diligence is also set to become a bigger issue in 2026 as both national and EU-wide rules become increasingly embedded in operations and regulators take a keener interest in enforcing them.

New human rights regulations

EU-wide rules on identifying, preventing and mitigating actual and potential adverse environmental and human rights impacts will also take effect in 2026 as the deadline for member states to transpose the EU Corporate Sustainability Due Diligence Directive (CSDDD) into national law comes into effect in July. The rules apply to large companies (those with 5,000 employees initially, reducing to those with 1,000 or more employees and revenues over €450 million after three years).

Penalties for non-compliance can be tough. The maximum limit of financial penalties member states need to provide for must be at least 5% of the net worldwide turnover of the company in the financial year preceding that of the decision to impose the fine. If a financial penalty is imposed, the decision relating to the infringement will be included in a public statement, and this will remain available for at least five years – effectively "naming and shaming" the company.

Additionally, where damage is caused jointly by a company and its subsidiary, or by the company and its direct or indirect business partner, those entities will be held jointly and severally liable. The CSDDD also introduces a civil liability regime which requires member states to ensure that a company can be held liable for damage caused to people or companies if it intentionally or negligently failed to comply with its obligations. If companies hadn't already had supply chain due diligence on their compliance radars already, that will need to change in 2026.

If companies hadn't already had supply chain due diligence on their compliance radars already, that will need to change in 2026.

Whistleblowing rules mature in the United Kingdom and EU

Whistleblowing has long been recognized as a powerful mechanism for employees and third parties to speak up about wrongdoing, but the level of protection they can expect often remains problematic. And so it goes with United Kingdom plans to encourage whistleblowing.

In September 2025 the U.K.'s third "failure to prevent" offense came into effect under the Economic Crime and Corporate Transparency Act (ECCTA). Two similar offenses – the failure to prevent bribery and tax evasion – are already in force under different legislation, namely the Bribery Act 2010 and the Criminal Finances Act 2017. Each requires corporates to police themselves, their employees and the third parties with whom they do business. Together, these laws are aimed at expanding the scope of corporate liability.

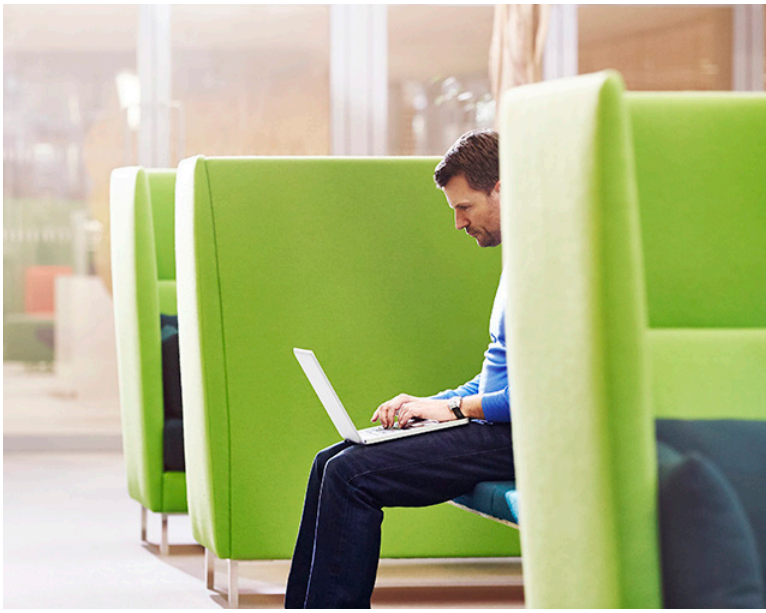
The U.K. government hopes the new offense – in tandem with the two existing ones – will put a renewed focus on the need to support whistleblowing as employees raise the alarm over suspected illegal business activity.

However, the key problem with ECCTA is that while whistleblowing is encouraged, disclosure is not incentivized and employee protections are not being improved. Other obstacles may also bar success. For instance, there has historically been relatively little transparency in the U.K. around the outcome of whistleblower reports, partly due to the fact that U.K. authorities – unlike the United States – do not offer financial rewards in exchange for information, which means there is little fanfare about the role whistleblowers may have played in a company and its executives being brought to book.

Not that there is a great track record of successful prosecutions. Since the Bribery Act came into effect in July 2011, there has only been an average of 10 prosecutions a year and only 10 deferred prosecution agreements (DPAs) up to early 2025 for "failure to prevent bribery." In addition, the first charges under the Criminal Finances Act were only brought almost eight years after failure to prevent tax evasion became an offense (and the case is ongoing).

Furthermore, the level of protection – as well as incentive – for employees to come forward is lacking. The Office of the Whistleblower Bill, which will create the independent authority meant to improve protections, has stalled and is still a long way from becoming a reality. Under its current form, the bill would widen the number of entities that can receive a whistleblowing report and introduce a criminal offense for those causing detriment to whistleblowers with a proposed maximum sentence of a fine or 18 months' imprisonment. It is due to have its second reading in spring 2026.

Meanwhile, talk of financially incentivizing whistleblowing has had a mixed reception: the Serious Fraud Office (SFO), the U.K.'s main anti-corruption enforcement agency, the Financial Conduct Authority (FCA) and the U.K.'s tax authority, HMRC, are supportive, but few others are, and many experts believe such a concept would need legislative change. As such, there are concerns that the three "failure to prevent" offenses may prove ineffective if whistleblower protection isn't improved as well.



The EU is also reviewing whether its Whistleblower Protection Directive is effective. In August 2025 the European Commission launched a call for evidence to evaluate how well the directive has been implemented across all EU member states since its adoption in 2019. Specifically, it will assess whether:

- The directive has strengthened whistleblower protection and encouraged reporting
- The benefits are proportionate to the costs; if it still meets today's challenges and future needs
- If is it aligned with other EU and international policy developments
- Whether it has achieved more than member states could have done individually

The evaluation is due to be completed by the end of 2026 – five years after the directive was meant to be transposed into national law. There has long been some criticism – and concern – that some member states were slow to pass legislation, and that in some countries there is still confusion about what the term "whistleblower" actually means, which doesn't bode well for the level of protection people might receive.

There is little doubt that 2026 will create several significant compliance challenges to companies operating in the EU and U.K., and across a range of operational areas. DORA requires in-scope organizations not only to look at their own operational resilience and reporting processes, but those of major IT service suppliers, while requirements under supply chain due diligence rules – both at national and EU level – will also require much deeper probing of third-party relationships, too. Meanwhile, the U.K.'s latest focus on corporate fraud will prompt companies to review their whistleblower hotlines and the measures they have in place to protect those who speak up as the EU also considers how its own whistleblower protection rules can be beefed up and improved.

2026 prediction

Through 2026 compliance teams will need to reassess how well-prepared their organizations are to respond to these new duties, as well as how their organizations can leverage the upsides of what these regulations are meant to create – namely, better cyber resilience, robust supply chain management and more open workplace environments where people can feel safe about raising governance concerns without reprisals. Regulatory enforcement may not take place immediately – but scrutiny will.

About the author

Yuval Grauer
Yuval Grauer is International EVP and Managing Director at NAVEX. He leads business growth in Europe, the Middle East, and Africa (EMEA) and the Asia-Pacific region (APJ).

Based in London, Grauer spearheads initiatives to extend NAVEX solutions across high growth markets. He brings years of strategic insight from his time at McKinsey & Company, combined with deep operational expertise and a proven track record of growing and scaling global businesses of all sizes. He holds an MBA from Columbia University in New York, a Master of Engineering from Universitat Politècnica de Catalunya, and continued studies in Economics at the Universitat de Barcelona.

The future of compliance and ethics: trends for the field into 2026

By Joe Murphy

What can we anticipate in the next year for the field of Compliance & Ethics (C&E)? I recently posted my ideas in Compliance and Ethics: Ideas & Answers on the longer-term future of our field, "The Future of Compliance & Ethics: Will We Boldly Lead the Way or Become a Noble but Failed Experiment?"

Here, I will first address a few topical issues and then discuss three possible areas for development.

Topical issues:

- What about collaborative AI, large-language models, etc.? This technology will be put to work by very creative people developing more sophisticated ways of committing crimes. We will need to use AI just to keep up.
- What about the current United States administration? C&E has been below the political level at the U.S. Department of Justice in 2025, and so the incentive system remains quietly in place. But this could vanish overnight if it becomes a political issue. Incentive-based C&E does remain in other countries. As long as it remains below the political/influencer spotlight in the U.S., it will remain. C&E people will need to focus on three reasons for C&E programs: the business case, the legal case and the moral case. But the legal case will be tougher to make in the U.S. in the short run than it has been in the past.
- Senior people will continue to be the prime drivers of misconduct and the highest source of compliance risk. As long as C&E people lack power and any role in incentives/promotions, this will continue unabated.
- More professors and commentators will offer to help us and tell us we are wrong in what we do in C&E. Fortunately, some will have useful insights.

Without genuine power, chief ethics and compliance officers cannot protect whistleblowers, challenge misconduct or ensure ethical behavior at the top.

- Government mandates on the details of what should be in C&E programs will continue in hyper-regulated industries like banking and finance. These over-regulated C&E programs will inhibit efforts to make the programs truly effective, and will continue to fail, because they are not based on fundamentals like power, incentives and preventing retaliation.
- Europe will continue to deal with the directive intended to prevent retaliation. Look for continued foot-dragging and circumvention. Government bodies are supposed to have their own anti-retaliation system. Don't expect to see very much here (I hope I am proven wrong).

Three essential elements for the future

1. **Power: the forbidden topic**
   We deal with crime and misconduct. These often originate – or are enabled – by those with power at the top of the organization. To counteract power, C&E professionals must also have power. Yet the word "power" rarely appears in our literature or conferences. Instead, we opt for softer terms like

"authority," and are usually reluctant to push. Lord Acton famously said, "Power tends to corrupt, and absolute power corrupts absolutely." In today's companies and other organizations, the top leaders come very close to absolute power. This can even be seen in lower levels where managers carve out their own little fiefdoms. If chief ethics and compliance officers (CECO) lack power, and only have a seat at what Nick Gallo calls the "kiddie table" – lacking direct access to the board – they lack the ability to do their job. Without genuine power, a CECO cannot protect whistleblowers, challenge misconduct or ensure ethical behavior at the top.

Will corporate boards start to recruit CECOs from other companies to join their boards? It would be a spectacularly good idea, but I don't see it happening. I suspect, though, that this is likely only to change when government drives the change. Will we do better in 2026 in addressing this reality? My pessimistic answer: no. But it is definitely important to keep trying.

