THOMSON REUTERS INSTITUTE

10 Global Compliance Concerns for 2026

Advances in technology are helping everyone, including criminals

December 10, 2025

How to prepare for 2026

Compliance and risk management professionals face a daunting list of challenges and concerns as they enter 2026. To further clarify those concerns, their potential impact, and how organizations can prepare for the challenges ahead, the Thomson Reuters Institute has published the "10 global compliance concerns for 2026." Although far from a comprehensive list and in no particular order, the following are the 10 key issues and concerns that corporate compliance and risk professionals are likely to encounter in 2026 and beyond.

Fraud, scams, and other financial crimes

In the world of compliance, technology is both friend and foe. On one hand, new technologies have given compliance professionals a powerful set of tools to protect institutions from financial crime, improve risk management, and conduct more thorough due diligence. But on the other hand, technological advances like AI and cryptocurrencies have given criminals an arguably more powerful set of tools to commit all manner of financial crimes, including money laundering, fraud, embezzlement, terrorist financing, extortion, and more.

More concerning for risk professionals, the problems are only getting worse. Ransomware, elder exploitation, investment scams, romance scams, crypto-wallet transfers, account takeovers, and so-called "pig butchering" are all on the rise and show no signs of slowing. Indeed, in 2024, Americans lost $12.5 billion to fraud, a 25% increase from 2023, according to the U.S. Federal Trade Commission (FTC). However, those are just the reported losses, and most fraud victims don't alert authorities.

Impact in 2026

For compliance and risk professionals, the growing proliferation of tech-enabled fraud represents a formidable threat. Compounding the problem is the fact that many compliance officers at small and midsize banks, credit unions, fintech firms, and other financial service organizations often lack access to advanced fraud prevention and detection technologies. So, while criminals are using the latest AI technologies to steal from people using increasingly creative methods, compliance personnel and financial investigators are often working at a technological disadvantage.

Recommended actions

Internally, companies and financial institutions should consider upgrading their compliance technologies and revisiting their processes for know-your-customer (KYC) and anti-money-laundering (AML) programs to ensure they can target the types of fraud most likely to affect their organizations. Rigorous, regular prevention and detection training for their professionals is also a must because the tactics and methodologies used by scammers are constantly evolving.

A more effective societal defense against fraud should include better victim support, more aggressive law enforcement, and global campaigns to spread awareness, says Teresa Anaya, the founder and director of AML Audit Advisory. “Coordinated global awareness is urgently needed because these operations are driving billions of dollars into illicit crypto flows every year,” she explains.

AI: Ethics and usage

Increasingly capable AI systems offer compliance professionals the means to improve efficiency, reduce costs, and create more reliable KYC and AML programs. However, as Jim Richards of RegTech Consulting points out, most private and public organizations are still trying to fight financial crime using older machine-learning technologies, whereas “the crooks are using more advanced forms of AI.”

In many ways, these more advanced generative AI (GenAI) and agentic forms of AI are a criminal’s dream come true. GenAI and agentic AI

systems can teach themselves, make independent decisions, and produce vast amounts of original — albeit fake — text, video, and images. Plus, they do it all autonomously, without any human intervention.

Using this technology, criminals can create tireless armies of attack bots that execute, learn, revise, and repeat their assaults until they achieve their desired goal, whether it be coaxing someone to click on a malware link or creating a whole city's worth of synthetic identities.

Impact in 2026

The main AI challenges for compliance professionals are threefold:

- They must work to understand how the systems currently available to them are limiting their ability to conduct thorough due diligence and protect their institutions
- They must decide where and how to deploy more advanced AI technologies to enhance their risk-management programs and keep up with the criminals
- They must incorporate any new AI technologies thoughtfully, ethically, and responsibly

Recommended actions

As enticing as the prospect of AI-enhanced compliance is, teams implementing these systems must also recognize that they should not operate AI systems without strict data-privacy procedures and human oversight in place.

To maintain trust in the system and ensure accountability, a qualified human being should review and validate AI output and frequently audit for accuracy. Leaders will also have to decide how much they want their risk-management programs to rely on AI, given that higher-value activities — such as investigation and prevention — are still the domain of well-trained professionals.

