

A SURVEY REPORT BY COMPLIANCE WEEK

Companies bullish on  
**NEW TECH**  
amid enhanced sanctions scrutiny



Sponsored by



## About us

---

### COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a quarterly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. [www.complianceweek.com](http://www.complianceweek.com)



Certa helps Fortune 500 firms with global third-party compliance, risk management, and ESG. Certa is a comprehensive platform to manage all third parties globally which can be personalized via a no-code studio and an open architecture with 120+ ready-made integrations. Certa has been recognized as a Top 50 Procurement Providers to Watch in 2022 by Spend Matters, and a Representative Vendor in Gartner's 2022 Market Guide for Third Party Risk Management Solutions and IT Vendor Risk Management Solutions. For more information or to schedule a demo, visit our [website](#), [Twitter](#), and [LinkedIn](#).

# Survey: Companies bullish on new tech amid enhanced sanctions scrutiny

Emerging technologies like automation and generative AI are on the radar as difference-makers for businesses serious about keeping pace with increasing regulatory scrutiny toward third-party due diligence and sanctions compliance.



BY KYLE BRASSEUR, COMPLIANCE WEEK

If sanctions are the top enforcement priority for the Department of Justice (DOJ), companies have got the message, according to a recent study.

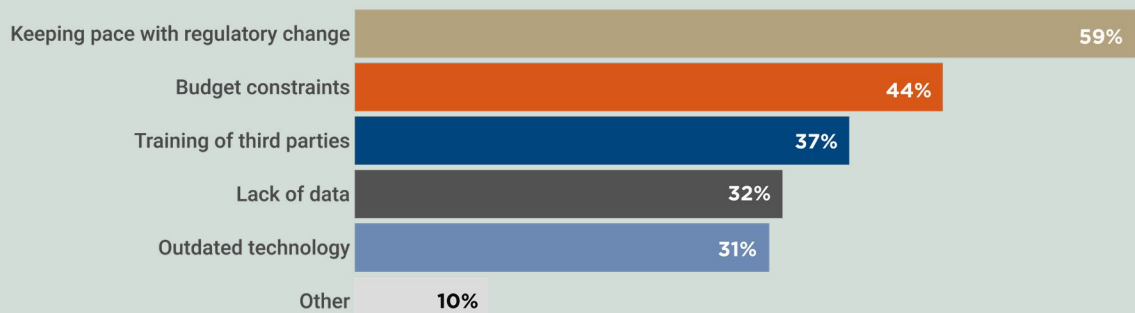
Nearly half the respondents (43 percent) to a survey conducted by Compliance Week and third-party risk management (TPRM) software provider Certa said increasing regulatory scrutiny was the main factor driving their organization's adoption of technology for third-party due diligence and sanctions compliance. Businesses also indicated keeping pace with the rate of regulatory change as the biggest challenge to ensur-

ing sanctions compliance (59 percent), ahead of budget constraints (44 percent), training third parties (37 percent), and lack of data (32 percent). More than one answer was permitted.

"Though organizations understand and are taking seriously the DOJ's current mantra that sanctions are the new Foreign Corrupt Practices Act, some still believe the cost of standing up an enterprise-grade sanctions compliance program is more expensive than any potential fine", said Dave Crozier, Senior Vice President of Digital Transformation and Partnership & Alliances at Certa. That said, those organizations understand

## What are the key challenges you face in ensuring sanctions compliance and conducting effective third-party due diligence at your organization?

Choose all that apply.



sanctions compliance demands are not slowing down and will only get more complicated, he added.

It's not just about avoiding fines; it's about safeguarding your brand's reputation and credibility. Flouting sanctions regulation can result in negative publicity that can have long-lasting repercussions," he said.

The survey, conducted online between August and September, received 145 total responses, nearly one-third of which came from senior compliance practitioners. Industries most represented included financial services (26 percent), health-care (12 percent), education (8 percent), and manufacturing and energy and utilities (7 percent each).

More than half the respondents (56 percent) worked for companies with less than 5,000 employees, while the most selected annual revenue range was \$1 billion to \$5 billion (25 percent).

Three-fourths of respondents (75 percent) described sanctions compliance and third-party due diligence as "very important" to their organizations. The figure is no surprise, but complications remain when ensuring sanctions compliance programs reflect the business's risk profile.

