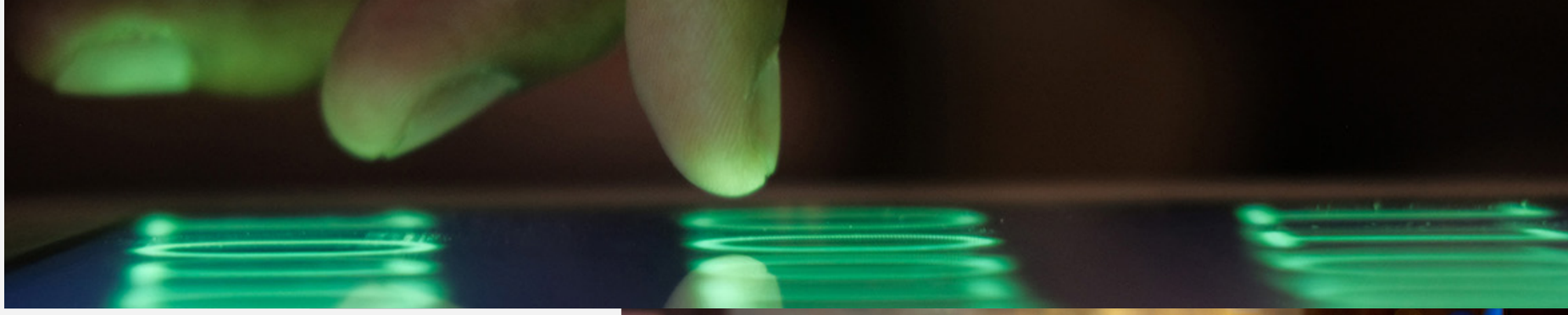


Meeting tomorrow’s challenges, embracing risk intelligently

PwC’s Global Economic Crime Survey 2024

pwc

Introduction

Risks are inevitable. It's whether a company takes, and mitigates, risks intelligently to grow and thrive that sets leaders apart.

In today's global, interconnected environment, economic crime is a pervasive challenge. Geopolitical pressures heighten sanctions and export controls risks. Exposure to bribery and corruption risks expands as global companies enter new markets in search of growth. There is increased public and regulatory scrutiny regarding use of forced labour and other environmental, social and governance (ESG) responsibilities—not just in companies but anywhere in the supply chains that support them. And, as the mergers and acquisitions market strengthens, acquirers can be exposed to potential liabilities associated with illegal acts hidden in their new assets. Economic crime risk is more complex than ever before—and it is far more challenging to both create value and protect it.

In parallel, governments around the world are signalling their rising expectations that companies do their part to prevent economic crime and more fully disclose its consequences. Regulatory enforcement and cross-border cooperation amongst law enforcement agencies are increasing in an effort to combat bad actors and the devastating impact their actions can have on individuals, businesses and economies.

It is against this backdrop that the PwC Forensics practice embarked on its Global Economic Crime Survey, the latest in a series of studies dating back more than 20 years. In our research, conducted between January and March 2024, PwC surveyed nearly 2,500 companies across 63 territories. Two-thirds of respondents were C-suite executives—including 450 General Counsel, Chief Compliance Officers and Chief Audit Executives—and 40% were from companies with revenues greater than US$1 billion. We also conducted over 45 interviews with senior executives from major corporations around the world to discuss their leading practices. This body of research gave us a unique lens on how today's boards and business leaders are addressing the economic crime risks their organisations are navigating daily.

We did a deep dive on some of the most challenging risks including procurement fraud, corruption, forced labour, export controls and sanctions. Our findings include:

1 **Fraud:** 55% report that procurement fraud is a widespread concern in their country, yet a minority are using available tools to identify or combat it. For example, nearly 20% do not use data analytics in any way to identify procurement fraud, and just 26% are leveraging data analytics to identify unusual bid patterns.

2 **Corruption:** 81% believe government efforts to enforce anti-corruption laws are becoming more robust or remaining steady in the countries in which they operate. While 77% are confident their compliance programmes can mitigate emerging risks, it is worrying that 42% of companies either don't have a third-party risk management programme or don't do any form of risk scoring as part of their programme.

3 **Forced labour:** 33% report that assessing the risk of forced labour in their supply chain is a priority for their company, and they have either assessed the risk or plan to in the near term. A third have mapped their supply chains to Tier 1 or Tier 2 suppliers, and in companies over US$5 billion in revenue, 65% have mapped to various extents.

4 **Export controls:** 59% agree that export controls have grown more complex, and more than half believe controls are being enforced more robustly than two years ago. While larger companies are unsurprisingly better prepared, just half of businesses overall say they have a robust export controls risk assessment process.

5 **Sanctions:** 44% of executives consider sanctions risk compliance a significant priority. Just 30% undertake a range of steps to test the strength of their sanctions compliance programme. Two-thirds consider the possibility of third parties engaging in impermissible activity a top two sanctions risk, which is a more than 20-point difference from other risks queried.

Across all of the risk areas surveyed, three common themes emerged as actions that could improve risk management and compliance: strengthening risk assessments, improving third-party risk management practices, and better leveraging data and analytics on behalf of compliance and investigations.

If management and boards don't already have a sense of urgency on the importance of analytics, they would be well-served to heed the US Department of Justice's words on the topic. In a recent speech, US Acting Assistant Attorney General Nicole M. Argentieri said, 'Just as we are upping our game when it comes to data analytics, we expect companies to do the same.' She added, 'Going forward, we are going to double down on these efforts to allow us to identify additional misconduct that may otherwise have gone undetected and bring to bear even more data, along with tools that can interpret and synthesise that information.'

For risk leaders, including those in Legal and Compliance functions, securing alignment with the CEO and board regarding the nexus between growth and risk is critical. PwC's most recent Global Risk Survey and Global Internal Audit Study both address the prevalence of a leadership disconnect on the appetite for risk and the opportunity for risk leaders to bring strategic insights to senior management to enable better decision-making.

When companies have the right data and insights to take risks with confidence, they can be more agile—whether in entering new markets or getting new products and services launched. Stakeholders and customers increase trust, investors build confidence, and growth and value creation result.

Throughout this report, we in the PwC Forensics practice share highlights of the regulatory and enforcement landscape globally and details on where companies stand in their efforts to improve risk management. We also feature leading practitioners' perspectives on critical steps to build compliance programmes that support businesses in maintaining trust and building resilience, contributing to the confidence to transform, invest and grow.

Meet tomorrow's challenges.
Embrace risk intelligently.