Cryptocurrency regulation and compliance

The rapid mainstreaming of cryptocurrencies and other digital assets has thus far outpaced most government efforts to regulate the sector. Further, the current U.S. administration has rolled back several regulations that once limited the ability of banks in the traditional financial system from offering crypto-based services. Enforcement pressure has also eased.

However, compliance challenges related to crypto assets persist due to their higher risk profile, inherent volatility, and fragmented regulatory landscape. Data breaches, digital theft, a lack of consumer protection, and the widespread use of crypto for money laundering and other criminal activities are also risk considerations.

Impact in 2026

The macro-trend for crypto in 2026 is likely to be the wider use of crypto assets and broader acceptance of them within the traditional banking system. In 2026, expect to see more traditional banks, startup and established fintechs, and even crypto-native banks offering services for digital assets, including loans, investment advice, third-party custody and trading services, fund transfers, and stablecoin issuance.

Efforts to develop a global standard for cryptocurrency regulation will also continue in 2026. The United States recently passed the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS) Act, which establishes a regulatory framework for so-called stablecoins, a type of digital asset whose value is pegged to a fiat currency — in this case, the U.S. dollar.

Many countries are also considering versions of the European Union's Markets in Crypto-Assets (MiCA) framework and the United Kingdom's 2023 Financial Services and Markets Act, which are among the most comprehensive frameworks developed to date.

Recommended actions

The trend toward more crypto involvement at traditional financial institutions means compliance officers will face increasing pressure to accurately assess the risks posed by working with crypto-based businesses and customers. Unfortunately, applying a meaningful, risk-based approach to

crypto assets is difficult if compliance personnel aren't familiar with crypto and lack experience assessing the legitimacy of digital assets or crypto-based businesses.

"Banking as a Service (BaaS) and fintech partner banking are booming, which is great," says Sarah Beth Felix, the founder and Chief AML Officer of Palmera Consulting. "But without proper oversight and controls, this can lead to even larger volumes of dirty money and illicit actors entering the U.S. financial system."

Most traditional banks have a posture that demonstrates abundant caution toward crypto in the current environment. Banks should also make it a priority to develop and implement KYC and AML policies that specifically address institutional risks related to crypto, including automation of 24/7 transaction monitoring for high-risk clients.

Data privacy

Concern over massive data breaches, frequent cyberattacks, and the misuse of personal data has spurred governments worldwide to enact stricter data-privacy laws. Meanwhile, public trust in any institution's ability to protect private data is eroding, and skepticism about how companies — particularly those involved in tech and AI development — collect and use customer data continues to grow.

Impact in 2026

Organizations that fail to enact and enforce strict data-management practices will face increasingly punitive measures for noncompliance in the coming years. In addition, other data-related risks include reputational damage, business interruptions, and loss of customer trust.

The need to comply with complex regulations, ensure data security, and maintain responsible policies for data life-cycle management could require organizations in both the public and private sectors to invest more heavily in updated security and compliance technologies. At the very least, encryption, strong access controls, and regular security audits are a must, as is automation of continuous monitoring activities and oversight of third-party access and interactions.

Recommended actions

In addition to technological upgrades, all organizations should recognize that most security breaches result from human error or malfeasance. Therefore, regular training on best practices around data privacy and security is a vital part of maintaining a secure technological ecosystem. All employees should be well-versed in password management, phishing recognition, and other potential threats; those in compliance roles should be regularly briefed on vulnerabilities relevant to their organization.

The professionalization of cybercrime

By 2031, cybercrime will cost the world $12.2 trillion annually, roughly $386,000 worth of harm every **second**, according to *Cybercrime Magazine*. The ongoing digitalization of modern life — including online banking, e-commerce, cloud-based computing, and AI — continues to open new frontiers for bad actors to exploit.

Ransomware, hacking, phishing, and other forms of electronic intrusion have been around for a long time, but one of the most disturbing trends in recent years has been the expanding **professionalization** of cybercrime.