2. **Incentives: a neglected essential**
Incentives drive behavior. Peter Drucker said it well: people respond to rewards, not preaching. Yet despite its inclusion in the U.S. Sentencing Guidelines for over two decades, many C&E programs ignore this critical area.

Promotions, raises, and recognition all signal what an organization truly values. I heard a professor in South Africa once say that an organization's real code of conduct is its budget. A CECO who ignores these incentive, reward and promotion systems isn't doing their job. Who would be dismissive of the CECO, for example, if the CECO actually had a say in who gets promoted?

Even simple acts – like recognizing ethical behavior or linking performance evaluations to values and active support for the C&E program – can be powerful. But fear, or lack of support, often stops C&E professionals from touching incentive systems. This silence signals weakness and can lead to irrelevance.

Will this change in 2026? Very likely, no or very little. I can predict that under the current administration we will not get the strong signals from government that incentives count. Since the field ignored even strong signals in the past, it is highly unlikely it will move in this direction if there are no signals at all. There are, however, many ways C&E people could at least start to deal with incentives. The "Using Incentives in Your Compliance and Ethics Program" guide I wrote for SCCE can help get anyone started on this road. So, while I cannot predict a dramatic shift in direction, 2026 could see some incremental progress in this direction.

We are the ones who fully understand how these legal gaps hurt the public and our profession.

3. **Speaking up to government and lawmakers**
While we wisely avoid lobbying on laws we're tasked with enforcing, we too often stay silent when legal systems directly undercut our work. Judges, laws, and regulators sometimes ignore or even weaponize our efforts. For example, sloppily written privacy laws create traps for C&E professionals, and compliance work may even be used against companies.

The U.S. Department of Justice, for all its written guidance, rarely, if ever, acknowledges prior existing C&E programs during actual enforcement actions. If no such program is ever praised – or even mentioned – how can organizations take the effort seriously or learn from the enforcers' actions? What actual cases can we show to management to prove that the government really takes our C&E programs seriously when it matters?

We are the ones who fully understand how these legal gaps hurt the public and our profession. Yet we remain silent, lacking a united voice to push back or educate. That is a costly weakness in our profession.

Will this change in 2026? I do not see any movement in this direction. But there is always hope that an established C&E organization, or a new and aggressive one, will see the need and step forward.

What the future requires

I've worked in and witnessed C&E around the world for nearly 50 years. If we want our profession to succeed and have real impact in preventing corporate and other organizational crime and misconduct, we must:

1. **Embrace power** as essential to controlling power
2. **Address incentives** directly – no program is credible without this
3. **Speak up** when laws or systems undermine our mission

Governments have driven much of the change in this field – and still hold the key. But they must act wisely:

- Don't ignore compliance programs when assessing corporate culpability
- Don't mandate them in a way that renders them mere technicalities
- Instead, **acknowledge real programs in enforcement decisions,** and **share lessons learned.** That's how we build effective, credible systems
- Do what you tell us to do: back up your words with actions

2026 prediction

Within 10 years, we will either have risen to meet these challenges or fallen into irrelevance. The window for action is closing fast. But we still have time – if we choose to use it.

About the author

Joe Murphy

For over 45 years, Joe Murphy, CCEP, has been a tireless champion of compliance and ethics in organizations and has done compliance work on six continents. He is currently an editor of the weekly newsletter, Compliance and Ethics: Ideas & Answers, https://ideasandanswers.com. Joe has published over 100 articles and given over 200 presentations in 21 countries. Joe is author of 501 Ideas for Your Compliance & Ethics Program and A Compliance & Ethics Program on a Dollar a Day. He is a Certified Compliance & Ethics Professional and a former member of the board of the Society of Corporate Compliance & Ethics. Joe was named one of The National Law Journal's 50 Governance, Risk and Compliance Trailblazers and Pioneers 2014 and received SCCE's Compliance and Ethics Award. He has been recognized as a lifetime member of the Australian Compliance Institute.

Labor rules are changing – staying ahead with policy, training and more for a healthier culture and fewer incidents

By Cindy Raz and Ed Mills

2026 will see significant developments in United Kingdom employment rights, as well as new pay reporting measures in Europe. In this article, we look at what this means in practice and how employers can stay ahead of the forthcoming changes – trends that may also be worth consideration well outside of Europe.

Expansion of day one rights

U.K. workers will gain increased rights from the start of their employment, under the Employment Rights Bill.

Unfair dismissal

All employees will benefit from **unfair dismissal protection from day one** of employment. Currently, there is a two-year service requirement before employees can bring an unfair dismissal claim (save for in limited circumstances, such as whistleblowers who can claim from the start of employment), but this will be abolished in 2027.

This is a significant change, meaning that many more employees will have unfair dismissal rights than before. Employers intending to dismiss any employee, including a new starter, will need to ensure they have a fair reason (such as poor performance, misconduct or redundancy) and follow a fair process. However, there will be a statutory probation period (likely to be nine months) during which the employer can terminate for performance or conduct with a lighter touch dismissal process.

In the United States, most workers are employed "at will," meaning employers can terminate employment for nearly any reason that is not unlawful. Unlike many other countries, the U.S. does not offer a general right to claim unfair dismissal. Instead, protections focus on specific violations—such as discrimination, retaliation, or breach of contract. As a result, wrongful termination claims arise only when a dismissal violates these defined legal standards, and employees typically pursue them through the EEOC, state agencies, or the courts.

This is a significant change, meaning that many more employees will have unfair dismissal rights than before.

Employers in the U.K. should ensure all new starters have a probation period in their contracts and that there is a process in place for regular performance reviews during probation. More widely, employers will need to review disciplinary and dismissal policies and processes and ensure managers are trained on managing conduct and performance issues.

Family and sickness

Paternity leave and unpaid parental leave will become day one rights in the U.K. from April 2026. At the moment, employees need minimum service before taking this leave (26 weeks' service for paternity leave and one year for unpaid parental leave).

Paternity leave consists of two weeks leave to be taken within a year of the child's birth/adoption, paid at the statutory rate (currently £187.18 per week). Unpaid parental leave may be taken for up to 18 weeks (but no more than four weeks in any one year) before the child's 18th birthday.

From 2027, there will be **enhanced dismissal protections for employees taking any type of family leave**, including maternity, adoption or shared parental leave. Employers will be unable to dismiss employees who are pregnant or on family leave, or who returned from family leave within the previous six months, except in certain narrow circumstances (details of which are currently subject to consultation).

Employees will have a new right to at least **one week of bereavement leave** following the death of a family member (the detail of which family members are covered is yet to be confirmed), from 2027.

Also, **statutory sick pay (SSP) will become available to all workers from day one** of sickness absence, from April 2026, as both the current four day waiting period and minimum earnings eligibility threshold (£125 per week) will be removed. SSP is payable at the statutory rate, currently £118.75 (or 80% of average earnings for workers who earn below the statutory rate).

Paid sick leave in the United States is not required at the federal level, so access depends on state and local laws or employer policies. This leads to wide variation in coverage, making it even more important for employers to support people when they need us most. Offering paid sick leave not only protects employee health but also strengthens trust, wellbeing and a healthier workplace overall.

Flexible working

Flexible working rules in the U.K. will be strengthened. Employees already have a **right to request flexible working** from day one of employment, which employers can only refuse for certain business reasons (e.g., impact on customer service). From 2027, employers will have to consult employees about their request and must explain why any rejection is reasonable. This is a higher bar for employers to meet and will require employers to review their current policies and practices and ensure managers receive training in how to handle flexible working requests in a compliant manner.

Flexible working in the United States is not guaranteed by national law, and employees generally have no statutory right to request it. Instead, flexible arrangements – such as remote work, flexible hours, or hybrid schedules – are set by individual employers and vary widely across industries and roles. Even without legal mandates, flexibility has become a key tool for attracting and retaining talent and supporting employee wellbeing.

Workplace harassment

Since October 26, 2024, U.K. employers have been under a **duty to take reasonable steps to prevent sexual harassment** of their employees, with compensation for sexual harassment claims increased by up to 25% if they breach this duty. In addition, the duty is enforceable by the Equality and Human Rights Commission (EHRC) which can issue enforcement notices and fines.

Key compliance measures for employers include:

- Carrying out a risk assessment and keeping it under regular review
- Having an effective sexual harassment policy which is relevant to the employer's specific workplace
- Training managers and staff in sexual harassment including raising and handling complaints
- Encouraging staff to "speak up" to report any concerns
- Investigating complaints and keeping a centralized record to identify trends
- Addressing third-party harassment risks

From October 2026, U.K. harassment laws will expand further. Employers will be liable for **third-party harassment** of any kind (not just sexual harassment) by third parties who their employees deal with in the context of their work, such as clients or suppliers. Employers will need to take steps to reduce the risk of third-party harassment, such as appropriate wording in contracts or in codes of conduct with clients and suppliers. Additionally, anti-harassment policies should be updated to encompass third-party harassment, and employers should clearly communicate to employees how they can report concerns about third-party harassment, including through designated "speak up" channels.

The active duty of employers to prevent sexual harassment, and the new third-party harassment rules, are similar to the California workplace violence laws which came into force in 2024. Both in California and the U.K., employers are obliged to take proactive, preventative steps to protect employees before any harm is done. It will be interesting to see whether this develops into a wider global trend in the future.

Workplace culture, 'speak up' and investigations

Workplace culture remains firmly in the spotlight and will continue to be so in 2026. There is ongoing scrutiny of **how employers handle "speak up" complaints**, against a backdrop of media coverage of historic misconduct allegations at high-profile organizations. Median report volumes have increased in Europe in the years following the passage of the EU Whistleblower Protection Directive, and

recent years have seen Workplace Civility-type reports in the region increase as well. Globally, report volumes remain at historically high levels.

Workplace culture remains firmly in the spotlight and will continue to be so in 2026.

The importance of ensuring that "speak up" reports are fully and transparently investigated is brought into focus by the forthcoming **restrictions on confidentiality provisions** in U.K. settlement agreements from October 2026. Employers will not be able to use confidentiality provisions or non-disclosure agreements to prevent employees from making allegations or disclosures about harassment or discrimination, including about how the employer responded to any allegations or disclosures.