Leading Practice Interviews

From February through April 2024, partners and other executives from the PwC Forensics practice conducted in-depth interviews with dozens of senior Legal, Compliance and Internal Audit executives from major corporations around the world, as well as with partners from the Covington & Burling and Freshfields Bruckhaus Deringer law firms. These discussions supplemented our questionnaire-based field research and covered the four risk areas in focus for this edition of our Global Economic Crime Survey. The discussions were conducted on a no attribution basis, and each of the main sections of this report make reference to practices highlighted by one or more of the companies that participated in the process.

We thank all the executives listed below and others who preferred to contribute anonymously for sharing their perspectives with us.

Vishal Arora
ArcelorMittal, Luxembourg

Maaike de Bie
Vodafone

Mark Broom
Orange

Jason Brown
GE Appliances (GEA)

Matthew Bruce
Freshfields Bruckhaus Deringer

Eleanor Cabrere
Navistar International Corporation

Francesca Chiani
Carrefour Italia SpA

Carlo Daneo
Ferrari

Adriaan van Dorp
ABN AMRO Bank

Matthew Drew
Tesco Plc

Malisa Dubal
General Motors

Massimo Ferrari
Barilla Group

Lisa Flavin
Emerson Electric

Jason Hand
Rio Tinto

Jantien Heimel
Vattenfall the Netherlands

Lauren Higgins
Tate & Lyle PLC

André Jägeler
Zeppelin

Safet Kopov
Hensoldt

Tom van de Laar
Rabobank Group

Roger Saldaña Madero
CEMEX

Shinobu Obata
NEC Corporation

Nicolas Petrovic
Sodexo

Paolo Quaini
ITA Airways

Alex Robinson
Nokia

Justin Ross
FedEx

Stefano Russo
EssilorLuxottica Group

Jennifer Saperstein
Covington & Burling

Jean-Christophe Sautory
L'Oréal

Tjerk Schlufter
Fresenius SE & Co. KGaA

Diederick Slijkerman
ProRail

Ignacio Gabriel Stepancic
Grupo Bimbo

Nina Stoeckel
C.H. Boehringer Sohn AG & Co. KG

Eric Strootman
ING Group

Jenny Tan
CapitaLand Investment Limited

Wouter de Veen
The HEINEKEN Company

Robert Walsh
AXA Group

Fraud

A fresh look at a persistent problem—procurement fraud

In all of its forms, fraud remains a persistent challenge.

Procurement fraud—one of the oldest forms of fraud—is still all too common. It is a significant cause for concern for small businesses and multinationals alike, regardless of geography or industry sector.

Our survey shows that procurement fraud, specifically, is among the top three most disruptive economic crimes experienced by companies globally in the past 24 months. More than half say procurement fraud is a widespread concern in their country.

While data to support diligence efforts on third parties is often plentiful and enterprise resource planning (ERP) systems reinforce good hygiene in procure-to-pay processes, technology isn't solely a force for good. In the hands of criminals, advanced technology also enables sophisticated efforts to perpetrate procurement fraud.

Risks are accentuated as companies move into new markets or begin sourcing from new countries. In some instances, with operations being established further from educational hubs, securing adequately qualified professionals, especially in gatekeeper roles, can be a challenge. Deploying effective training on conflict of interest policies, procurement processes and fraud controls can be slow to start or intermittent in frequency.

In the face of such challenges, management would be well-served to revisit risk assessment processes, redouble training efforts, and explore enhanced controls that rely to a greater extent on data analytics and automation.

A deeper look

The good news is that 59% of companies completed an enterprise-wide fraud risk assessment in the last 12 months, and a further 12% plan to do so within a year. Nearly three-quarters (71%) say the board is regularly updated on efforts to investigate allegations or mitigate fraud risk.

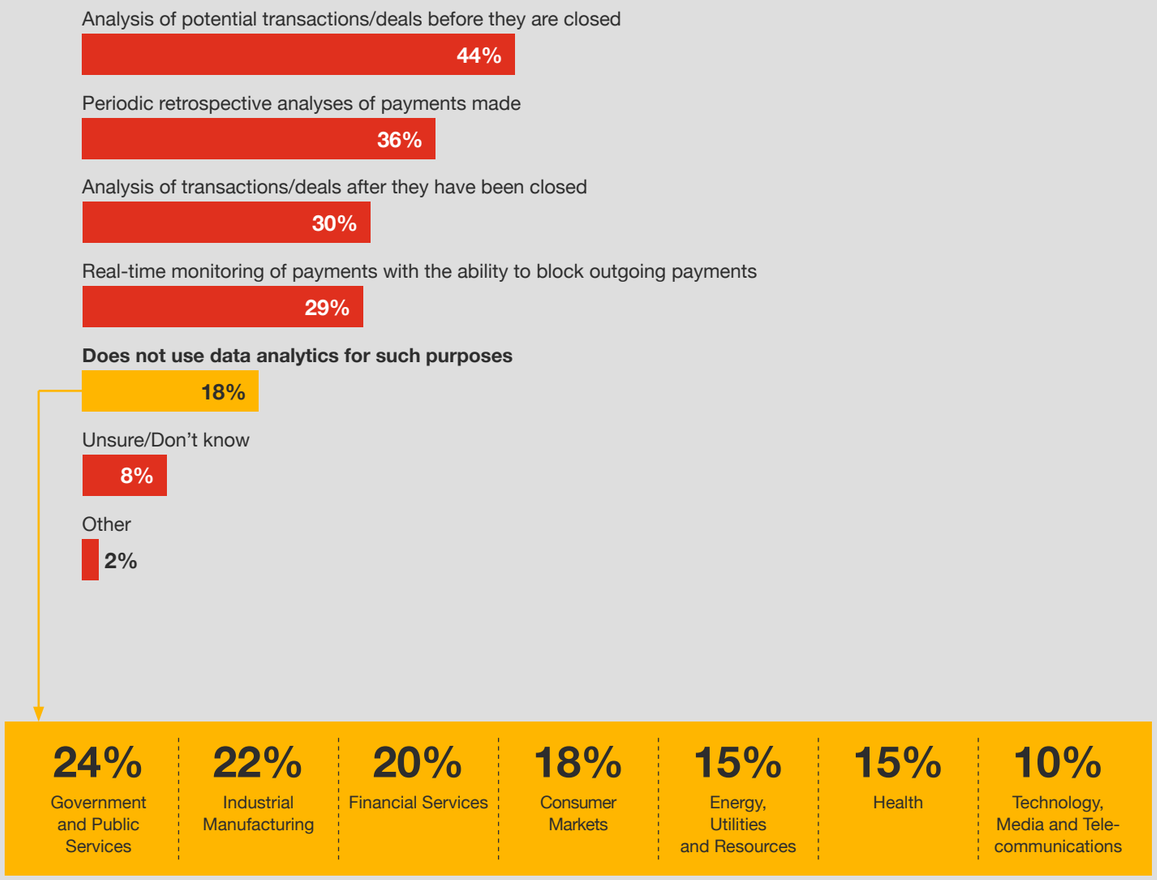
However, there is substantial room for improvement. Nearly 20% of companies do not use data analytics in any way to identify procurement fraud. Industrial Manufacturing (IM) lags all other industries in this regard, signalling significant opportunity to employ more advanced fraud detection techniques. In contrast, Technology, Media and Telecommunications (TMT) leads in analytics use, with 90% of companies using some form of analytics to identify procurement fraud, including to analyse transactions before they close and to conduct real-time monitoring of payments. TMT's analytics use likely contributes to why a smaller share of those in the sector report the procurement fraud they experienced had serious impact.