Impact in 2026

The professionalization issue is unfolding on two main fronts:

- Increasingly organized and sophisticated criminal operations that often model their operations after legitimate corporate enterprises, such as ransomware as a service (RaaS)
- Powerful nation-states, such as Russia, China, and Iran, are working with transnational criminal organizations and developing alliances that did not exist before

“What we’re seeing now is an alignment of incentives and interests where these countries are either tolerating, actively supporting, or covertly resourcing criminal groups that are doing all kinds of things to undermine the West,” says Urriolagoitia “Rio” Miner, the founder and CEO of FCI Tradecraft.

Recommended actions

The security community has done a fairly good job of devising a set of best practices that includes encryption, antivirus software, multifactor authentication, biometric passcodes, strong passwords, virtual private networks (VPNs), and frequent security updates. Taken together, these practices represent a formidable — although not always perfect — firewall against cyberattacks.

Organizations that want to strengthen their security profile should work toward developing a culture of security and regularly train frontline employees on the latest trends in cybercrime, according to Miner.

Financial crimes enforcement

The Financial Crimes Enforcement Network (FinCEN), a unit within the U.S. Department of the Treasury, has been reevaluating its enforcement approach to better align the agency's efforts with the current administration's priorities. However, confusion about what those priorities are, how to address them, and how financial institutions should respond has left many regulators and compliance professionals searching for some elusive clarity.

Impact in 2026

In general, the Trump administration has said it wants to create more efficient compliance processes, reduce the regulatory burden on financial institutions, and revamp current reporting requirements to generate more actionable leads for law enforcement.

Thus far, FinCEN has issued alerts regarding several abandoned or delayed regulations and has offered revised reporting rules for financial institutions. Among the changes are:

- **Beneficial ownership information (BOI).** After years of working to develop a database of beneficial ownership for companies doing business in the U.S., FinCEN abandoned its requirement for U.S. companies to file BOI information in March. However, foreign companies doing business in the U.S. must still report.

- **Residential real estate reporting.** FinCEN postponed reporting requirements for all-cash, residential real estate transactions until March 1, 2026, after which the new rules will take effect.
- **Suspicious activity reports (SARs).** To reduce the number of unnecessary and so-called **defensive** filings, FinCEN has streamlined some aspects of the SAR filing process. For example, SARs no longer need to be filed for transactions near the $10,000 threshold unless suspicious circumstances warrant it, and institutions no longer need to file a document every time they decide **not** to issue a SAR.

Recommended actions

FinCEN is reportedly reevaluating its operations and is expected to announce additional changes in 2026. As a result, corporate compliance professionals may soon find themselves considering how to respond to even more FinCEN alerts and notices, as such regulatory change increasingly occurs through published advisories and typology-focused guidance rather than through the passage of new, formal rules.

“In 2026, I fully expect compliance professionals to be inundated with FinCEN alerts and notices,” says Palmera’s Felix, adding that these publications carry an implicit expectation that financial institutions operationalize them. That, in turn, requires AML compliance teams to reassess whether their technology solutions are nimble and robust enough to translate FinCEN's evolving guidance into effective, day-to-day controls.

Sanctions and tariffs

The ongoing conflict in Ukraine and a global trade war have turned regulations involving sanctions and tariffs into a revolving carousel of uncertainty. Near-constant changes mean the rules for compliance are not always clear. Nevertheless, all indications suggest that regulators, trade authorities, and law enforcement are ramping up their enforcement efforts related to sanctions and tariff avoidance, raising the risk of penalties for noncompliance.

Impact for 2026

The U.S. Department of Justice (DOJ) has issued memorandums indicating its intent to aggressively pursue criminal and civil penalties for customs fraud and tariff evasion. Toward that end, the DOJ has formed a new Market, Government, and Consumer Fraud Unit (MGCFU) that will be responsible for investigating tariff noncompliance, including misclassification of goods and country-of-origin disputes. The DOJ has also expanded the reward structure of its whistleblower program to include those who provide tips on customs and tariff fraud.

Sanctions, too, have become increasingly important in the overall effort to dissuade individuals, groups, organizations, and countries from engaging in various illicit activities, particularly money laundering, terrorist financing, and human-rights abuses.