The proposal is likely to have a significant impact on settlement agreements. Often, both employer and employee want to maintain confidentiality in a settlement involving harassment or discrimination, given the sensitivity involved. There has been some indication from the government that these restrictions will not apply if an employee requests confidentiality, but it is unclear how this would work in practice. If it is not possible for parties to agree on enforceable confidentiality provisions, this could result in fewer settlements, because either or both sides may feel they have less to lose from litigation if they cannot settle the matter in the knowledge that the details will stay private.

For financial services firms, new rules from September 1, 2026 will address **non-financial misconduct by regulated employees.** Any act of bullying, harassment or violence by an employee will have to be treated by the firm as a potential breach of the Financial Conduct Authority (FCA) Conduct Rules. The FCA may also introduce further guidance on how non-financial misconduct (including outside work) should be approached when assessing whether an employee should be permitted to continue their work in a regulated environment.

Pay reporting and transparency

Expansion of UK pay reporting requirements

Employers operating in the U.K. with 250 or more employees are required to report annually on their gender pay gap figures. From 2027, employers will also be required to publish an action plan setting out how they plan to reduce their gender pay gap, with these plans being recommended on a voluntary basis from April 2026.

In future, the U.K. government will be extending the gender pay gap reporting requirements to cover **disability and ethnicity pay gap reporting** (likely from 2027, although not confirmed). In addition to reporting the pay gap figures, it is proposed employers would be required to report on the overall breakdown of their workforce by disability and ethnicity, as well as the percentage of employees not disclosing their personal data for these characteristics.

Whilst it is common for employers to hold gender data which can be linked with pay, this is not always the case for data about ethnicity and disability, which, if it is collected at all, is often done so anonymously. In preparation for the new reporting requirements employers will need to review the data they already hold and assess what additional information they need to collect to calculate their ethnicity and disability pay gap, and how to do so in compliance with GDPR.

Pay equity remains a challenge in the United States, with persistent gaps across gender, race, and disability status. Women – especially women of color – and workers with disabilities continue to earn less on average, and protections vary widely without federal pay transparency requirements. Closing these gaps is essential to building fair, inclusive workplaces where all talent is valued and rewarded equitably.

EU pay transparency directive

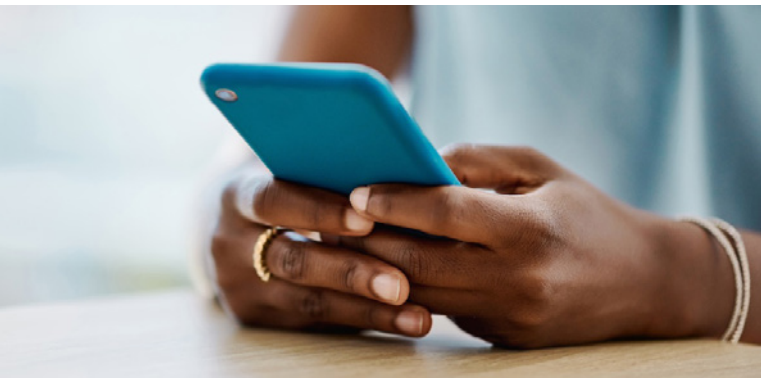
New gender pay gap reporting requirements will come into force in 2026 for businesses with EU operations, under the EU pay transparency directive, with timing and frequency of reports varying depending on the size of the employer:

- Employers with 250 or more workers will have to report gender pay gap figures from 2027 and annually thereafter
- Employers with 150-249 workers will have to report from 2027 and every three years thereafter
- Employers with 100-149 workers will have to report from no later than 2031 and then every three years thereafter

Individual EU countries may also choose to extend the reporting requirement to smaller employers (for example, Ireland is applying the rules to employers with 50 or more employees). Where the employer has a gender pay gap of 5% or more, which cannot be justified, the employer will be required to conduct a joint equal pay assessment with worker representatives.

There will also be new measures relating to **pay transparency in recruitment and promotion** including:

- A requirement to inform job applicants about the starting salary/pay before interview
- A ban on asking job candidates about their pay history
- A right for workers to ask employers for information about pay levels and pay and promotion criteria



Employers with EU operations should use the time ahead of implementation to prepare, including reviewing their pay structures and addressing any anomalies, considering pay data currently held and how any additional data will be collected.

Employers with EU operations should use the time ahead of implementation to prepare, including reviewing their pay structures and addressing any anomalies, considering pay data currently held and how any additional data will be collected. In addition, they should assess existing recruitment practices and the changes which may be required under the new pay transparency framework.

To prepare for growing pay transparency, U.S. employers should start by conducting regular pay equity reviews, standardizing compensation structures, and documenting clear criteria for hiring and promotion. Training managers to discuss pay openly and aligning internal policies with emerging state requirements will also be essential. Ultimately, readiness comes from embracing fairness and clarity in how pay decisions are made and communicated.

2026 prediction

Global employers will need to consider how to approach pay reporting, information and transparency across the different countries in which they operate. Although the EU requirements will only apply to employees in EU countries, many multi-national employers will want to aim for a consistent approach across all the jurisdictions in which they operate, from best practice and employee relations perspectives.

About the authors

Cindy Raz
Leading the HR and organization development functions, Cindy Raz, chief people officer, brings more than 20 years' experience leading human resources functions and business operations within rapid-growth organizations. Since joining NAVEX, Cindy has led several change initiatives associated with the merger and acquisition of multiple companies, including enhancing existing cultural programs, reducing undesired employee turnover and establishing people programs and strategies as a critical contribution to business success.

Cindy has been nominated for the Portland Business Journal's HR Leadership Award has served as a featured presenter at multiple industry events and is a featured HR Executive and Benefits Pro author. A graduate of Portland State University, she is certified as a senior certified professional with the Society for Human Resources Management and a senior professional in human resources with the Human Resources Certification Institute.

Ed Mills
Ed has significant experience of advising on whistleblowing compliance programs and conducting complex investigations, often involving whistleblowing disclosures and cross-border issues. In addition, Ed advises clients on a broad range of employment issues including board level disputes, team moves, discrimination, TUPE, collective consultation, trade union issues and litigation in the Employment Tribunal and the High Court. He also advises on business immigration issues including sponsorship under the UK Visas and Immigration 'points-based system'.

Ed is recognized by Chambers and Partners for his wide range of employment work and is listed as a 'Leading Individual.'

What's old is new again – 2026 presents new and enduring challenges in risk assessment

By Kyle Martin

The more things change, the more they remain the same. Every year, you look at your governance, risk and compliance (GRC) program with renewed optimism. This is the year you will figure it out. This is the year when things get easier. By December, you are left looking back on the shifting priorities that distracted your team, the new regulations where you had to quickly react, and the sense that January is right around the corner, so you can try again.

Of course, if this was simply an annual problem neatly mapped out against a calendar, maybe we could get there more easily. Rather, it's a continuous cycle that blurs the line between old and new challenges. GRC professionals experience a kind of imposter syndrome within the community where they feel constant obligation to use more automation, test the newest AI, review more data, comply with the newest framework, and yet so many have not mastered the fundamentals. How can we advance our programs if we don't have the foundation?

The GRC imposter syndrome – doing everything except the essentials

GRC imposter syndrome is the pervasive feeling among risk and compliance professionals that their programs must constantly evolve faster than everyone else's. This manifests within our business in several ways.

- **Chasing the coolest new acronym or AI tool instead of understanding basic ownership and accountability.** If your process doesn't work manually, it will not work automatically either. You can't skip to the finish line.
- **Your program focuses on proving maturity rather than informing action within the business.** The point of the risk assessment isn't to produce a dashboard. The point of the risk assessment is to understand uncertainty within the business and where mitigation is needed to achieve your business outcomes.
- **Benchmarking against peers instead of establishing your business's risk appetite and setting your risk tolerance, then aligning your risk activity to those specific attributes.** While the fundamentals of your GRC program might feel the same as everybody else's, this is where you get to put the finishing touches on your program that really make it work. How does our risk management process align to our priorities, not everybody else's?

Focus on outcomes over optics. Ask the question "so what?" You produced the coolest new heatmap, dashboard, risk quantification…so what? If your business doesn't have a clear next step with that data, it's time to go back to the basics and understand what you're doing to manage risk, not just report on it.

A significant aspect of GRC imposter syndrome is that GRC professionals are overwhelmed by getting started in the first place. An industry expectation is that you need to start

with this robust, perfectly managed risk register that is flawlessly mapped to mitigating controls. The truth is that almost nobody is there, and that the process of GRC should be continuous anyway. Wherever you are is great, and many of you didn't start with risks at all, did you?

Risk and Compliance: The chicken and the egg

What came first? Risk or Compliance? Most GRC professionals would tell you it should be Risk, and that seems to be a widely accepted practitioner outcome. However, starting with risk can be really challenging. You need to look at every angle, align risk with business outcomes, engage with every department, prioritize those issues. While risk in business is inherent, starting with risk is proactive in nature, and being proactive is hard.

Why can't we start with Compliance? After all, this is where a lot of companies are anyway. You had to comply with a regulatory requirement or an annual audit. Naturally, your risk register evolved from compliance gaps, and while it may not be as robust as the proactive risk management crowd, it's a practical starting point that was born out of necessity.

The truth is that Risk and Compliance are symbiotic in nature, and they grow together. When GRC professionals let perfection get in the way of progress, they ultimately don't move their program forward and skip the basics. Ultimately, we know this relationship isn't only necessary but it's improving. In our 2025 State of Risk & Compliance Report survey, 93% of respondents said compliance was at least engaged to some degree in the risk assessment and management process. As we said at the time, "It appears clear that collaboration between these functions is occurring, but the exact nature of that collaboration may be unsettled."

Survey insights and the state of 2026 – cracking the egg

Risk and Compliance can no longer evolve separately. At the end of the day, it doesn't matter how the egg got here – it's ready to hatch. Topics such as AI governance, data privacy, and ESG are shared concerns across the business, best led by an integrated risk and compliance vision. And when evaluating your GRC program, risk and compliance mature through proper governance.

In the same State of R&C survey, 70% of compliance teams were said to be highly engaged in risk assessment and management. However, only 24% believe their assessment process is effective. 2025 represented convergence without clarity. Functions are working together more, but not necessarily working effectively or efficiently. The connective tissue of the GRC program is still forming in so many organizations and most simply need to lean into that instead of running away or getting overwhelmed.

The real opportunity in 2026 is not about adding more AI or new dashboards, it's about doing the right things the right way. There is a clear shared purpose between risk and compliance that truly enables a proactive future that has seemed impossible in years past.