In addition, many companies are not aware of the scale of their losses to procurement fraud. Nearly a third (32%) do not attempt to quantify these losses, and another third (31%) do so only on an infrequent or ad hoc basis. As in analytics use, the TMT sector leads in quantification efforts along with Financial Services (FS), while IM lags, with just 17% quantifying procurement fraud loss at least annually.

When it comes to mitigating the risk of procurement fraud, the vast majority are strengthening processes regarding documentation and authorisation and are revising vendor selection processes.

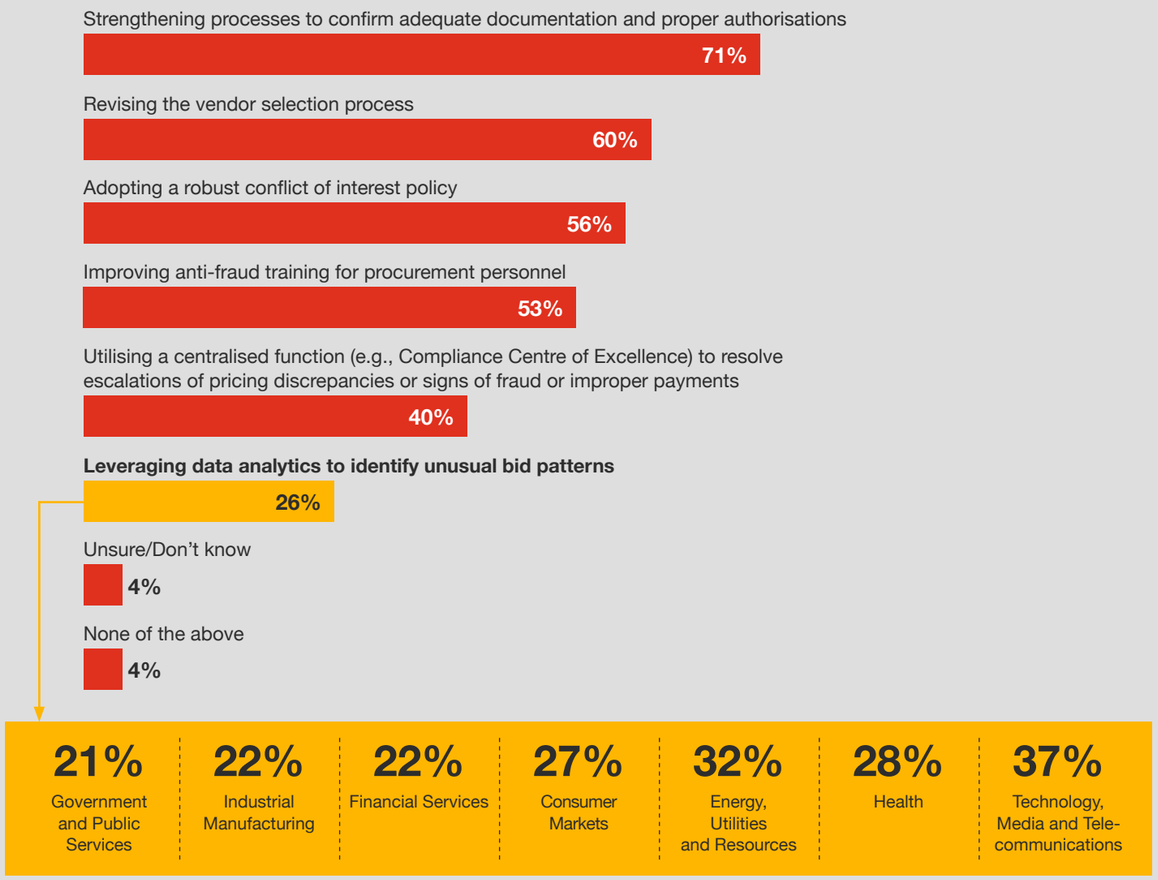
Far fewer are using data analytics. TMT also leads in using analytics to identify unusual bid patterns. Energy, Utilities and Resources (EUR) is a close second in use of analytics which is not surprising given the industry is the sector most concerned about procurement fraud. Given that companies in the sector manage huge capital expenditure projects and often operate in challenging jurisdictions, they have good reasons to aggressively manage the risk.

Data analytics—an essential element, overlooked by some



Q8. How does your organisation use data analytics to identify procurement fraud, waste or abuse? Base: All respondents = 2446

Uncovering bid rigging—a missed opportunity



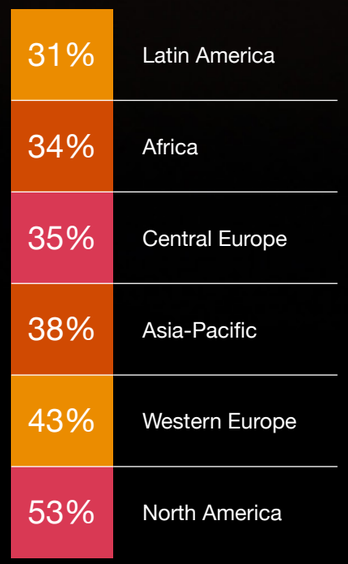
Q11. What steps, if any, is your organisation taking to mitigate the risk of procurement fraud? Base: All respondents = 2446

TMT, Energy, Utilities and Resources (EUR) and Health sectors also more often have a centralised function to resolve escalations of pricing discrepancies or signs of fraud or improper payments. North America stands out for employing this leading practice, with 53% utilising a centralised Compliance function.

Strengthen anti-fraud efforts through escalation—Centres of Excellence can help

40%

Utilising a centralised Compliance function (e.g., Compliance Centre of Excellence) to resolve escalations of pricing discrepancies or signs of fraud or improper payments



Q11. What steps, if any, is your organisation taking to mitigate the risk of procurement fraud? Response choice: utilising a centralised Compliance function (e.g., Compliance Centre of Excellence) to resolve escalations of pricing discrepancies or signs of fraud or improper payments.
Base: All respondents = 2446

Please note that the percentages do not add up to 100% due to rounding.