"Most organizations have a general idea what sanctions compliance means," said Crozier. "They struggle to understand whether or not their policies, capabilities, and screening are commensurate with their peers—with what the DOJ would expect of a program for a company of their size, scale, and funding."

This was reflected in how few respondents (25 percent) said they envision the future of sanctions compliance and third-party due diligence at their organization to be "very mature" (i.e., enriched and integrated). Companies were more likely (62 percent) to select "somewhat mature" (i.e., standardized), a safer option that acknowledges how many believe there's always room for improvement.

"Those that are saying they're 'very mature' have invested in data, matching, algorithms, or outside services that can do that combination," said Crozier. "To go from simple to very mature, they're going to have to invest in systems integration."

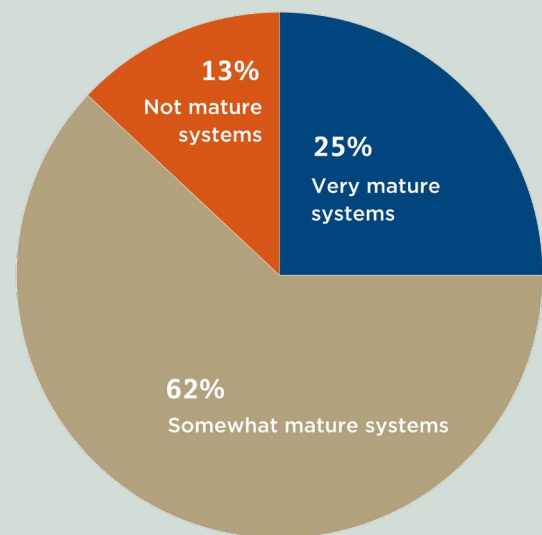
### Technology opportunities

Asked what technologies their companies have implemented or explored to enhance sanctions compliance and third-party due diligence efforts, respondents most selected TPRM software (50 percent), followed by data analytics and reporting platforms (38 percent) and enhanced know your customer (KYC) solutions (33 percent). More than one answer was permitted.

Looking ahead at which technologies/trends would have the most significant impact in the space, the top answers were automation (69 percent), process orchestration (62 percent), and generative artificial intelligence (AI) (51 percent).

The number of compliance programs bullish on generative AI less than a year since it hit the mainstream following the

## How do you envision the future state of third-party due diligence and sanctions compliance at your organization?



launch of OpenAI's ChatGPT might be surprising to some. Not to Jag Lamba, Founder and Chief Executive Officer at Certa.

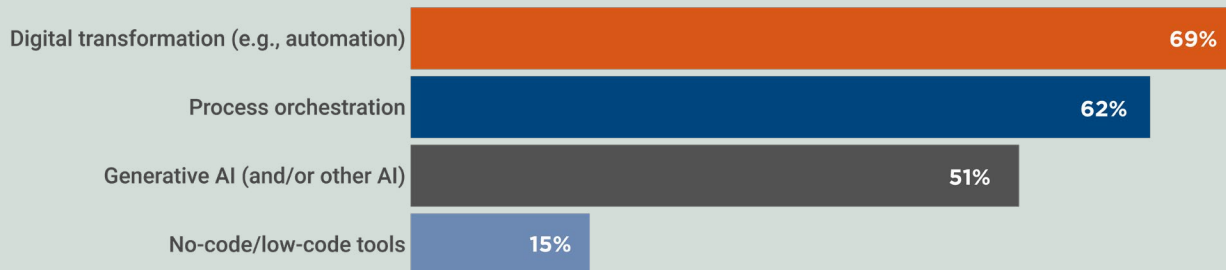
"The only surprise to me is it's only 51 percent," said Lamba. "It's 100 percent the future. Overall, the impact generative AI will have on this space will be massive and will enable a second wave of AI transformation. It's going to make life much easier."

