traliant

2026 Compliance Predictions Companies Can't Afford to Ignore

Can your company prove its commitment to doing the right thing? That's the question regulators, industries, employees and the public will all be asking in the year ahead.

Harassment Risk

Rising and More Politicized

Data from the first half of FY 2025 shows that nearly two-thirds (64%) of new EEOC lawsuits included Title VII claims, which cover workplace harassment, discrimination and retaliation. This continues the sharp upward trend seen in 2024, when the EEOC logged 88,531 new discrimination charges, with harassment accounting for about 40% of the charges.

64% of new EEOC lawsuits included Title VII claims, which covers workplace harassment, discrimination and retaliation.

In Traliant's 2025 State of Workplace Harassment Report, 46% of survey respondents said they had witnessed harassment happen to another employee in the past 5 years, while nearly 24% said they had personally been a target. The survey also suggests harassment is underreported, with 49% of respondents saying they would not report harassment due to fears of retaliation.

Other data also suggests that harassment risk remains elevated and extends beyond sexual harassment. Political divisions, religious tensions and cultural flashpoints are fueling more identity-based and interpersonal conflicts at work. SHRM's 2024 Civility Index found a 27% rise in workplace incivility, largely driven by social and political tensions.

Courts across the country are signaling that employers who don't train all employees, not just those in mandated states or roles, may lose key legal defenses in harassment claims.

Why it matters

Even if your organization operates in a state without a training mandate, the risk of doing the bare minimum has never been higher. Regulators, boards and investors are heightening scrutiny of workplace culture and conduct. The cost of inaction extends beyond penalties, eroding trust, retention and reputation.

Compliance training course recommendations

- Preventing Workplace Harassment
- Bystander Intervention
- Creating Inclusive Workplaces

The New Rules of Fair Management

From Good Intentions to Defensible Actions

Managers have emerged as one of the greatest sources of organizational risk, not through malice, but through everyday decisions and interactions that now carry legal and reputational consequences. In an era of heightened polarization and expanding employment laws, what a manager says, does, or overlooks can expose an organization to claims of bias, discrimination or retaliation.

From leave and accommodation requests to pay equity and performance evaluations, fairness is being redefined through consistency, transparency, and the equal application of policies and practices. Enforcement agencies are increasingly looking at whether managers are putting these principles into practice, not just understanding the rules.

63% of respondents in Littler Mendelson's 2025 Employer Survey expressed concern about discrimination and harassment claims.

This climate is fueling concern among insurers, who are bracing for a surge in claims. In Littler Mendelson's 2025 survey, 63% of respondents expressed concern about discrimination and harassment claims. Alarmingly, 45% specifically cited DEI-related litigation as a top concern, nearly double the rate reported in 2024.

Why it matters

Regulators and courts increasingly judge fairness by managerial consistency. Organizations must equip managers to navigate this environment with both empathy and precision. Offhand comments, uneven enforcement or failure to document decisions can all be interpreted as evidence of discrimination or favoritism.

Compliance training course recommendations

- Disability, Pregnancy and Religious Accommodations
- Family Medical Leave and Other Protected Leave
- Interviewing and Hiring Lawfully
- Wage and Hour Fundamentals
- Discrimination Prevention for Managers

Workplace Violence Prevention

A Crisis Driving Regulation

Workplace violence continues to take a devastating toll on both people and organizations. In 2023, the U.S. Bureau of Labor Statistics reported 740 fatalities linked to workplace violence, underscoring the human cost. Beyond the loss of life, the organizational impact is enormous. Violence costs U.S. businesses up to $130 billion annually, when factoring in turnover, absenteeism, medical and legal expenses, workers' compensation, security upgrades, lost productivity and damage to brand reputation.

By 2024, the FBI documented 24 active shooter incidents nationwide, highlighting the very real risk of extreme violence in workplaces and other public settings.

Traliant's 2025 Employee Survey on Workplace Violence and Safety shows the threat is escalating: 30% of employees said they had witnessed workplace violence (up from 25% in 2024), and 15% said they had personally been targeted (up from 12%).

States are responding. California's SB 553 requires nearly all employers to implement written workplace-violence prevention plans, complete risk assessments, and train staff annually. New York's Retail Worker Safety Act, effective mid-2025, adds training, reporting, and "silent response" requirements for large retailers. Texas has enacted similar rules for healthcare facilities. At least five other states (Alaska, Massachusetts, Ohio, Oregon, and Washington) are considering legislation to strengthen workplace violence prevention.

30% of employees said they had witnessed workplace violence and 15% said they had personally been targeted.

Why it matters

Organizations should treat workplace violence prevention not only as a compliance requirement, but as a moral and business imperative. Employees are increasingly anxious about their safety, and those fears directly affect engagement, retention and workplace culture. Without documented prevention plans, training and incident logs, employers risk legal exposure, operational disruption and a loss of employee confidence in their safety and well-being.

Compliance training course recommendations

- Workplace Violence Prevention
- Active Shooter Response
- De-Escalation

Code of Conduct Comes Back to the Forefront

Tip Volumes at Record Highs

The SEC's Office of the Whistleblower received nearly 25,000 tips in 2024 — the most ever — paying $255 million to 47 individuals. Regulators also fined 11 companies for maintaining policies that discouraged reporting.

Employees are increasingly bypassing company-managed systems to report directly to regulators or share concerns publicly on social media signaling a growing lack of trust in internal channels.

According to a 2025 Traliant study, 57% of employees say they've observed a potential Code of Conduct violation, yet 39% did not report it to HR. Over a third said they weren't sure how to respond when faced with an ethically ambiguous situation.