The takeaway

Risk assessments don't get better with age

Procurement fraud erodes profitability, destroys value and undermines a positive corporate culture. Unfortunately, bad actors exist inside and outside of the business. Insider threats are not limited to cybercrime or intellectual property theft—countering procurement fraud should be an element of companies' insider threat programmes. Businesses should regularly refresh risk assessments for their highest-risk segments and geographies and improve efforts to risk score vendors by including more varied sources of data. Companies should also consider offboarding vendors without activity in the prior 12 months and refreshing risk scores relatively more frequently for the highest-risk vendors.

Implementing a robust procurement fraud risk management effort often requires involvement by individuals at mid-management levels, not just from Procurement and Supply Chain, but also from Human Resources, Information Technology Security, Compliance, Internal Audit and Investigations. This combination helps to make fraud risk more visible within the organisation, and to align objectives and efforts across the enterprise.

Companies within a given industry sector may also benefit from considering a consortium model, partnering with both public and private organisations to share intelligence where appropriate on trends, known risks and anti-fraud strategies. The US insurance industry has successfully adopted this collaborative approach, leveraging large data sets to train anti-fraud analytic platforms. This model is finding increasing traction on a global basis.

Insights from leading practitioners

Our Leading Practice Interviewees had further recommendations, including:

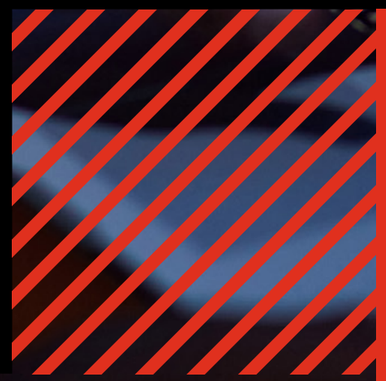
Encourage a speak up culture.
When the company's contracts with suppliers are technically complex, the possibility of request for proposal manipulation and bid rigging is elevated. Whistleblowers are often critical to uncovering misconduct.

Maintain a robust COI policy.
A well-defined conflict of interest (COI) policy is essential, as is regular training on that policy. Some of our interview respondents ask staff to complete both a pre-employment COI questionnaire and a post-employment certification, which together raise awareness of the risk and can increase the number of reported matters.

Break down silos.
Avoiding internal silos is important. The Compliance function needs to secure buy-in from procurement on a risk-based approach to third parties, including due diligence ahead of onboarding, onsite audits where appropriate and re-screening of legacy vendors. Internal Audit is another key partner, and while its risk metrics may differ from Compliance, the two functions need to team closely and have access to the other's data analytics and related dashboards.

Explore AI and GenAI use cases.
Artificial Intelligence (AI) and Generative AI (GenAI), in combination with advanced analytics and automation, can contribute to better contract lifecycle management and assist in identifying procurement-related risks through enhanced monitoring.

Strengthen defences.
Technology is unfortunately part of the problem too. Criminal organisations, some of our interviewees explained, are using AI to create fake invoices and to impersonate senior executives as part of spear-phishing attacks. Other respondents emphasised the role played by employees in facilitating procurement fraud and advocated that these risks be addressed as part of the company's insider threat programme. Continuous monitoring of employee emails, where legal and feasible, was mentioned by several executives.



Advanced transaction monitoring for procurement fraud

Transaction monitoring solutions for procurement fraud utilise sophisticated algorithms and machine learning techniques to detect suspicious activities and patterns in procurement transactions. By analysing vast amounts of data, these solutions can identify potential instances of fraud, such as overbilling, kickbacks and collusion.

Combining these solutions with graph analytics can further enhance effectiveness. Graph analytics enables companies to visualise and analyse complex relationships between entities such as suppliers, employees, and third parties. Due diligence using publicly available company records can help organisations map out relationships and connections of entities, allowing them to gain a more holistic understanding of the beneficial owners of third parties and identify any potential conflicts of interest or hidden relationships. This combination of transaction monitoring and graph analytics can significantly reduce the risk of procurement fraud and other improper payments.

Corruption

Governments around the world are signalling their rising expectations that corporate compliance programmes become more sophisticated.

Rising expectations and missed opportunities—today's third-party risk management challenges

Law enforcement authorities and regulators have raised the bar for third-party risk management as well as the use of data analytics in support of compliance and investigation efforts. New or recently revised protections or incentives for whistleblowers in numerous jurisdictions increase the pressure on companies to learn of and react to allegations of misconduct quickly, whether that conduct is within the company or at a third party. The decision regarding whether, and to whom, to self-report is as fraught as ever.

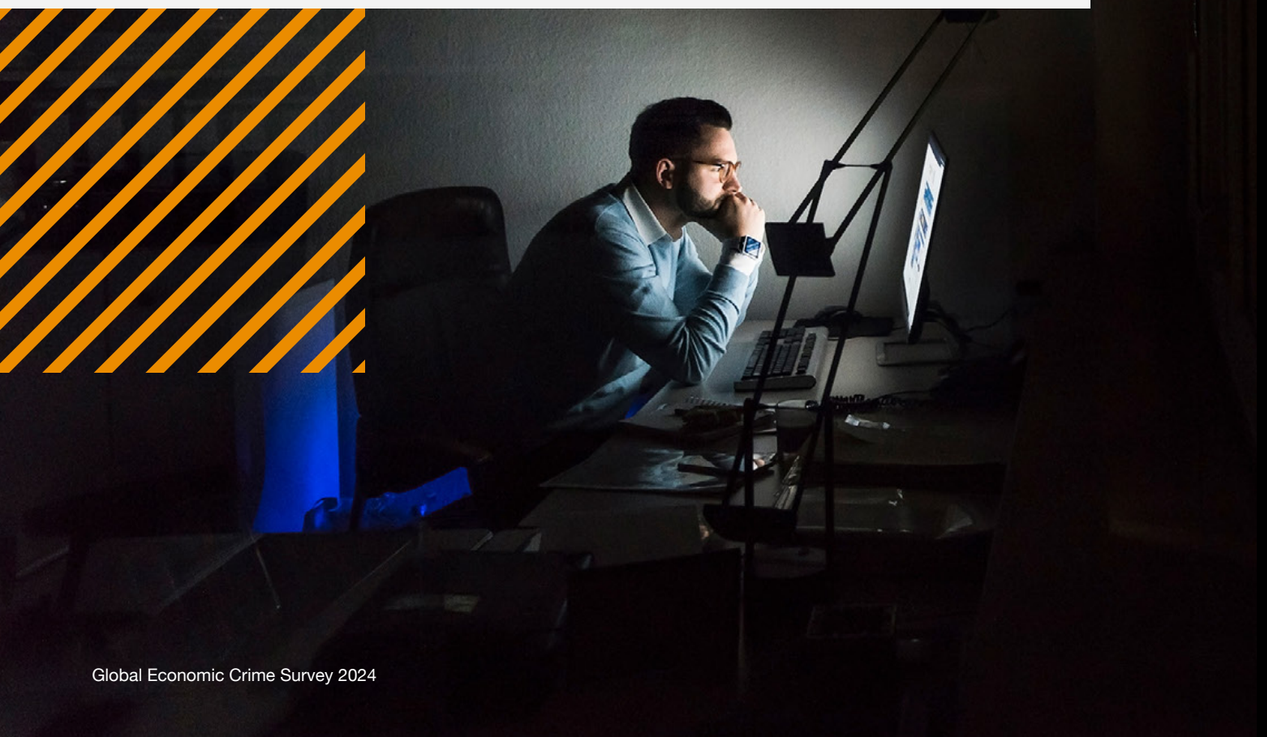
The US Department of Justice (DoJ), for example, has established a range of programmes to encourage whistleblowers. One pilot programme[i] aims to fill in the gaps in existing whistleblower programmes from the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission, focusing on financial crime, foreign bribery outside of the SEC's jurisdiction, domestic bribery, and the newly adopted Foreign Extortion Prevention Act (FEPA).[ii]