Setting the foundation for effective risk assessments

Establish the foundation of your program with three key questions. There is always more to expand upon, but in search of basic concepts, start here:

1. **What are our business's strategic objectives?** (Business can be replaced by department, program, product – any target in which you might be evaluating risk against.)
2. **What is our business's risk appetite?** Risk appetite is the amount and type of risk an organization is willing to accept to achieve strategic objectives. Risk appetite is typically stated in a qualitative manner and does not require a complicated process. It is meant to guide executive decision-making and overall prioritization.
3. **What is our business's risk tolerance?** Risk tolerance is the acceptable level of variation around the risk appetite. If your risk appetite is driving 65 mph, your risk tolerance might be 60-70 mph. If you find yourself going 80 mph, then you likely pursue corrective action and slow down.

> ***"An effective compliance program is one that evolves and improves over time."***
>
> **– United States Department of Justice Guidance of an Effective Compliance Program.**

Understand your governance framework – who owns the risk assessment and what are the different roles and responsibilities across the organization? This process should also include the "so what?" to your overall process. Why are you doing this assessment to begin with and what is the intended outcome? This will help you establish your scoring approach and the chicken and the egg of risk vs. compliance.

If starting with risk...

- What risks exist that could impede your strategic objectives?
- What stakeholders should contribute to that risk identification, if not explicitly called out in the governance framework?

If starting with compliance...

- What are the key controls to evaluate and where are there gaps?
- How effective is the control if it is in place?

Assign a disposition to each risk – then decide what to do...

- **Accept** (must be within our risk tolerance)
- **Mitigate** (ensure owner, timeline, and clear success metric)
- **Transfer** (typically insurance or outsourcing)
- **Avoid** (exit an activity, remove from scope)

Beyond the foundation, any solid risk assessment process has a clear understanding of reporting and continuous improvement. Once again – so what? We complete the assessment with a clear understanding of where we have gaps in our program. How do we fill those gaps and improve them systematically? And how do we make this process better next year?

"An effective compliance program is one that evolves and improves over time." – United States Department of Justice Guidance of an Effective Compliance Program.

Overcoming the GRC imposter trap

GRC maturity isn't driven by better processes, it's driven by culture. Effective programs are top-down in nature.

- Shift your mindset from doing everything, to doing the right things right. It's not about maturity models; it's about executing with excellence.
- Simplify your GRC program into practical steps with clearer outcomes. Fewer processes with more accountability and documented ownership. Evaluate the usage of AI for consistency rather than fixing broken manual processes.
- Imperfection is part of a healthy GRC culture. It's inevitable, but it doesn't have to be overwhelming. Find comfort in the uncomfortable and recognize it is all part of the journey.

The irony of 2026 is that the biggest breakthroughs in this industry won't come from AI or analytics, but rather from discipline and focus. If the 2026 version of our GRC programs has a theme, it should be humility. Getting back to the basics will be more impactful than any technological innovation. In the end, organizations that thrive will be those that stop pretending to be ahead.

2026 prediction

In 2026, we will see a significant influx of new GRC providers leading with agentic AI, solving very specific problems that are attractive to buyers. These disruptive providers will find themselves in at least 25% of deals by the second half of 2026. However, fewer than 10% will make it past initial stages of review as information security evaluation intensifies in this new era of GRC + AI. Fundamentally, the providers that can lead you through the basics will prevail.

About the author

Kyle Martin
Kyle Martin is an accomplished leader with over 14 years of experience in Compliance and Risk Management. Currently serving as the vice president of GRC Solutions at NAVEX, Kyle drives direction and execution of strategic initiatives for the organization. With a keen understanding of industry best practices and requirements, Kyle is instrumental in guiding NAVEX customers toward effective risk and compliance programs.

Signals show heightened stress on workplace cultures

Why civility, retaliation fears and imminent threats reveal the cultural risks compliance must address in 2026

By Sarah Jo Loveday

The health of workplace culture is often measured by how employees choose to raise concerns and whether they trust their organization enough to do so. The NAVEX 2025 Whistleblowing and Incident Management Benchmark Report and the companion Regional Report reveal that reports tied to *Workplace Civility*, namely behaviors that may not meet the threshold of harassment or discrimination but nonetheless corrode workplace culture, remain a major share of global reporting. At the same time, reports of *Imminent Threat to a Person, Animals or Property* have increased, underscoring rising tensions inside organizations.

As 2026 approaches, compliance and HR leaders face an urgent question: how to ensure employees feel safe reporting misconduct without fear of retaliation, while also addressing the cultural stressors that are producing both workplace civility concerns and reports of imminent threats.

The global rise of workplace civility concerns – a regional story

Workplace Civility encompasses reports of abusive or disrespectful behavior connected to work that don't constitute harassment or discrimination under legal definitions. Think of it as the daily erosion of respect, like bullying without protected-class implications, chronic undermining of colleagues or patterns of belittling behavior that poison team dynamics.

Globally, *Workplace Civility* represents the largest *Risk Type*. The 2025 NAVEX Whistleblowing & Incident Management Benchmark shows it accounted for a median 17.7% of reports in 2024, up from 15.8% in 2021. Though slightly down from 2023's peak (18.2%), the multi-year trend demonstrates employees are willing to call out behaviors that undermine respect and collegiality.

The regional data is even more telling. The 2025 Regional Benchmark Report found that *Workplace Civility* reports increased (by frequency) in every region except North America between 2023 and 2024. Europe, APAC and South America all saw stronger growth in this category, suggesting that outside of North America, maturing reporting cultures are surfacing a wider array of workplace issues once considered only "HR matters" rather than compliance issues.

The regional divergence is particularly significant. The increases in Europe, APAC and South America suggest maturing reporting cultures where employees increasingly recognize that these "soft" cultural issues warrant formal complaints.

This is significant as organizations expand globally, the data shows that employees in Europe, APAC and South America are reaching a cultural inflection point, treating civility and respect as matters of ethics and compliance and not just interpersonal disputes. That shift signals a maturation of reporting systems beyond North America.

Why *Workplace Civility* matters more than organizations think

Too many organizations dismiss *Workplace Conduct* issues, the category encompassing *Workplace Civility*, discrimination, harassment and retaliation, as "not a compliance issue". The data a demolishes this misconception.

Workplace Conduct (reports concerning employee relations or misconduct) **dominates reporting worldwide**. **Global** NAVEX data shows that in 2024, **54% of all reports** submitted through whistleblowing and incident management systems related to *Workplace Conduct*. The regional picture reinforces this trend. Looking at the *median reporting levels originated* in each region, at least half of all reports involved *Workplace Conduct*. In 2024, the median share was **50% in APAC, 66.7% in South America and 57.9% in Europe.**

Civility issues serve as an early warning system for cultural erosion. They highlight the "everyday frictions", including rudeness, disrespect or verbal abuse, left unchecked can escalate into formal harassment or discrimination cases.

The substantiation data becomes even more interesting when examining company ownership. Private organizations across all regions showed higher substantiation rates than public companies. In Europe, private companies substantiated 50% of reports versus 45% for public companies. APAC showed the same pattern – 50% private, 47% public. In South America, the gap was even more pronounced, with 67% of private company reports substantiated compared with just 43% in public firms.

This suggests privately held organizations either experience more straightforward misconduct or invest more thoroughly in investigations. Regardless, the message is clear. When organizations take misconduct seriously enough to investigate properly, they consistently find problems.

When workplace civility breaks down, broader compliance suffers. Employees who experience or witness chronic disrespect become less likely to speak up about other misconduct. The connection between day-to-day cultural toxicity and major compliance failures is well-documented and it shows that when people don't feel psychologically safe, they stay silent about fraud, safety violations and ethical breaches.

The retaliation paradox – regional disparities reveal investigation gaps

If civility concerns mark the early tremors of workplace stress, retaliation reports represent the fault line. While relatively small in number, the median rate of retaliation reporting has steadily increased from 2.43% in 2021 to 2.84% in 2023 and 3.08% in 2024. Retaliation carries an outsized cultural risk. According to the NAVEX Whistleblowing & Incident Management Benchmark Report, when employees believe retaliation is likely, they may stop reporting altogether.

The problem is two-fold. First, retaliation reports have shown a consistently low *Substantiation Rate* over several years, with only 18% being substantiated globally in 2024. Second, regional disparities compound the issue. Retaliation cases for organizations in Europe are substantiated 32% of the time, nearly double the rate in North America (17%), according to data from the regional benchmark report. APAC has a substantiation rate of 28%. This suggests both investigative rigor and cultural perceptions of retaliation differ dramatically across regions.

The *Case Closure Time* data adds another dimension to this concern. Globally, the median *Case Closure Time* for Retaliation cases increased from 28 days in 2023 to 32 days in 2024.

For compliance leaders, the challenge isn't just preventing actual retaliation but also addressing the fear of retaliation. Both real and imagined consequences matter. For younger generations entering the workforce in 2026, this gap between real and feared retaliation will matter even more. Gen Z employees, in particular, are both more vocal about fairness and less tolerant of opaque processes. They expect transparency, accountability and authenticity from their employers. If organizations cannot convincingly show that retaliation is rare, taken seriously and promptly addressed, younger workers may either remain silent about misconduct or exit the organization altogether.

Understanding fear versus reality across cultures in the context of retaliation

Anonymous reporting rates among employees are consistently higher outside North America, though they vary depending on whether measured by headquarters or report origination. In Europe, a median 65% of employee reports were anonymous by headquarters in 2024, compared with 50% by report origination. APAC showed 67% by headquarters and 60% by origination. South America registered the highest levels, with 70% by headquarters and 67% by origination. Globally, the median stood at 57%, according to the Regional Benchmark Report.

For compliance leaders, the challenge isn't just preventing actual retaliation but also addressing the fear of retaliation. Both real and imagined consequences matter.

These patterns reflect cultural attitudes toward authority and workplace hierarchy. Higher anonymity in Europe, APAC and South America suggests greater fear of being identified, whether from concern over retaliation or norms that discourage direct confrontation. Effectively, the rate of anonymity is a proxy measure for fear and trust which means the more people choose anonymous reporting, the less confidence they have that naming themselves won't carry negative consequences.

The follow-up rate to anonymous engagement offers another insight. The global median follow-up rate to anonymous reports fell to 26% in 2024, down from 36% in 2019. Organizations in APAC (33%) and South America (29%) show relatively stronger follow-up with anonymous reporters, while Europe lagged slightly behind those regions at 34%, highlighting regional differences in how organizations sustain communication with those who report anonymously. This suggests organizations in these regions recognize the cultural barriers to named reporting and invest more in sustaining communication with anonymous reporters.