Examples of the ways in which generative AI can enhance sanctions compliance and due diligence efforts include:

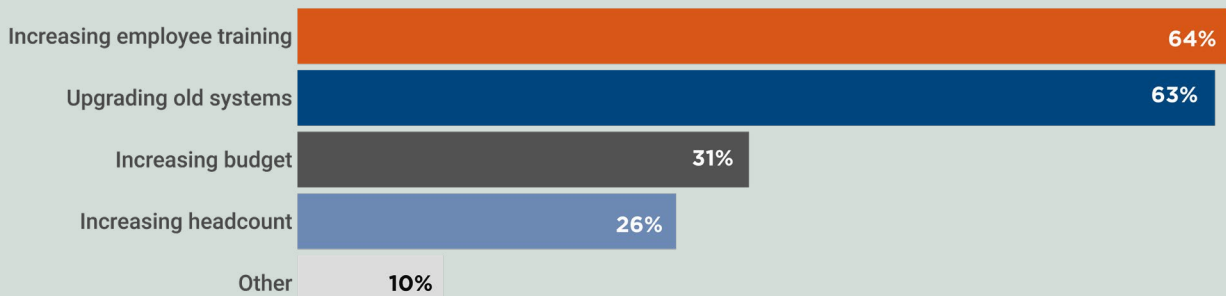
- » Automating the process of converting policy text to control frameworks, including sanctions screening, looking up ultimate beneficial owners, and exception approvals;
- » Converting unstructured data to structured data;
- » Reducing time burdens associated with filling out compliance forms;
- » Enhancing reporting so that managers can interact directly with the compliance system rather than going through analysts; and
- » Enabling the desire among compliance professionals to move from one-off technology solutions to comprehensive suites that ease training burdens.



**What emerging technologies or trends do you believe will have a significant impact on sanctions compliance and third-party due diligence? Choose all that apply.**



**What steps are you taking to prepare for these future developments? Choose all that apply.**



To that last point, 64 percent of survey respondents said increasing employee training is how they are preparing for future technological developments and a vital step to ensure compliance readiness.”

“The space is moving so quickly. ... The real differentiator between the firms that crush it and the firms that just try to get some buzz using generative AI is how deep is their current technology stack,” Lamba said. “If they have a strong technology stack today, then, going forward, you can really enhance that using generative AI. If you have a shallow technology stack now—i.e., forms with not a lot of depth under the surface—then generative AI is not going to help you.”

In October, Certa launched CertaAssist, which merges generative AI with third-party management to enable enhanced workflow optimization, data visualization, and onboarding.

Asked where they felt AI capabilities would most improve their due diligence and compliance efforts, respondents selected continuous monitoring of third parties (75 percent), advanced risk modeling (62 percent), and enhanced automated

decision-making and KYC processes (47 percent each). More than one answer was permitted.

#### Resource restrictions

Budget constraints remain the largest obstacle to adopting new technologies (59 percent), followed by lack of awareness of tools on the market and their capabilities (47 percent). Nearly a quarter of survey respondents (22 percent) indicated their business was relying on in-house tools.

The issue with tackling sanctions compliance alone is keeping up with the speed of change, said Crozier. Areas becoming increasingly important include the quality and cleanliness of your data. The need for full-cycle controls to ensure compliance is only becoming more critical as government agencies enhance their own technological capabilities.

“While you might have been able to get away with [playing it slow to minimize costs] in the past, it is absolutely not something you will continue to get away with,” Crozier said. “The more companies do not comply or take that approach, the higher the fines are going to get.”