Another pilot programme offers the possibility of non-prosecution agreements to individuals who voluntarily self-disclose actionable and original information on criminal conduct.[iii] How successful these DoJ programmes will be remains to be seen, but for context, in Fiscal 2023, the SEC received more than 18,000 tips and paid out nearly US$600 million in awards to 68 whistleblowers, an average of almost US$9 million per payment.[iv]

In addition, the DoJ has clarified guidance relating to corruption-related matters in the context of mergers and acquisitions, making it clear that the Department expects self-disclosure within six months, remediation within a year, and the disgorgement of ill-gotten gains.[v] In most cases, corporations that meet DoJ expectations could likely expect declinations. Meanwhile, industry-sector sweeps are continuing, and traditional monitorships appear to be giving way to 'self-monitorships.'

'FCPA enforcement has been active and robust for at least the last 15 years, and it will remain a cornerstone of the corporate enforcement programmes at DoJ and the SEC. The FCPA units at each agency continue to be heavily resourced. And politically, support for anti-corruption remains strong, as evidenced by the Foreign Extortion Prevention Act, which will provide DoJ yet another avenue for reaching corrupt conduct as part of an integrated enforcement toolkit, including the FCPA, the FEPA, anti–money laundering laws, fraud statutes and other federal criminal statutes.'

Steven Fagell, Covington & Burling



Surfacing new allegations of wrongdoing is clearly the over-arching priority. 'In addition to voluntary disclosure and whistleblower programmes, the DoJ and the SEC will continue to leverage news sources, web crawlers, collaboration with foreign counterparts, information gleaned in ongoing investigations, and advancements in AI, data analytics, and other technologies to prowl for new cases,' as Adam Studner of the Covington & Burling law firm observed. 'The long and short of it is: a robust anti-corruption enforcement environment is here to stay.'

Outside the US, there have been many notable developments. The United Kingdom has a new Serious Fraud Office Director, who is likely to lead a larger organisation, wielding new pre-investigation powers under the recently adopted Economic Crime and Corporate Transparency Act 2023.[vi] France has revised its guidelines on deferred prosecution agreements, offering significant incentives for timely self-disclosure and robust internal investigations.[vii]

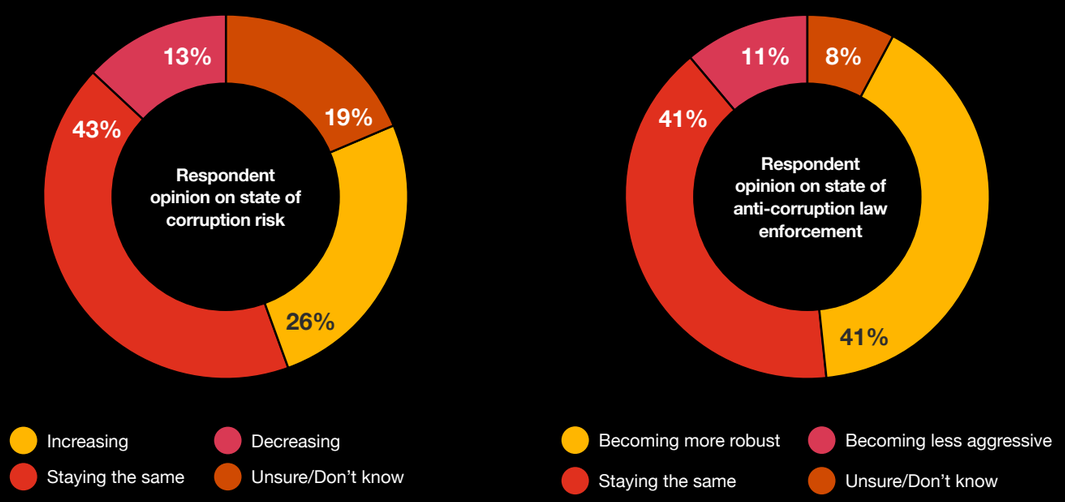
In Germany, while there has not been progress on corporate criminal liability reform, a new Whistleblower Protection Act was adopted to implement the EU's Whistleblower Directive.[viii] And from January 2024, Germany's Supply Chain Act will impose certain additional human rights and environmental due diligence obligations on companies with as few as 1,000 employees.[ix]

In Asia-Pacific, Australia's Parliament adopted the Combatting Foreign Bribery Bill, a long-delayed but landmark legislative change that introduces a new absolute liability offense of failing to prevent bribery of a foreign public official.[x] High profile corruption scandals in Japan, South Korea, and Malaysia garnered headlines and may signal willingness to more aggressively prosecute domestic and foreign bribery.

Given all of the above, it is not surprising that our survey confirmed more than eight in ten (81%) executives believe government efforts to enforce anti-corruption laws are becoming more robust or remaining steady in the countries in which they operate—that number reaches 92% for respondents based in North America.

The pressure on companies to establish and maintain effective anti-corruption compliance programmes, leveraging data analytics to inform and accelerate decision-making, is clearly significant. Robust third-party risk management remains a core issue given that third parties are involved in most major incidents of bribery or corruption. In fact, all corporate FCPA resolutions in 2023 involved payments to foreign government officials that were channelled through third parties.[xi]

Corruption risks are not receding, while enforcement efforts are gathering pace



Q12. In your opinion, have risks associated with corrupt or improper payments to government officials/and or commercial customers increased, decreased or stayed the same in the last 12 months in the country where you live? Base: All respondents = 2446. Q14. How are government efforts to enforce anti-corruption laws changing in the country/countries in which you operate? Base: All respondents = 2446

Please note that the percentages do not add up to 100% due to rounding.