Taken together, the data indicates that outside North America, employees' fears of retaliation, whether real or imagined, manifest in higher reliance on anonymous channels. Compliance programs that proactively engage these reporters, rather than dismiss anonymous reports as less credible, will be better positioned to build trust and encourage reporting in 2026.

The grim reality of imminent threat reports

Perhaps the starkest signal of workplace stress in NAVEX data is the rise in reports of *Imminent Threat to a Person, Animals or Property*. These reports grew from a median **1.29% of all cases in 2023 to 1.53% in 2024**. While still a small share overall, the figure is deeply concerning because these cases can carry life-or-death implications and because they are substantiated at an extraordinary **90% rate**.

That level of confirmation underscores two things. First, employees do not raise "imminent threat" concerns casually. They are almost always grounded in real, observable danger. Second, the rise reflects more than just isolated incidents. It signals escalating stress, conflict and instability inside workplaces.

When unresolved civility issues, harassment or interpersonal tensions are left unaddressed, they can spiral into situations where employees fear actual harm. In this sense, imminent threat reports are not just about security or safety. They are a cultural indicator that trust has broken down, tensions have gone unmanaged, and the workplace no longer feels safe either physically or psychologically.

For compliance leaders, this means imminent threat cases must be treated as both a safety risk and a culture signal. Programs should coordinate closely with HR, security and employee wellness functions not only to respond swiftly to immediate dangers but also to identify and address the underlying workplace stressors driving these reports.

When unresolved civility issues, harassment or interpersonal tensions are left unaddressed, they can spiral into situations where employees fear actual harm.

How compliance can lead in 2026

Taken together, the data tells a story of workplaces under strain. Employees are raising concerns about civility and more often feel on edge, as shown by the rise of imminent threat cases. Yet, fears of retaliation still suppress reporting, particularly in regions where substantiation lags.

To address these challenges, compliance programs should:

- **Elevate *Workplace Civility* as a strategic compliance priority.** Treat *Workplace Civility* reports as a frontline compliance issue. Train managers that disrespectful behavior isn't just unpleasant. It's a compliance risk that erodes the psychological safety required for effective reporting. Track *Workplace Civility* reports by department and manager to identify toxic areas requiring intervention, investigate consistently and use findings to inform action plans.
- **Reinforce anti-retaliation protections.** Make policies visible, enforce them consistently and communicate outcomes. Transparency is key to reducing perceived retaliation and giving employees confidence that raising concerns will not backfire.

- **Adapt to regional maturity.** Recognize that reporting cultures vary across Europe, APAC, North America and South America. In these regions, civility reports are increasing as employees test the system and gauge whether their concerns will be taken seriously. Compliance should tailor messaging and follow-up engagement to local expectations, ensuring employees feel heard regardless of whether they report anonymously or openly.
- **Integrate imminent threat protocols.** With substantiation so high, organizations should establish rapid response teams that bridge compliance, HR and safety/security.
- **Track all intake methods holistically.** Employees use multiple channels in significant proportions. For example, in Europe 12% of reports came through phone in 2024, 56% web and 32% other channels. APAC showed 7% phone, 61% web and 32% other tools, South America 17% phone, 63% web and 20% other channels. Each region has distinct preferences, so ensure all channels are resourced and monitored.
- **Watch for escalation patterns.** The link between civility breakdown and rising imminent threat reports is clear. In 2024, the median-of-medians case data shows employees typically waited eight days between an incident and reporting it. While that's relatively fast, it still leaves time for harm to escalate, highlighting why early action on civility issues is critical to preventing more serious threats.
- **Prioritize timely resolution.** In 2024, the global median case closure time was just 21 days, but for reports made to organizations in Europe, APAC and South America it stretched to 69, 56 and 48 days respectively. Long delays not only prolong risk but also undermine employee confidence in the system.

2026 prediction

As 2026 approaches, workplace reporting data shows cultures under heightened stress. Civility concerns are rising globally, imminent threats are climbing and retaliation remains both a real and perceived barrier to trust. Compliance leaders who take these signals seriously by treating civility as compliance, addressing retaliation head-on and building rapid responses to imminent threats will help their organizations move from reactive risk management to proactive culture building.

If 2024 and 2025 represent the "new normal", then 2026 may be the year when employees' willingness to speak up defines whether workplaces grow more resilient or more fractured.

About the author

Sarah Jo Loveday
Sarah is the founder and managing director of Peopleknd., an HR consultancy based in London, specializing in various HR and people & culture matters, including employment law, performance management, people strategies, ED&I, staff engagement, HR policies & procedures, recruitment & selection, restructuring & redundancy, workforce planning, and organizational development.

Contributing to thought leadership in HR, Sarah Jo authors the HR column for the London Chamber of Commerce and Industry's Business Magazine. Sarah Jo studied Human Resources Management and Industrial Relations (MSc) at Alliance Manchester Business School (2012) and People Analytics at the University of Cambridge (2022). She is a keen supporter of inclusive entrepreneurship and female entrepreneurs.

The expanding role of the board of directors in compliance

By Rebecca Walker

Robust oversight of the compliance program by a company's board of directors makes a meaningful – and often critical – difference. Boards can provide chief compliance officers (CCOs) with the independence and authority required for an effective program. It is not uncommon to see faltering programs that regain their footing when guided by an engaged audit committee chair, or, conversely, wither because the board failed to act when the CCO needed support.

Over the past two decades, progress in board oversight of compliance programs has been substantial. Many boards now view compliance not as a legal formality but as a central pillar of governance. Yet, even with that progress, there is still significant room to grow.

In 2026, regulators, investors, and employees alike expect boards to do more than simply be the recipients of a quarterly report on hotline activity. There is now an expectation that boards actively oversee the compliance program and the company's reporting and response systems. The very best boards, however, go further still. They use their oversight role to help shape an organization's ethical culture. Boards can set the expectation for integrity, accountability and transparency. When that expectation is clear, the effect cascades across the enterprise, shaping management priorities, influencing employee behavior, and building enduring organizational values.

Many boards now view compliance not as a legal formality but as a central pillar of governance.

Legal expectations

The elevation of compliance oversight at the board level is reinforced by both legal precedent and regulatory guidance. A line of Delaware cases (*Caremark* in 1996, *Marchand v. Barnhill* in 2019, and *In re Boeing Company Derivative Litigation* in 2021) underscores directors' duty to oversee compliance systems. These decisions make clear that boards have a fiduciary obligation to ensure:

- Mechanisms exist in an organization to identify and escalate red flags
- Compliance systems and internal controls are in place
- Controls exist in mission-critical risk areas

Regulators echo this expectation. The U.S. Department of Justice's *Evaluation of Corporate Compliance Programs* (ECCP) highlights the importance of board-level access for CCOs and timely escalation of significant issues. The ECCP asks whether Compliance has direct reporting to the board; how frequently the CCO meets with directors; whether the board holds executive sessions with Compliance; and what information the board actually examines in their exercise of oversight. The memorandum also recognizes that the CCO's direct access to the board facilitates an appropriate level of autonomy. The DOJ has emphasized that effective oversight is not solely structural; it depends on the board's informed involvement in risk discussions and in the program more generally.

Together, these legal expectations set a clear standard: boards must not only receive compliance information but use it to exercise active, documented oversight. Because the board of directors is the highest governing authority, its support has far-reaching consequences. While a company can *have* an E&C program without board support, it cannot – by definition – have an *effective* program without it. And when senior leadership's support is uneven, board support becomes even more essential.

What the data shows

While most large organizations now have formal mechanisms for board oversight of compliance, recent NAVEX benchmarking data suggests there is still significant room for improvement. In the 2025 State of Risk & Compliance Report – which surveyed nearly 1,000 risk and compliance professionals:

- 64% said their boards receive periodic compliance reports, which is below expected and essentially unchanged from 2024 findings (66%)
- Only 52% said their boards have formal oversight of the compliance program
- 43% said their boards include members with compliance experience or expertise
- Only 37% reported that boards hold executive or private sessions with compliance
- Only 33% reported that their boards are "highly engaged"

These figures undoubtedly represent meaningful progress compared to a decade ago, but they also point to significant opportunity for improvement.

The data also reveal a clear maturity gap. Among organizations with more developed compliance programs, half reported that their boards have compliance expertise, 43% said they hold private sessions, and 39% described their boards as highly engaged, much greater levels than indicated for the least mature organizations.

The board's engagement contributes not only to greater independence and authority for the CCO, but also more engaged leadership support. The link between governance and performance is no longer theoretical – it is measurable.

Why board oversight matters

Board engagement matters not just to meet regulatory expectations, but because it strengthens both the compliance program and the organization's culture. Boards that actively oversee compliance programs help create an environment in which management models ethical conduct under pressure.

The 2025 State of Risk & Compliance Report revealed a critical connection between board oversight and leadership support of compliance programs. When there is above average board engagement in a program, management behaviors – from senior leadership, all the way down to first-line managers – are significantly more supportive of compliance. In other words, the board's engagement contributes not only to greater independence and authority for the CCO, but also more engaged leadership support. The link between governance and performance is no longer theoretical – it is measurable.

Characteristics of strong board/ Compliance relationships

Across industries, several common practices distinguish organizations where effective board oversight meaningfully advances the compliance program.

Clarity of oversight: Effective boards have defined responsibilities for compliance oversight – often captured in the charter of the oversight committee as well as in the compliance program charter – and receive regular reports on program performance and risk trends. Board reporting should be live, as well as written. This ensures consistency and prevents oversight from becoming diffuse or episodic.

CCO access to the board: The CCO must have unfiltered access to the board or its designated committee, including regularly scheduled executive sessions. These discussions reinforce independence and build trust between the board and compliance leadership.

Values and culture: Sophisticated boards understand that C&E programs are about far more than compliance. They help create a culture of integrity, where doing the right thing (including acting in compliance with law and policy) is simply expected. These boards understand that culture is the single greatest driver of ethical behavior and that the compliance function plays a central role in supporting and measuring culture.

Visible support for ethical leadership: The board plays a critical role in setting the tone at the top of an organization when they emphasize the importance of creating a culture of integrity. As noted earlier, NAVEX research shows that organizations with more active board oversight report stronger ethical leadership behaviors at the managerial level – reinforcing the link between governance and culture.

Integration into risk governance: Effective boards view compliance not as a silo but as part of the organization's risk governance framework, informing board discussions about emerging technologies, supply chain integrity and other strategic areas.