Indeed, the number of economic, diplomatic, military, and environmental sanctions has expanded considerably over the past couple of years, and compliance lists are constantly being updated.

Recommended actions

Sanctions screening is one area in which automation and AI are a boon for compliance personnel. Manual list matching is no longer necessary when software programs are available that monitor list updates, provide continuous monitoring capabilities, and use dynamic risk scoring to evaluate matches and issue alerts.

Tariff compliance is somewhat more complicated, if only because the shifting geopolitical landscape introduces so many uncertainties. Once again, however, dedicated trade software that automates product classification can help companies track tariffs, avoid penalties, and ensure they are not overpaying.

Sanctions and trade compliance professionals must also maintain a clear, consistent focus amid changing political and regulatory priorities. “It is vital for AML and sanctions compliance professionals to maintain their focus on finding suspicious activity and illicit actors and reporting them in a timely and effective manner to law-enforcement partners," says Palmera’s Felix.

Indeed, tools and technologies may evolve and administrations may shift, she adds, but the core mandate of compliance — to detect, escalate, and report potential wrongdoing — remains constant.

Environmental, social, and governance compliance

Corporate compliance and sustainability officers are spending increasing amounts of time tracking, gathering, and reporting compliance data on their organization's environmental, social, and governance (ESG) activities. Not surprisingly, new ESG regulations also come with additional compliance burdens and costs. However, failing to meet these standards can lead to penalties, brand damage, loss of customer loyalty, loss of investment capital, hiring difficulties, and employee defections.

Impact in 2026

Regulatory turmoil around ESG reporting promises to complicate almost every aspect of ESG compliance in 2026.

On one hand, anti-ESG sentiment in the United States is chipping away at — or in some cases, dispensing with — certain ESG reporting obligations, particularly climate-related requirements. In March, for example, the U.S. Securities and Exchange Commission (SEC) voted to indefinitely pause its enforcement of disclosure rules for climate-related risks and greenhouse gas emissions. In addition, more than 20 states have passed legislation either prohibiting or limiting ESG considerations in investment and business decisions that involve state assets or contracts.

On the other hand, many other states are **expanding** their ESG disclosure requirements in response to federal retreat on the issue, with California leading the way. Regulatory details for the California Air Resources Board's (CARB) new SB 253 and SB 261 climate-reporting requirements are expected to be released in early 2026. However, the first reports under SB 261 are due January 1, 2026, and greenhouse gas emissions reports under SB 253 are due in mid-2026.

Meanwhile, ESG regulations in the EU continue to proliferate. The EU's Corporate Sustainability Reporting Directive (CSRD) and Corporate Sustainability Due Diligence Directive (CSDDD) comprise a double dose of

comprehensive sustainability disclosure requirements. These directives cover virtually every aspect of corporate oversight, including governance, strategy, resource use, supply chains, environmental impact — air, water, and land — and more.

The CSRD and CSDDD primarily target companies with more than 1,000 employees. However, these laws have become such a political flashpoint that efforts are underway to either weaken or gut some of the most onerous requirements.

Recommended actions

Given the volatility and uncertainty of ESG compliance requirements over the next several years, organizations must closely monitor regulatory developments and upcoming reporting deadlines.

Organizations should prioritize their ongoing ESG efforts in two areas:

- Strengthening sustainability data and governance by ensuring that internal processes, data systems, and oversight structures can generate consistent, accurate, and verifiable information to meet current and future compliance obligations
- Focusing on decarbonization and broader risk mitigation to improve resource efficiency and reduce exposure to an increasingly uncertain business environment

Third-party providers and supply chain integrity

Today’s supply chains are a complex web of third-party business arrangements that span the globe in the multifaceted journey from raw materials, through manufacturing, to a finished product. However, it is virtually impossible to determine whether foreign suppliers are fully compliant with all local and international regulations.

Despite this setback, organizations are still responsible for ensuring their supply chains are legal, ethical, and sustainable. Indeed, companies can be held liable if their suppliers are in violation of the law.