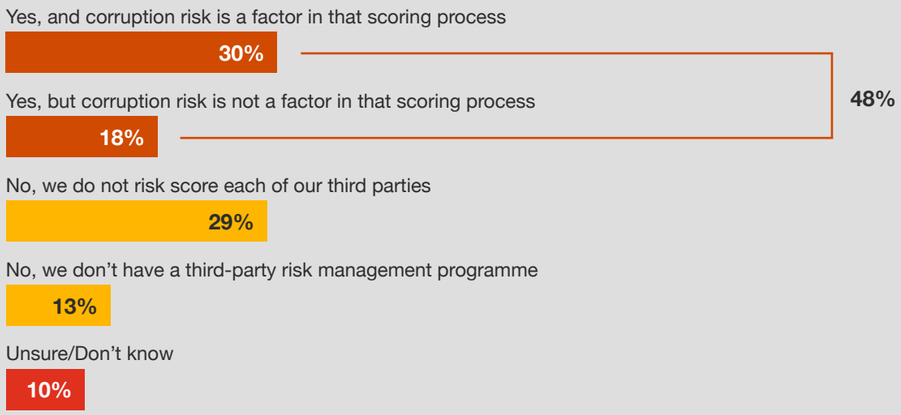
A deeper look

On the surface, executives show confidence that their compliance programmes can mitigate emerging corruption risks. More than three-fourths (77%) agree they have it handled. Contributing to this compliance programme confidence is that nearly as many (70%) are confident that their company has a complete and accurate understanding of all third parties (vendors, channel partners and other third-party intermediaries). This could very likely be false confidence, as a deeper look shows that most are not universally employing the best practices needed to effectively mitigate third-party risk and combat corruption in today's environment.

PwC finds that, in practice, it is very common for even multi-billion-dollar, publicly traded companies to have incomplete information about their suppliers, distributors and other third-party service providers. Sometimes it is because of disparate systems from prior acquisitions, or from having divisions, regions or countries that enjoy significant operational autonomy. Without an integrated accounting system as well as a vendor/accounts payable management system, gaining a complete view of existing third parties can be difficult. Nonetheless, the importance of ongoing monitoring of third parties—and robust diligence on higher-risk new third parties—cannot be overstated.

Among the components of an effective third-party anti-corruption compliance programme, risk scoring, monitoring and audits are all critical. Here's where companies stand on these fronts. Half (48%) conduct risk scoring as part of their third-party risk management, and nearly two-thirds of those that risk score consider corruption risk in that process. What's alarming is that 42% of companies either don't have a third-party risk management programme at all or, if they do, risk scoring is not done.

Room for improvement in risk scoring



Q15. Does your organisation assign a risk score to each of its third parties as part of its third-party risk management programme?
Base: All respondents = 2446

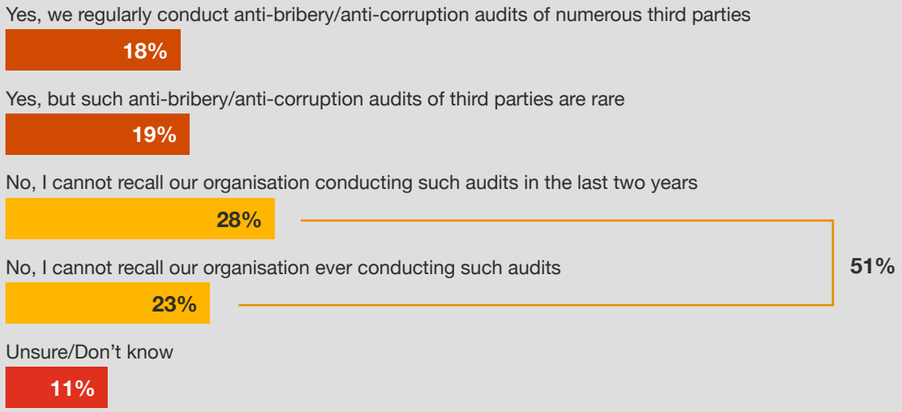
Of course, third-party risk management programmes should reflect the risk profile of the organisation. However, it is important to recognise that standard third-party onboarding is not the same as due diligence from a corruption perspective. Every company would benefit from some form of risk scoring. Without it, there is no other way to tier the level of due diligence and ongoing monitoring that one party merits relative to another. Regions where risk scoring occurs the least include Asia-Pacific and Latin America. Even in North America, 29% of respondent companies don't risk score third parties.

When it comes to anti-bribery/anti-corruption audits of third parties, just 18% of companies conduct such audits regularly. This percentage is higher in the TMT and Health sectors, while substantially lower than the average in EUR. Clearly all sectors have much room for improvement. Respondent companies in North America conduct regular anti-bribery/anti-corruption audits at nearly twice the rate of many other regions.

The use of data analytics, a robust internal investigation process and root cause analyses are all important elements in an effective anti-corruption compliance programme. For example, some companies, particularly in FS, TMT and Health, are using analytics to do continuous monitoring of certain transaction types. What's notable is that 23% are not using data analytics to support the Compliance function in any way. Given that data analytics does not have to be expensive to implement, this is truly a missed opportunity for these businesses.