Meanwhile, one in five organizations experienced a significant integrity incident in 2024, according to Corporate Compliance Insights which is evidence that many companies are still struggling to turn ethical principles into everyday practice.

At the same time, the U.S. Department of Justice is reinforcing the message that transparency pays off, updating its Corporate Enforcement and Voluntary Self-Disclosure Policy to reward organizations that proactively report and remediate misconduct with reduced penalties or even declinations of prosecution.

The result is a widening gap between what organizations say in their Codes of Conduct and how effectively they live those values day to day.

57% of employees say they've observed a potential Code of Conduct violation, yet 39% did not report it to HR.

Why it matters

The "we didn't know" defense is obsolete. Regulators expect organizations to detect and disclose issues before they surface publicly, and now explicitly incentivize companies that do. Employees no longer give employers the benefit of the doubt when it comes to ethics or accountability; they speak up externally when internal systems fail them.

Compliance training course recommendations

- Code of Conduct
- Whistleblowing

Artificial Intelligence and Algorithmic Bias

Regulation Catches Up to Mass Adoption

AI is no longer experimental, it's operational.

Research from McKinsey & Company reports that 95% of U.S. firms use some form of generative AI. That rapid pace of adoption has regulators racing to respond.

The EU Artificial Intelligence Act entered into force in August 2024, and full obligations for "high-risk" AI systems (covering areas such as employment practices, scheduling tools, credit-scoring and essential services) become effective by August 2, 2026. Meanwhile, in the U.S., the Colorado Artificial Intelligence Act is set to become effective in June 2026, mandating bias audits and human oversight of AI systems.

Research from McKinsey & Company reports that 95% of U.S. firms use some form of generative AI.

At the same time, regulators such as the U.S. Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC) are warning that unexplainable algorithms and unmanaged decision-making models can violate current laws on discrimination, fair employment and consumer protection. The result: organizations will need to be able to defend their models as fair, explainable and governed.

Why it matters

Regulators and stakeholders alike will demand clear AI accountability. Who approved this model? How was it tested? Who's responsible for oversight? As AI becomes embedded in daily operations, compliance will shift to measurable governance. That means establishing cross-functional oversight, training employees to use AI responsibly and ensuring outcomes are transparent, traceable and fair.

Compliance training course recommendations

- AI in the Workplace
- AI Guidance Micro Reels

Cybersecurity and Breach Disclosure

The Four-Day Rule Era

The U.S. Securities and Exchange Commission's cyber-incident disclosure rule has made cybersecurity a governance and transparency issue, not just a technical one, and it's penalizing firms for vague or misleading cyber-reports. Effective late 2023, public companies are required to report material cyber events within four business days of determination. In the first year, disclosures rose by approximately 60%, yet fewer than one in ten included meaningful detail on impact or mitigation.

Meanwhile, the threat landscape is undergoing a dramatic transformation: AI-driven attacks are on the rise, increasing 47% in 2025, and the average cost of such a breach reaching US $5.7 million, up 13% year-on-year. Attackers are employing generative AI, deep-fakes, hyper-targeted phishing (click-through rates some 4.5 times those of traditional attacks), and automated systems executing thousands of attempts per second.

As cyberattacks become more frequent, realistic and personalized through AI, companies must strengthen employee readiness to recognize and respond to emerging threats. Traliant's 2025 State of Cyber Report found that 78% of surveyed employees lacked confidence in spotting sophisticated threats like video deepfakes and voice spoofing.

78% of surveyed employees lacked confidence in spotting sophisticated threats like video deepfakes and voice spoofing.

Why it matters

Traditional cyber-defenses are becoming less adequate as speed, scale and deception increase. At the same time, regulators expect companies to explain not only that an incident occurred, but how it was managed, contained and communicated. Clarity, timeliness and accountability now define effective disclosure. Compliance now means demonstrating governance under pressure and showing that your team can execute when it counts.

Compliance training course recommendations

- Global Data Privacy Awareness
- Cybersecurity Awareness
- HIPAA
- FERPA Micro Reels

Bonus Insight

The Proof Movement Redefines Training

In 2026, evidence will outweigh promises. Whether it's proving your workplace is safe, your AI systems are fair, or your investigations are timely, compliance success will depend on showing, not just saying, that your policies, systems, and people perform as intended.

That same expectation for proof is reshaping how organizations deliver compliance training. Regulators, auditors, and boards are no longer impressed by completion rates alone; they want tangible evidence that training changes behavior, improves awareness, and reduces risk. Federal agencies like the DOJ and EEOC have made it clear that a company's training quality and compliance culture can directly influence enforcement decisions, even affecting the size of penalties or settlements.

To meet this higher bar, organizations are shifting their format, frequency, and delivery of training itself. Static, once-a-year courses are quickly giving way to dynamic, ongoing learning models designed to reinforce knowledge and measure impact. One example is "micro," high-impact lessons that deliver clear, practical guidance in just 2–3 minutes. Inspired by TikTok and Instagram, these bursts of learning meet employees where they are, right in the flow of work, making education feel more like social media and less like a mandatory chore.

Organizations that can demonstrate not only that employees were trained, but that the training worked, will be best positioned to earn trust and withstand scrutiny.

Why it matters

Compliance is no longer being measured by completion, but by comprehension. Training is evolving from a regulatory obligation into a company's first line of legal defense, which is proof that its culture, controls and people can stand up to oversight and deliver results when it matters most.

Let Traliant help you create a meaningful impact in your organization.

929-294-7111 | www.traliant.com

traliant