Impact in 2026

Several regulatory changes targeting supply chain compliance will kick in over the next few years, particularly for multinational firms and companies operating in the EU.

First, the EU's CSDDD begins phasing in mandates requiring the mapping and monitoring of all tiers of a company's supply chain, including ongoing risk assessments for human rights and environmental violations. Jurisdictions have until mid-2026 to incorporate the CSDDD into local legislation, with reporting requirements beginning in 2027.

In the latter half of 2026, the EU's Cyber Resilience Act (CRA) will introduce new cybersecurity requirements for digital services and products in the supply chain. Specifically, the CRA mandates that companies acquire a Software Bill of Materials, which is an inventory detailing all components, libraries, and dependencies within a software product. Beyond that, they must also conduct more frequent audits, build cybersecurity into their products, report vulnerabilities, and provide frequent security updates.

However, the CRA's reporting obligations don't begin until December 2027.

Recommended actions

To comply with the CSDDD and other regulatory changes, affected companies need to adopt a comprehensive, risk-based approach to supply-chain management, due diligence, and third-party oversight. Reporting requirements and enhanced due-diligence capabilities may also require upgrades to an organization's data management and supply chain visibility technology and systems.

Regulatory changes

Staying current with regulatory changes is a near-constant responsibility for compliance professionals. In the digital era, many of these changes involve paying more attention to every aspect — more data, more reporting, more requirements, more transparency, etc. If the pressure to provide more comprehensive information isn't enough, most government entities want that information as quickly as possible, or even in real time.

Impact in 2026

Most of the new regulations that public and private-sector organizations are likely to encounter in 2026 will involve AI governance and accountability, cybersecurity, data privacy, climate-risk disclosure, transaction monitoring like e-invoicing, and cryptocurrencies. Furthermore, most of these regulations will hold companies to a higher standard of accountability, with increasingly punitive penalties for noncompliance.

Regardless of the regulatory changes involved, the processes for managing and addressing them are likely to involve dedicated software and some form of AI. Manual systems simply can't keep up with the accelerating pace of data gathering and reporting necessary for compliance, and the speed and volume of data acquisition and analysis required will only increase.

Recommended actions

Depending on an organization's size, global reach, and industry, leaders will need to take the necessary steps to ensure that their technological ecosystems are sufficiently powerful and responsive enough to meet compliance obligations. If not, a cascade of negative consequences is likely to unfold, requiring even more resources and time to address. Action now will pay dividends later.

How to prepare for 2026

Compliance leaders within corporations and financial institutions that seek to strengthen their risk management and fraud detection capabilities in the coming year should consider taking the following steps:

- **Perform a compliance risk-assessment refresh.** Map your team's current competencies, then identify gaps and address them.
- **Strengthen governance structures.** Determine who is accountable for AI systems, vendor risk assessments, ESG reporting, and related areas within your team and the organization. Make it a priority to solidify board and leadership oversight and buy-in.

- **Invest in technology and automation.** Make the case to leadership that investing in the compliance function can yield dividends in terms of problems avoided. Look into acquiring such tech components as compliance automation tools, vendor risk-assessment platforms, data governance systems, trade management software, and sanctions compliance software.
- **Review and update policies and procedures.** Assess your organization's current compliance policies to make sure they cover new risks and domains, such as AI, third parties, supply-chain integrity, digital assets, and more.
- **Train and build awareness across the organization.** Make sure the organization trains all employees about avoiding phishing traps that could lead to cybersecurity problems and other compliance issues. Many emerging risks — like third-party, cybersecurity, and phishing — are human or cultural issues as much as they are technical.
- **Plan for the unexpected.** Run scenario models to identify and anticipate potential risk factors and minimize uncertainties. Although it is impossible to predict every risk, planning for contingencies may better prepare your team.

To navigate the evolving landscape of compliance and risk management effectively, organizations must proactively embrace these strategies. Compliance and risk teams that move early on these priorities will not only fortify defenses against emerging risks but also position themselves to navigate the evolving regulatory landscape of 2026 and beyond with greater confidence and strategic foresight.