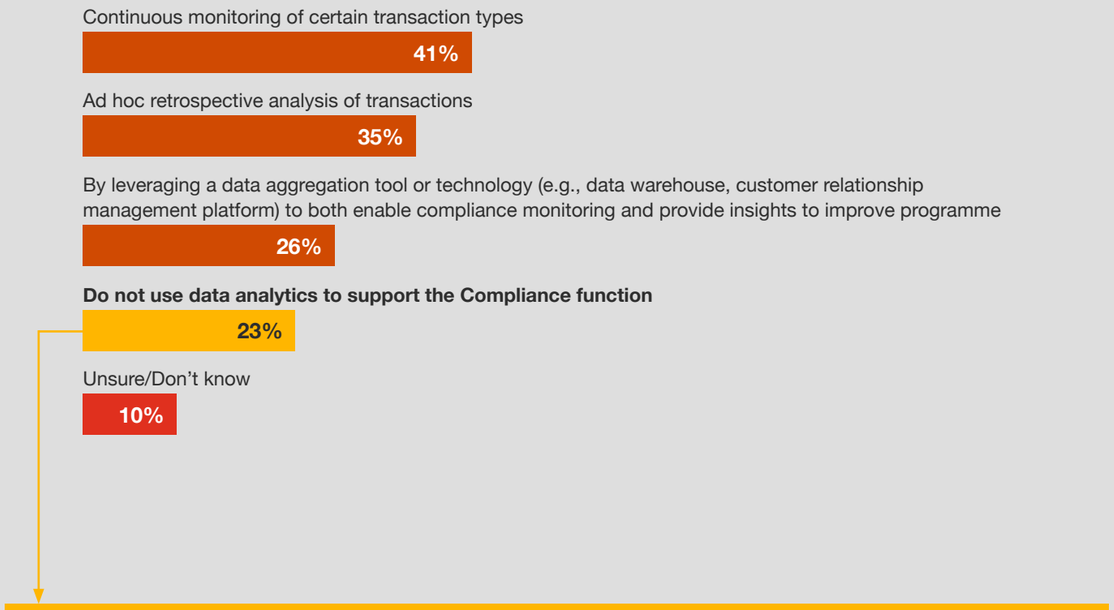
'While companies are seeking to innovate and use data analytics in their compliance and ethics programmes, they tend to still rely on traditional tools and methods, such as whistleblowing hotlines, policies and training,' noted Ben Morgan of the Freshfields Bruckhaus Deringer law firm. 'We think this is an area that will become more important and relevant in the future, especially in light of the DoJ's and the UK Serious Fraud Office's expectations around reasonable procedures and corporate compliance.'

On-site audits—underused and underappreciated



Q16. Has your organisation conducted an anti-bribery/anti-corruption audit at one or more of its third parties in the last two years?
Base: All respondents = 2446

Anti-corruption compliance without data analytics? A cause for concern



Q18. How does your organisation use data analytics in support of its anti-corruption compliance objectives?
Base: All respondents = 2446

Well-designed internal investigation processes can help speed response times to allegations of inappropriate conduct (which is particularly important given substantial incentives for whistleblowers to report to government entities) and can better inform the company's decision-making regarding self-reporting. Having established these processes, it is important to regularly review them, especially as the expectations of regulators and law enforcement evolve and data privacy laws change. Nearly 40% of companies are meeting this goal, having reviewed their process within the last 12 months. In contrast, 30% have not done a review within the last year, and an additional 16% don't have an investigation function at all.

Best began once a substantial portion of the facts are known in an investigation, root cause analysis to better understand the 'why' and the 'how' of a fraud is an essential element of continuous improvement. Such analysis can include, for example, the identification of internal control gaps, system limitations, or instances of management override, as well as factors external to the company. This is low-hanging fruit for nearly half of companies that are currently either not doing root cause analysis or are doing so infrequently or without applying lessons learned. Companies would be well-served to not focus too narrowly on the specific issues that arose in an investigation, but rather to broaden the scope of their analysis to consider how the root causes might materialise elsewhere in the business.

The takeaway

Conducting effective third-party anti-corruption audits

It is not only good business—but prudent from a compliance perspective—for companies to regularly review both their approach to assessing and monitoring their third parties and to performing anti-corruption compliance audits.

Companies should consider the frequency and type of audits they utilise. Unfortunately, companies too often exercise audit rights reactively rather than proactively. Assessments of lower-risk third parties are often performed remotely, using desktop procedures focused on information that is already available internally, often without the third party's involvement or awareness. The primary focus is on analysing internal company documentation for compliance with applicable due diligence procedures and testing transactions from the company's internal accounts payable and/or expense data for red flags.

For higher-risk third parties, companies should consider the value of in-person, onsite visits to the third party's facilities. Such visits are typically incremental to the desktop work and can include, for example, the addition of interviews with third-party personnel, an assessment of the third party's compliance programme, and transaction testing from the third party's books and records. These audits, especially those that include transaction testing, require more resources to perform and involve significantly more socialisation and alignment both within the organisation and externally with the third party. However, the resulting insights can be considerably more valuable than those developed through desktop procedures alone.

The third-party audit selection methodology should be risk-based and incorporate input from not just Compliance, but the business and other functions. What companies should avoid, however, is falling into a routine of following informal, undocumented practices that are inconsistent and cannot be objectively justified and may result in an aversion to selecting third parties that may be particularly sensitive or challenging to assess. The frequency with which a given third party is subjected to onsite audit can be risk-weighted; suppliers that pass an audit with high marks may not need to be revisited for three or four years, extenuating circumstances notwithstanding.

The investigative process and the board's role

An effective investigative function contributes to both risk mitigation and compliance. Many enforcement agencies specifically consider how the company investigates misconduct when evaluating a corporate compliance programme. Boards of directors should, therefore, regularly press management to revisit how they manage their internal investigation function, with a specific focus on how data is collected and reviewed, root cause analyses are performed, and lessons learned are fed back to inform continuous improvement. Key performance indicators (KPIs) to track the effectiveness and efficiency of the investigative process, as well as monitor for trends, include such metrics as incident report volume (reports per 100 employees), substantiation rate, average time to substantiation decision, cases by incident type and by location, and average days to close cases, among others.

Insights from leading practitioners

Our Leading Practice Interviewees had further recommendations, including:

Leverage predictive analytics.
Take steps to explore the use of AI to produce next-level predictive analytics, utilising disparate sources of data from within the company (e.g., gifts and entertainment spending, whistleblower hotline activity, human resources reviews) and about external parties (e.g., changes in use of suppliers or channel partners) that may identify business units or geographies at higher-risk.

Consider AI to monitor regulatory change.
For companies operating in dozens of countries, consider GenAI tools that can read, interpret and monitor regulations across markets concerning changes, for example, to the legal definition of public officials, corporate criminal liability or public procurement tendering rules, allowing in-house legal and compliance to engage external counsel on the most complex developments.

Conduct employee surveys.
Brief annual employee surveys focusing on ethics and compliance can provide useful additional data points to inform other risk management activities. Embedding these short surveys into annual compliance training can increase participation rates.

Embrace ombuds programmes.
Establishing a network of ombuds—or 'compliance champions' in the business units/company locations who are not full-time members of the compliance organisation—can be highly effective, as they help disseminate key messages and best practices while contributing to a willingness of employees to raise issues. These roles can be time-limited to increase the number of business executives who have more intense interactions with the Compliance function.

Strengthen country risk rankings.
Country risk rankings should go beyond simply using the Transparency International Corruption Perceptions Index score and cursory reviews of government touchpoints. Compliance and internal audit should team to agree on a range of external and internal data sources that can form a more holistic view of risk in each of the countries where the business operates, including recent acquisitions or divestitures, compliance concerns raised, results of internal investigations, prior internal audit findings, employee survey results, etc.