# Sanctions are the New FCPA: **Revamping Corporate Compliance for Stricter Sanctions Regimes**

## Comparing Sanctions Compliance to the FCPA

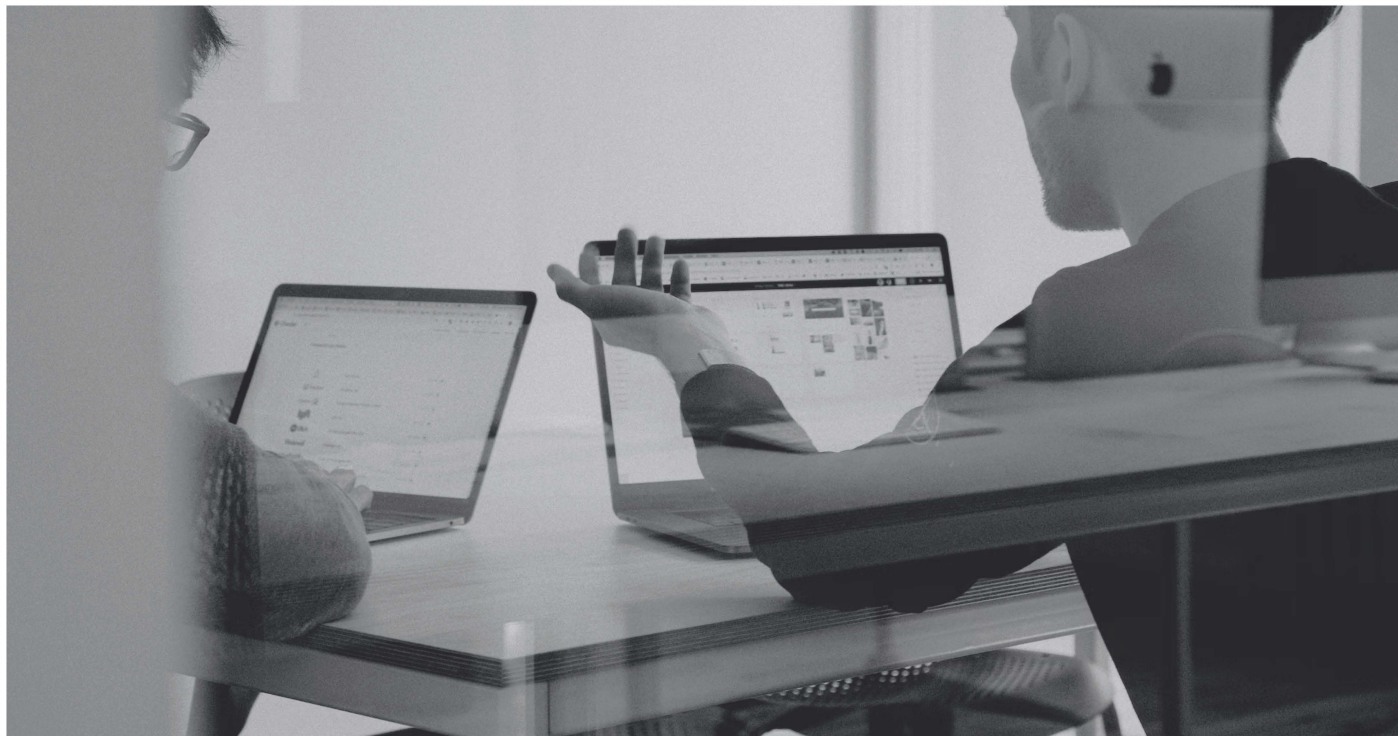
Corporate compliance programs need to adapt to the increased focus on U.S. sanctions, and this will mean implementing new practices compared to those in place for FCPA regulations.

At a minimum, all U.S. corporate compliance programs, including the FCPA and sanctions programs, are legally required to follow guidelines from the DOJ and the U.S. Sentencing Commission (USSC) [6, 7].

Since the FCPA has been around for more than four decades, most compliance officers have become proficient at designing FCPA compliance programs.

The good news is that many of those practices can transfer to sanctions compliance as long as such programs answer these questions:

- Is the compliance and ethics program well-designed and effective?
- Are the risk assessments tailored to the relevant business activities and environment?
- Does compliance training give practical steps to become compliant?
- Does the program have a confidential internal whistleblowing mechanism and investigation process?
- Does it require due diligence for its third-party relationships, mergers, and acquisitions?
- Is the compliance program adequately resourced?
- Does the organization have a culture of ethics and compliance from the top down?
- Do compliance officers have sufficient autonomy and authority to consistently monitor and enforce compliance programs?
- Does the program work in practice? Is it continuously monitored, reviewed, and improved?



# How Sanctions Compliance Differs from FCPA Compliance

Companies cannot focus on FCPA compliance alone while sanctions compliance becomes more urgent. Due to the differences between the two, organizational compliance needs an overhaul

---

## Sanctions

### I Core focus

The focus is on the beneficiaries of transactions.

Sanctions apply even when the transactions by themselves are like any other normal customer or vendor transactions.

### I Risk assessments and controls

Since sanctions violations may harm large populations, sanctions compliance demands comprehensive risk assessments and controls.