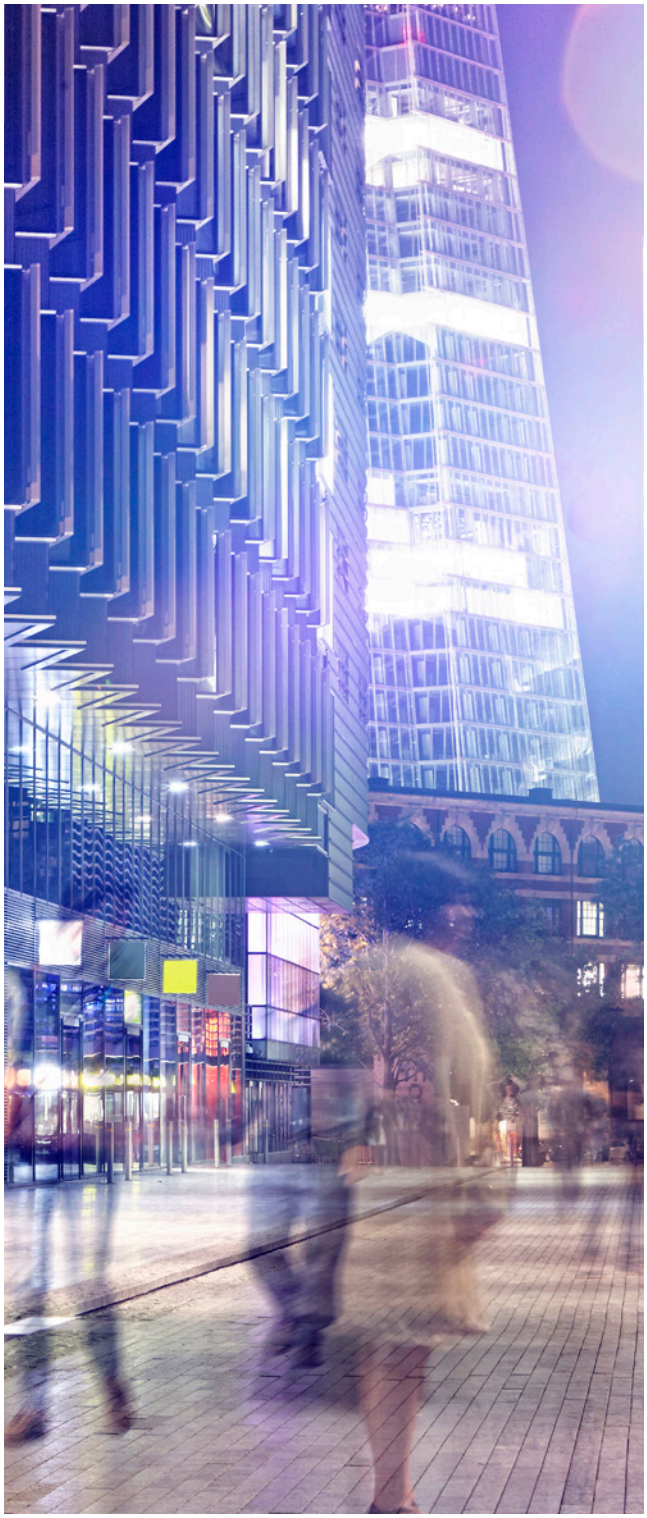
Data-driven oversight: Boards increasingly expect to see not only summaries of program activity but also trend data – including hotline metrics, investigation outcomes, training completion and culture survey results, but extending to data analytics of business performance, procurement information, gifts and entertainment, and conflicts of interest, among other areas. The focus has shifted from "what compliance did" to "what the data reveals."

From oversight to insight

The most advanced organizations have moved beyond viewing compliance reports as backward-looking summaries. Instead, they treat the board/compliance dialogue as a forward-looking discussion about risk, opportunity and culture.

This shift is partly a function of data analytics and technology, which now allow compliance teams to deliver timely insights rather than static reports. But it is also a matter of mindset. Boards that ask probing questions about topics such as the root causes of misconduct, the effectiveness of training or the implications of new business strategies signal that compliance is integral to performance.

This dynamic partnership changes how decisions are made. Ethical considerations enter earlier into strategic planning, and compliance leaders are viewed as contributors to value creation rather than custodians of policy adherence.



Practical steps for 2026

Organizations seeking to strengthen the alignment between boards and compliance can take several practical steps:

- Revisit charters and escalation protocols. Document the board's oversight role and the CCO's access.
- Schedule regular executive sessions. Regularly scheduled time for discussion with the CCO, separate from management. In addition, consider periodic pre-meetings or informal check-ins between the CCO and the committee chair to reinforce the relationship.
- Enhance information quality. Replace static reporting with dashboards and analysis that highlight trends, root causes, and potential systemic risks.
- Invest in director education. Provide training that links compliance oversight to fiduciary duties and emerging risks such as AI and supply chain integrity.
- Assess culture and speak-up health. Encourage the board to review culture metrics, hotline data, and survey insights as part of regular oversight.
- Benchmark and reassess. Use tools such as NAVEX benchmarking data to evaluate how the organization's oversight practices compare to peers and to identify gaps and track progress.
- These measures not only strengthen compliance governance but also protect directors and senior leaders by ensuring that oversight responsibilities are demonstrably fulfilled.

2026 prediction

The coming year will see boards and Compliance continue to converge. As regulatory expectations expand and stakeholder scrutiny intensifies, boards will evolve from periodic overseers to more continuous partners with compliance leaders. Organizations that invest now in building this alignment will stand out not only for their ethical cultures but also for their resilience in navigating complex global risks. The next frontier of compliance excellence will be defined in part by how effectively boards and compliance officers shape the organization's culture. For many organizations, the boardroom will be not just where strategic decisions are deliberated, but also where ethical culture is nurtured.

About the author

Rebecca Walker

Rebecca Walker is a partner in the Santa Monica, California office of Kaplan & Walker LLP, a law firm that counsels organizations on the development, implementation and enhancement of compliance and ethics programs. Rebecca specializes in compliance and ethics law and assists organizations in structuring their programs, revising codes of conduct and other related policies. She has conducted numerous assessments of compliance and ethics programs and has served as a monitor for the Department of the Air Force and consulted with the U.S. Securities and Exchange Commission. Rebecca is the author of Conflicts of Interest in Business and the Professions: Law and Compliance, as well as a number of other compliance surveys and published articles. Rebecca received her B.A. from Georgetown University and her J.D. from Harvard Law School.

Fundamentals that won't change amid 2026's regulatory headwinds

By Sidney Bashago and Daniel Kahn

While regulatory turbulence is always a challenge, 2026 may represent an especially notable year given political changes in key international markets. Although compliance programs will need to prepare and adapt to changing winds, the fundamentals of building an effective program remain the same.

This article addresses the major global shifts driving a changing landscape for compliance programs, some factors that are likely to change in 2026, and the fundamental aspects of an effective compliance program that will not change.

Although compliance programs will need to prepare and adapt to changing winds, the fundamentals of building an effective program remain the same.

Changing landscape

With every new United States administration, there are shifts in priorities, including in corporate and regulatory enforcement. This past year is no exception, there have been several significant policy changes and priority shifts.

For example, in June of 2025, the U.S. Department of Justice (DOJ) announced new guidance regarding enforcement of the Foreign Corrupt Practices Act (FCPA) in response to President Trump's executive order pausing FCPA enforcement pending the release of this new guidance. The guidance sets out four non-exhaustive areas of focus for FCPA investigations or enforcement actions where bribery negatively impacts U.S. interests:

1. Cases involving cartels and transnational criminal organizations (TCOs), even if indirectly or tangentially
2. Bribes paid in connection with a bid involving a U.S. company (regardless of whether the bribe-paying company is American)
3. Cases involving U.S. national security interests, including corruption in sectors such as defense, intelligence and critical infrastructure
4. Alleged misconduct that bears strong indicia of corrupt intent, rather than conduct that involves routine business practices or low-dollar, generally accepted business courtesies

While the new administration is narrowing the focus of FCPA enforcement, it is expanding into areas that were not priorities in the last administration, including trade and customs fraud (including tariff evasion), immigration, diversity, equity and inclusion programs, and the elimination of cartels and TCOs. Other areas of enforcement, such as antitrust, healthcare fraud and sanctions, remain priorities across administrations.

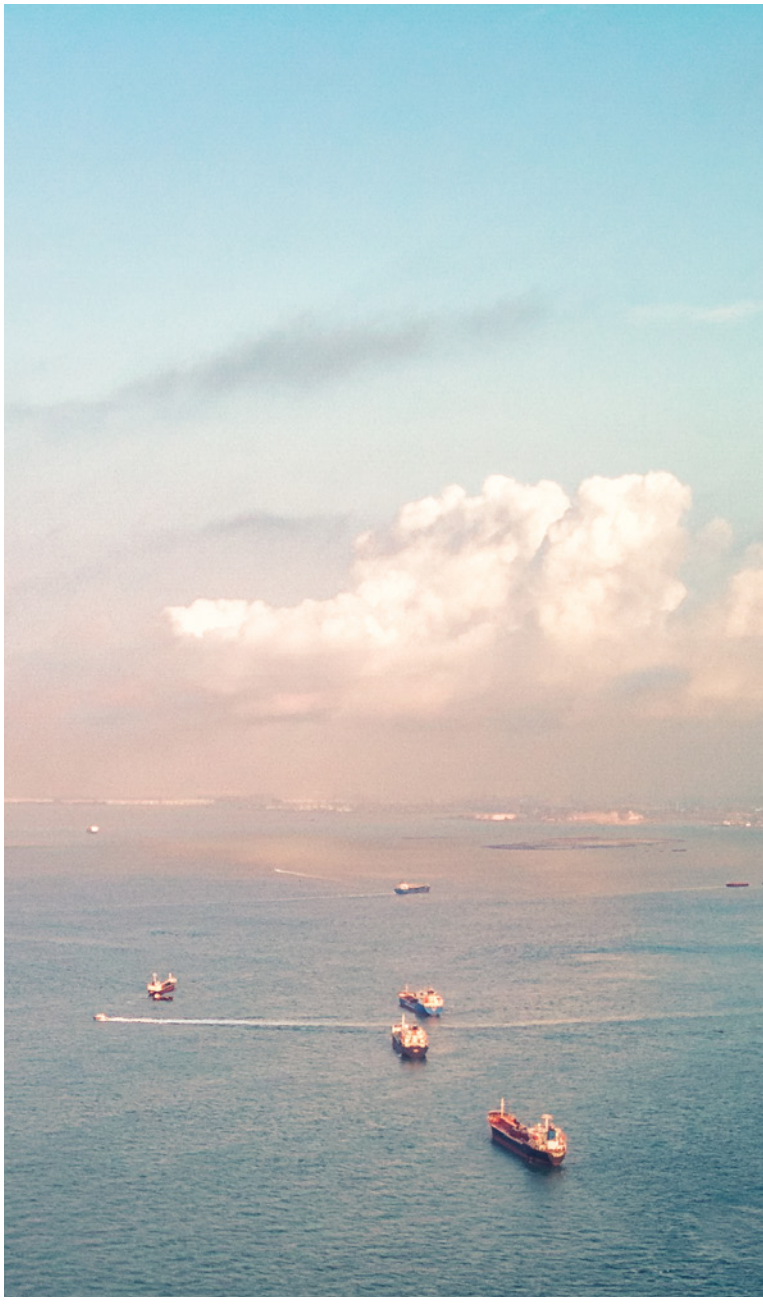
More broadly, DOJ has announced new enforcement policies intended to encourage companies to voluntarily disclose misconduct and cooperate with DOJ investigations. Among the most important policy changes, DOJ simplified and amended its Corporate Enforcement Policy (CEP), a policy that was initially formalized in the first Trump administration, to further encourage self-disclosure of corporate misconduct.

The revisions to the CEP highlight the benefits of self-disclosure, building on incentives established by prior iterations of the CEP, including those revised under prior administrations. Whereas DOJ's prior policy created a presumption of a declination for companies that voluntarily self-disclose misconduct, fully cooperate and make timely and appropriate remediations, in the absence of aggravating circumstances, the new policy requires a declination in those circumstances.

In addition, during the last administration, DOJ created burdensome requirements to achieve a declination when aggravating circumstances (such as participation by senior executives) were present. In such cases, the company was required to disclose "immediately," provide "extraordinary" cooperation and remediation, and have had an effective preexisting compliance program at the time of the misconduct. This high standard was difficult to meet, left considerable discretion to prosecutors, and seemed to create a disincentive for companies to voluntarily disclose misconduct. The new policy revisions in June of 2025 eliminated these requirements, and made clear that, in the face of aggravating circumstances, "prosecutors retain the discretion to nonetheless recommend a CEP declination based on weighing the severity of those circumstances and the company's cooperation and remediation."

Another notable revision establishes a specific approach for "near miss" voluntary self-disclosures, for example where DOJ was already aware of the misconduct when the company disclosed, but the company otherwise meets the CEP requirements. In such circumstances, the Criminal Division shall resolve through a non-prosecution agreement (NPA), shall not impose a monitor, shall provide a 75% reduction of the fine, and can limit the term of the NPA to less than the standard three years.

DOJ also indicated that it would use independent compliance monitors in fewer cases, and would ensure monitors that are imposed stay within their mandate and cost less. DOJ outlined several examples, including a cap on the monitor's hourly rates, budgets for all monitor workplans, which the monitor may not exceed without DOJ permission, and at least biannual meetings between DOJ, the monitor, and the company.



For its part, the U.S. Securities and Exchange Commission (SEC) has trumpeted a more traditional approach to enforcement, turning its focus away from novel theories of liability and an acute focus on cryptocurrency, and instead focusing on more traditional violations of the securities laws, including fraud on investors.

Taken together, these policy announcements are likely to create a much more favorable environment for corporations to voluntarily disclose misconduct and to achieve more lenient results based on good corporate behavior.

DOJ and SEC, however, are also continuing to pursue methods of identifying corporate misconduct, thereby emphasizing the "stick" side of the equation in addition to the "carrot." While the SEC's whistleblower program has been in place for well over a decade now, DOJ only began a whistleblower pilot program in August of 2024. Yet the new administration seems intent on maintaining it. In fact, DOJ updated the program to make whistleblowers eligible for an award if they report misconduct in four new areas that align with its priorities:

1. Procurement and federal program fraud
2. Trade, tariff, and customs fraud
3. Violations of federal immigration law
4. Violations involving sanctions, material support of foreign terrorist organizations, or those that facilitate cartels and TCOs, including money laundering, narcotics, and Controlled Substances Act violations

Looking ahead to 2026

We should begin to see how DOJ will implement the new version of the CEP, and how companies that have voluntarily disclosed misconduct will be treated. These will all have significant impacts on corporate decision-making in the face of allegations of misconduct.

For example, if DOJ exercises its discretion to award companies CEP declinations even in the face of aggravating circumstances (such as executive-level involvement), and that such determinations are made within a short period of time (e.g., 6-12 months as opposed to 3-4 years), companies will be much more willing to voluntarily self-disclose misconduct when they identify it. We will also begin to see whether coordination and cooperation with foreign governments – something that has been a hallmark of corporate enforcement over the past several administrations – will continue apace or begin to slow. This would have a significant impact on corporate investigations and prosecutions, and in turn on corporations facing regulatory scrutiny.

With the evolving policies and priorities, now would be a good time to conduct a risk assessment to ensure the compliance program is designed to address some of the newer priorities, including risks posed by trade/customs fraud, diversity, equity and inclusion programs, and cartels and TCOs.

Fundamental and unchanging aspects of a compliance program

Although there have been significant changes to the enforcement landscape, an effective compliance program remains a critical way to address the changing environment. With the evolving policies and priorities, now would be a good time to conduct a risk assessment to ensure the compliance program is designed to address some of the newer priorities, including risks posed by trade/customs fraud, diversity, equity and inclusion programs, and cartels and TCOs.

As has been the case across administrations, it is also critical to ensure companies have sufficient controls around third-party interactions, including risk-based due diligence and monitoring and auditing of payments and activity. To the extent that a company is exposed to trade/customs fraud or cartel and TCO risks, it is likely third-party relationships are where that risk exists (or at least is the highest).

Finally, although the priorities are shifting, it is also important not to ignore areas that pose risks to a particular company, even if those risks are not priorities

of the administration. For example, even though FCPA enforcement appears not to be a high priority for the administration, companies would be wise not to de-emphasize anti-corruption compliance. As an initial matter, the new FCPA guidance suggests that DOJ and SEC will still remain active in this space. Moreover, corruption may violate laws in other countries that do remain active. France, the U.K. and Switzerland have announced a joint task force to investigate and prosecute foreign bribery. Finally, the statute of limitations for FCPA violations are five years for anti-bribery violations and six years for accounting violations, and DOJ has methods of extending the statute of limitations for several years.

2026 prediction

While this past year made clear what the administration's regulatory and enforcement priorities would be, 2026 should demonstrate how the government intends to carry out those priorities. As DOJ's and SEC's policies become clear, enforcers are then able to turn to carrying out the day-to-day job of investigating and prosecuting violations of law that are clear priorities.

About the authors

Sidney Bashago
Sidney represents companies, boards and individuals in critical situations, including when they are facing scrutiny by the DOJ, SEC, CFTC and other criminal and regulatory authorities. She also advises companies and boards on governance and compliance. Her clients include companies across industries including healthcare, technology, telecommunications, consumer products, media and mining and metals, as well as financial institutions, hedge funds, cryptocurrency companies and private equity firms.

Sidney has extensive experience in anti-corruption matters, as well as in matters involving allegations of securities fraud, whistleblower protection regulation violations, market manipulation, money laundering and other financial crimes. She has secured numerous declinations and favorable resolutions in these matters over her time at the firm. Sidney regularly advises clients on the design of and enhancements to their anticorruption compliance programs. She is a frequent panelist at both domestic and international conferences on anti-corruption.

Sidney has also represented multinational companies, boards and other entities on various critical workplace misconduct matters, including highly sensitive sexual misconduct investigations, proactive assessments, crisis management and related compliance.

Daniel Kahn
Daniel Kahn is a former senior DOJ official with more than two decades of experience in criminal and regulatory investigations and headed DOJ's Fraud Section and FCPA Unit. He represents companies and individuals in government enforcement matters, conducting internal investigations and in compliance matters, and has secured numerous favorable resolutions for clients with various enforcement authorities.

Dan is ranked in Band 1 for his FCPA work by Chambers, which also recognizes him for White-Collar Crime & Government Investigations. The Wall Street Journal described Dan as DOJ's "most recognizable expert on the Foreign Corrupt Practices Act." At DOJ, Dan was acting Deputy Assistant Attorney General of the Criminal Division and Chief of the Fraud Section, and Chief of the FCPA Unit, and supervised matters involving the FCPA, money laundering, and commodities, securities, healthcare and procurement fraud.

At DOJ, Dan played a central role in developing enforcement policies on the FCPA, corporate enforcement, compliance and monitors. He worked with authorities around the world, and tried a number of cases to verdict. Dan co-authored a treatise on corporate criminal investigations, and teaches Corporate Criminal Investigations at Harvard Law School and Global Anti-Corruption at Georgetown Law Center.

Looking back, moving forward: a 15-year journey in whistleblowing and incident management benchmarking – what's next?

By Carrie Penman

Our Whistleblowing & Incident Management Benchmark Report turned 15 this year! As our teams of experts, data scientists and researchers explored the latest numbers, we realized how far we've come since those early days. What started as a small research project to see if we could measure internal reporting trends has now grown into the world's largest collection of reporting data by far, with over two million reports from around the globe analyzed annually. That's a lot of insights and board reports – and even more stories to tell.

Much has changed since our first reports. Our customer base has grown internationally and we are now able to provide an increasingly meaningful view of global trends in internal reporting. Much of what we've seen over these years is very positive. The embrace of internal reporting programs continues to grow around the world.

Yet much has stayed the same. The underlying risks organizations face when individuals feel disempowered in reporting misconduct endure. While many of our observed metrics reflect progress, in some cases, we hoped to see more. That's why 2026 is shaping up to be a pivotal year: organizations that truly support a culture of transparency and "speaking up" will have the edge as employees expect solid internal reporting systems everywhere they go.

Our hope in sharing this free research each year is simple: we want to help everyone evolve and mature their program and we believe these metrics help "lift all boats." The more employees trust their internal reporting programs, the stronger their cultures of ethics and compliance become. Hitting the 15-year mark – and publishing this Top 10 Trends in Risk & Compliance Report – felt like the perfect time to reflect back and look ahead. So, what do the numbers tell us about getting ready for 2026?