---

## FCPA

The focus is on preventing corrupt transactions based on the givers, their intent, and the business outcomes.

Recipients of bribes are not its focus.

FCPA risk assessments have a different focus — preventing corrupt transactions. But they are critical elements of corporate compliance and must be thorough.

---

# Sanctions

## Enforcement agencies

U.S. sanctions are enforced by these major agencies (among others):

- The DOJ
- The Treasury's Office of Foreign Assets Control (OFAC)
- The Treasury's Financial Crimes Enforcement Network
- The Department of Commerce's Bureau of Industry and Security (BIS)
- U.S. Customs and Border Protection
- Department of Homeland Security
- Department of State

Compliance officers must monitor frequent guidelines from all these departments.

## I Screening controls

Screening is an essential risk control for sanctions.

It is done using watchlists like:

- OFAC sanction lists [\[8, 9\]](#)
- BIS entity list [\[10\]](#)

Entities are often added to and removed from watchlists.

So, screening requires constant real-time automated monitoring and properly configured screening tools.

## I Recommended compliance structure

Due to the novelty, number, and complexity of sanctions programs and watchlists, a strong, centralized compliance structure with highly competent compliance officers is the wiser choice.

## I Affected industries

Sanctions impact a large number of industries and multiple business activities, including sales, partnerships, financing, and supply chains.

But new industries like drones, information technology, and artificial intelligence are unaccustomed to sanctions and likely to be the focus of regulatory surprises in the future [\[11, 12\]](#).

---

# FCPA

The FCPA is enforced by only two agencies, the DOJ and the Securities and Exchange Commission.



There are no government watchlists of forbidden third parties under the FCPA. Compliance is more about screening partners and overseas agents with less risk of corrupt transactions.

Its risk controls are monitoring the transactions, expenses, and benefits of transactions.

Since the FCPA has been around for more than four decades, its compliance structures are well-understood.

The FCPA applies equally to all industries and has become a standard component of compliance across all U.S. industries [\[13, 14, 15\]](#).





# How to Rebuild Corporate Compliance Programs for Sanctions

Given the differences between sanctions and FCPA compliance programs, companies can make several improvements to their compliance programs to comply with sanctions.

## I Communicate the Value of Sanctions Compliance

A successful corporate compliance program must persuade employees to see the value of sanctions compliance. Many business benefits are likely to be very specific to the company, industry, or location, but some general benefits also accrue:

- Large clients and governments perceive compliant vendors and suppliers favorably, giving them a competitive advantage [\[16, 17, 18\]](#).
- Proactive sanctions compliance can help a company avoid legal and operational costs of violations that can run into millions of dollars [\[19\]](#).
- A company can avoid reputational damage from doing business with sanctioned entities.

## I Emphasize the Ethics of Sanctions Compliance

Studies show that companies that demonstrate their commitment to corporate ethics increase employee loyalty and, possibly, motivation [\[20, 21\]](#).

For example, consider the Uyghur Forced Labor Prevention Act and the sanctions on Russia for its invasion of Ukraine [\[22, 23\]](#). Polls show that most Americans support sanctions on China and Russia [\[24, 25, 26\]](#).

Corporate compliance programs should emphasize the “ethical upside” of sanctions to encourage compliance by employees.

## Encourage Senior Management to Support Compliance

Sanctions compliance may lead to decisions that are unpopular with operating teams, such as dropping a lucrative but risky customer. So the tone at the top of the company must emphasize compliance's value by advocating for strict compliance in all business activities.

Senior managers should demonstrate robust support for compliance officers. Announcing difficult business decisions alongside compliance officers will increase the respect from operational units towards compliance.

## Enact Enhanced Risk Assessments and Controls for Sanctions

Sanctions compliance programs need comprehensive risk assessments and controls. Those assessments must:

- Be customized to the company's sanctions risk profile, but remain flexible to adapt to business and regulatory changes.
- Monitor changes in sanction lists and entity lists.
- Follow compliance program guidance from the DOJ, USSC, and OFAC [6, 7, 27].

Unfortunately, one recent survey of compliance and ethics professionals revealed that only 45% had bolstered their sanctions risk controls [28]. When sanctions are becoming "the new FCPA," companies must urgently start improving their risk frameworks.