Predictions for 2026: what's on the horizon?

Internal reporting is here to stay

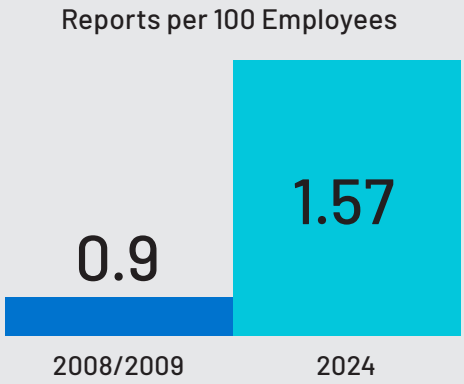
More than 80% of professionals surveyed globally for our 2025 State of Risk & Compliance Report said employees were most likely to make a report internally versus to an external entity (or simply to not make a report in the first place). This is remarkable validation for the embrace of internal reporting programs as cited by nearly 1,000 practitioners in compliance, risk, legal, human resources and other related fields.

Our long-term customer internal reporting data also shows the embrace of internal reporting programs is only increasing. In 2008/2009, organizations received a median 0.9 *Reports per 100 Employees*. Our latest report, which examines data from 2024, found a global median of 1.57 *Reports per 100 Employees*. That's nearly a 75% increase in reporting levels.

Often, reporters simply want to see a problem fixed and they want their management team to handle it. This is despite some instances when the whistleblower programs of external entities such as the United States Securities and Exchange Commission may offer incentives – monetary rewards – for certain substantiated cases. Reporters continue to see internal reporting programs as the go-to channel to most efficiently raise and address concerns.

These increasingly engaged reporters will also expect results. Median *Case Closure Time* has decreased from 32 days in 2009 to 21 days in 2024 – reporters in 2026 will be more likely to consider these sorts of metrics to be "the norm," and organizations falling behind these trends will find themselves challenged to engage employees in embracing a culture of ethics and trust in internal reporting.

In 2008/2009, organizations received a median 0.9 Reports per 100 Employees. Our latest report, which examines data from 2024, found a global median of 1.57 Reports per 100 Employees.



What does this mean for 2026? While our data suggests the possibility that internal reporting rates may be reaching a plateau, they have increased quite substantially in the long term. Employees and third parties will increasingly expect organizations to have robust channels through which to report misconduct and make inquiries without fear of retaliation. And where those channels fall short, employees – along with customers, regulators and others – will notice.

Be prepared for more reports of retaliation

Allegations of retaliation carry special weight among the categories of misconduct and should be tracked, managed and reported with special attention. Retaliation for making a report – or simply the fear of it – disincentivizes reporting in the first place. Misconduct goes unrecognized and unmitigated. Risk grows, perhaps unknown to those who manage it. Employees lose trust that their organization will do the right thing.

Thankfully, reporters are speaking out a bit more about retaliation. In 2009, 0.62% of all reports pertained to retaliation. In 2024, the median share was 3.08%. That said, research done by the Ethics and Compliance Initiative has shown that far more employees say they have experienced retaliation than those who report it. Organizations should not assume that few reports of retaliation mean it isn't happening and need to take proactive steps to prevent and detect it.

Of particular concern, the *Substantiation Rate* for retaliation reports lags far behind overall *Substantiation Rate*, but it is improving ever so slightly. In 2009, median *Substantiation Rate* for retaliation reports was 11%. It reached a high point of 27% in 2014 but has been below 20% ever since. Noting that the overall *Substantiation Rate* for all cases in 2024 was 46%, there is much more work to do to better identify and resolve retaliation cases.

In perhaps our most shocking finding this past year, approximately 45% of substantiated retaliation cases did not result in discipline or employment separation – and almost 14% resulted in no action. Lack of response to validated retaliation reports transfers non-retaliation policies to the paper program list.

In 2026, organizations need to foster better understanding of a no-tolerance policy for retaliation. Our industry has spent decades pressing this point, and after long efforts, employees are starting to come to the table ready to call out retaliation. Organizations without clear policies, messaging, and action around anti-retaliation in 2026 will fall behind.

Report quality is going up

It's surprising to consider the overall *Substantiation Rate* was at a median 29% in 2009, and in 2024, 46%, as noted above. This is a huge improvement, and the latest in a long-term, generally upward trend. It may be safe to assume organizations are doing a better job educating potential reporters about what constitutes actual misconduct and inviting more context to inform quality investigations.

For 2026, the bar will be set even higher. Companies need to offer more in-depth training, easy access to policies, and ongoing reinforcement of their values to keep improving the quality of reports they receive. Reporters are starting to expect this level of support—and may hesitate to step forward if it's not there.

'Workplace Civility' is getting noticed

While representing a relatively newer category of misconduct for the purpose of NAVEX analysis, the *Workplace Civility* category – reports related to abusive or disrespectful behavior connected to work that are not harassment or discrimination – is becoming a key risk area. As explored elsewhere in this Top 10 Trends in Risk & Compliance Report, this is another misconduct category (or, in our words, *Risk Type*) worthy of special note as an indicator of the hard-to-define risks behind fostering a healthy workplace culture.

As recently as 2021, *Workplace Civility* reports represented a median of 15.8% of all reports – one of the highest *Risk Types* in our report. That median has only become larger – at 17.7% of reports in 2025.

For 2026, this trend is worthy of some serious contemplation. Reporters appear to be more comfortable using internal reporting systems to elevate concerns about all sorts of issues. *Workplace Civility*-type issues are inherently nuanced but may provide some of the richest indicators of culture and risks facing a given organization. We expect these reports to continue to represent a significant share of all reports in 2026 – and organizations that pay attention to these reports will learn much about their cultures and risk management.

More people are putting their names on reports

Looking back to 2009, a greater share of reporters today are willing to put their name behind an allegation. This is a boon for investigations by providing more context to allegations, and a signal that some reporters increasingly trust they will not face retaliation for raising concerns about misconduct. A median 65% of reports were anonymous in 2009, and in 2024, 54%.

For 2026, anonymous reporting remains a key part of any internal reporting program. In general, anonymous reporting seems to have leveled off in the mid-fifty percent range, but we note that organizations continue to receive a higher percentage of web reports which are more likely to be anonymous. With anonymous reporting remaining steady, this may represent an increased *expectation* of protection from retaliation, one that organizations should continue to uphold.

Report outcomes showing higher than expected 'no action'

Over the past 15 years, we have broadened the range of metrics we examine to provide greater insight into the "how and why" of reporting. One newer set of metrics is on report outcomes. What happens as a result of a substantiated case? While it is encouraging to observe that many reports are being treated with the seriousness they deserve, a significant concern remains: close to 15% of substantiated cases do not result in any follow-up action – no training, no policy change, no coaching, and no meaningful discipline. And – 14% of substantiated retaliation cases result in no action.

When this occurs, individuals may question the value of reporting issues or whether needed change will occur. For organizations seeking to build trust in their reporting systems and encouraging employees to speak up, it is essential to identify the reasons behind this lack of response and ensure that concerns are effectively addressed—otherwise, morale may suffer, and the reporting process itself could be undermined. For 2026, organizations will want to track this metric closely.

Archives reveal other notable trends

In perusing the old reports we found other notable changes we can consider for our future programs. For example, in 2008, 43% of anonymous reporters followed-up on their report in the system – close to half. Now, we barely pass 25%. Why have so many employees chosen to step back once they have filed a report?

Further, while we think we are receiving a lot of *Workplace Conduct* reports now, in 2008, human resources related cases were 70% of the reports. And finally in a sign of the times, in 2008, 15% of the reports were submitted via the web (which actually is surprisingly high). In 2024, the median of web reporting was 58%. We expect web reporting to continue to grow in share.

Conclusion

These are some of the key trends we've spotted over the past 15 years. If you're a regular reader of our report, you know we're always digging deeper and finding new ways to make sense of the data. Point-in-time benchmarking is still valuable, but looking at the long game reveals even more insights and opportunities to improve – and plenty of reasons to be optimistic about the future. It has been an honor for me to have been involved in preparing each one of these 15 reports.

2026 prediction

In 2026, employees, third parties, and everyone else involved will have a clearer sense of what strong internal reporting programs look like – and they'll continue to expect more. That means easier reporting, strong protection from retaliation, and real results with appropriate actions taken. Advances in case data analytics will further enable organizations to spot trends and risk areas faster and more easily. Are you ready for what's next?

About the author

Carrie Penman

As one of the earliest ethics officers in the industry, Carrie Penman has been with NAVEX since 2003 after serving four years as deputy director of the Ethics and Compliance Officer Association (ECOA), now ECI. A scientist by training, she developed and directed the first corporate-wide global ethics program at Westinghouse Electric Corporation from 1994-1999.

As chief risk and compliance officer for NAVEX, Penman leads the company's formal risk management processes. She also oversees its internal ethics and compliance activities employing many of the best practices that NAVEX recommends to its customers. Penman has extensive client-facing risk and compliance consulting experience, including more than 15 years as an adviser to boards and executive teams; most recently as NAVEX's senior vice president of Advisory Services. She has also served as a corporate monitor and independent consultant for companies with government settlement agreements.

Penman was awarded the inaugural Lifetime Achievement Award for Excellence in Compliance 2020 by Compliance Week magazine. In 2017, she received the ECI's Carol R. Marshall Award for Innovation in Corporate Ethics for an extensive career contributing to the advancement of the ethics and compliance field worldwide.

NAVEX | Navigator Series

Trusted by over 13,000 organizations, including 70 percent of Fortune 100 and 500 companies, NAVEX is the global leader in risk and compliance solutions. The NAVEX One platform strengthens risk and compliance programs, empowering organizations with unparalleled industry benchmark data and insights. NAVEX One provides a 360-degree view of enterprise, third party and ecosystem risk for enhanced regulatory compliance and proactive risk management. With offices in the U.S., Europe and Asia, and a global customer base, NAVEX continues to define the future of governance, risk and compliance.

Visit our blog or follow us on LinkedIn, Facebook, and YouTube.

Legal disclaimer

This content is informational. It is not and should not be relied upon as legal advice. Please consult your attorney for advice relating to your specific circumstances.

AMERICAS

5885 Meadows Road, Suite 500
Lake Oswego, OR, 97035
United States

info@navex.com
www.navex.com
+1 (866) 297 0224

EMEA + APAC

London
1 Queen Caroline St.
London W6 9YN
United Kingdom

info@navex.com
www.navex.com/en-gb/
+44 (0) 20 8939 1650