## Collect Comprehensive Intelligence on Customers and Third Parties

Sanctions compliance also requires more in-depth analysis of suppliers and customers to mitigate sanctions risks, with steps such as:

- Screening for sanctioned suppliers throughout the chain, whether direct, third-party, or fourth-party.
- Verifying that customers and suppliers are not money-laundering or trade-financing risks.
- Identifying the ultimate beneficial owners (UBOs) of customers and suppliers and ensuring that no UBO is a sanctioned entity.
- Remembering that sanctions apply if a risky customer's funds flow through the U.S. financial systems.

To implement these steps, a compliance program needs a platform with features like:

- Real-time access to external data on entities
- Monitoring of regulatory watchlists
- Integration of various screening services

## Centralize Compliance Data, Reporting, and Auditing

The program should seek to centralize all data on an enterprise-wide platform for the following benefits:

- Compliance and business teams can share mutually helpful data, like screening and revenue information on a customer.
- The platform becomes a system of record that is updated in real-time and offers the same data consistently to all teams.
- It can provide detailed data analytics and reports on sanctions risk levels by monitoring watchlists and integrating screening services.
- Companies can maintain detailed documentation and audit trails to show adherence to regulations and build defensible positions against investigations.
- Voluntary self-disclosure of any violations, along with proof of attempts to comply, can help a company avoid penalties [29].

## Centralize Compliance Data, Reporting, and Auditing

The program should seek to centralize all data on an enterprise-wide platform for the following benefits:

- Compliance and business teams can share mutually helpful data, like screening and revenue information on a customer.
- The platform becomes a system of record that is updated in real-time and offers the same data consistently to all teams.
- It can provide detailed data analytics and reports on sanctions risk levels by monitoring watchlists and integrating screening services.
- Companies can maintain detailed documentation and audit trails to show adherence to regulations and build defensible positions against investigations.
- Voluntary self-disclosure of any violations, along with proof of attempts to comply, can help a company avoid penalties [29].

## Focus on Remediation and Continuous Improvement

Since sanctions are still new to many corporate compliance programs, companies must design continuous improvement measures to:

- Conduct root-cause analyses of all sanctions compliance failures
- Design, test, and implement new risk controls to avoid failures in future
- Regularly review and update the compliance program

## Implement Rigorous Internal and External Training

Since sanctions rules can be complex, employees in compliance and business teams must receive training appropriate for their roles and responsibilities.

Compliance officers do have work to do on this point: One recent survey of compliance and ethics professionals revealed that just 25% of respondents planned to enhance their sanctions training [28].

This gap can be closed by training employees using simplified language, decision checklists, search tools, and automated integrated workflows rather than making them read pages of legalese [30].

## Upgrade Non-U.S. Corporate Compliance Programs for U.S. Sanctions

Just like the FCPA, many sanctions programs empower U.S. regulators to impose sanctions on non-U.S. persons and entities [31].

In other words, non-American companies that rely on U.S. financial and banking systems are at risk for enforcement too, and must also enhance their corporate compliance programs with the same strategies above.

# Conclusion

Enforcing sanctions is becoming a priority for geopolitical reasons. The good news is that many fundamentals of FCPA compliance carry over to sanctions too. But the bad news is that sanctions compliance is a different challenge that needs better corporate compliance programs.

Certa, an end-to-end third party risk management platform, helps implement and automate complex enterprise compliance programs for F100 companies globally.

Get in touch with our experts to learn more about how Certa can streamline your sanctions compliance program.





# Unified third party risk & compliance management, powered by AI.

Scale Your Compliance 

Evolve with Your Needs & Global Regulations 

Minimize Your Exposure 

Full Visibility, All in One Place 

Modern Enterprises rely on  certa

## Uber

Reduced 50% in operating costs. [Learn more >](#)

## box

Reduced vendor onboarding cycle times by nearly 80%  
cycle times by nearly 80%. [Learn more >](#)



Ready-to-use Modules for major Compliance use cases:

ABAC	Sanctions/OFAC 50
AML/KYC	UFLPA
LkSG	

**300%**  
Faster onboarding

**10x**  
Increase in efficiency

**100%**  
Transparency & control

**certa.ai**