Benchmark your compliance programme.
Periodically undertake compliance programme assessments designed to benchmark existing programmes against regulatory expectations and peer best practices.

Enterprise-level data warehouses drive compliance programme effectiveness too

Enterprise-level data warehouses, which already exist in many larger companies for business purposes, can utilise advanced analytics and data mining techniques to extract valuable insights for the Compliance function too. Advanced targeted analytics can help companies identify high-risk areas, such as regions or departments with a higher likelihood of corruption, and take proactive measures to mitigate those risks. The integration of disparate data sources, such as regional ERP systems, treasury systems, learning management systems, expense management systems, hotline and investigation management systems, and third-party due diligence systems, allows for more accurate and efficient monitoring of financial transactions and related event data.

Furthermore, these data warehouses enable companies to holistically monitor and track KPIs related to corruption detection, prevention and compliance. Example KPIs include incident reporting rates, compliance training completion rates, compliance audit results, and third-party compliance training. By analysing these KPIs, companies can assess the effectiveness of their frontline processes, controls and overall compliance programmes. Enterprise-level data warehouses enhance compliance programme effectiveness by ensuring consistent and standardised reporting, making it easier to demonstrate compliance with regulations and internal policies.

Moreover, enterprise-level data warehouses enable companies to expedite investigations into potential violations and respond quickly to whistleblower allegations, audit examinations or regulator inquiries. By accessing and analysing relevant data from the disparate source systems that are already consolidated in the data warehouse, companies can quickly gather evidence, identify responsible parties, and take appropriate disciplinary or legal actions in less time and by using less internal and external technical resources.

Supply Chain

Protecting human rights through deep supply chain visibility

Rising public scrutiny and a rapidly evolving regulatory landscape are placing increased pressure on companies to identify and mitigate risks associated with forced labour and other human rights abuses in their supply chains.

As Tom Plotkin of the Covington & Burling law firm has noted, key changes include 'significant recent developments in the European Union and intensifying enforcement by US authorities. These compliance challenges are not limited to a narrow set of industry sectors operating in a handful of higher-risk jurisdictions, but rather impact all companies doing business globally.'

Many of the new and emerging regulations in the EU, including the Corporate Sustainability Due Diligence Directive,[xii] are mandating supply chain mapping and human rights–related risk assessments. Case in point: the reporting requirements mandated in the EU's Corporate Sustainability Reporting Directive (CSRD), which went into effect in January 2024, include, in certain circumstances, that companies disclose information about human rights and forced labour issues in their value chains.[xiii] Our survey shows that nearly three-fourths of companies for which CSRD may be relevant have determined its applicability to their organisations. However, the remaining 27% have either not heard of CSRD or have not yet studied it to assess whether their business is impacted. Furthermore, in March 2024 the European Council and Parliament announced a provisional agreement to prohibit products made with forced labour.

In the US, intensifying enforcement has been largely focused on supply chain forced labour risks and, in particular, potential violations of the Uyghur Forced Labor Prevention Act (UFLPA).[xiv] US Customs and Border Protection detained US$1.42 billion in shipments in 2023 as part of its UFLPA enforcement, impacting sectors including automotive, apparel, electronics, pharmaceutical products, and others.[xv]

A deeper look

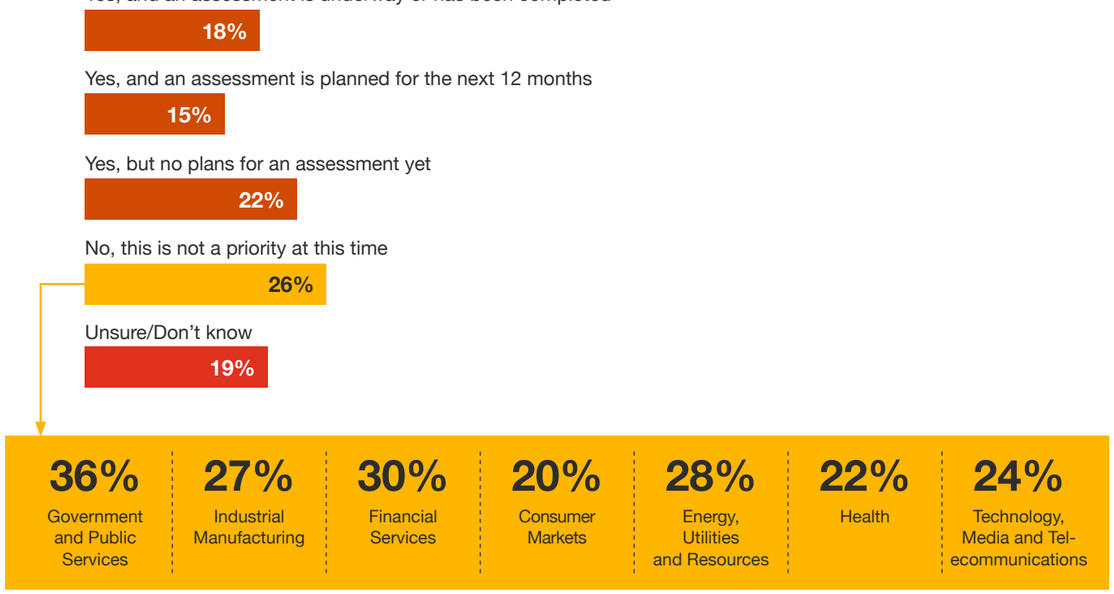
The good news for companies and their boards is that there are excellent resources available to guide corporate efforts. 'Companies setting out on their human rights/forced labour compliance journey,' explained Tom Plotkin, 'would be wise to consult two foundational documents—the United Nations Guiding Principles on Business and Human Rights and the OECD Due Diligence Guidance for Responsible Business Conduct.' These documents lay out many of the essential elements of an effective compliance programme and are helpful benchmarks to assess both existing and nascent programmes.

Given that one in three executives globally (33%) believe assessing the risk of forced labour in their supply chain is a priority for their company and that nearly 50% of those in Western Europe have done a risk assessment or are planning one in the coming year, hopefully these companies are availing themselves of the UN and OECD guidance.

To fully understand where within their supply chains the highest human rights risks lie, many companies have started down the path of supply chain mapping. More than one-third (36%) have mapped their supply chains to Tier 1 (T1) or Tier 2 (T2) suppliers. Nearly 50% of those in Western Europe and North America have mapped their supply chains to T1 or T2.

Across sectors, the Consumer Markets (CM) sector is furthest along in its mapping, with 42% having mapped to T1 or T2. As the effort to get to Tier N can be resource intensive, developing a sophisticated supplier engagement strategy, as well as understanding the associated technical complexities, is essential.

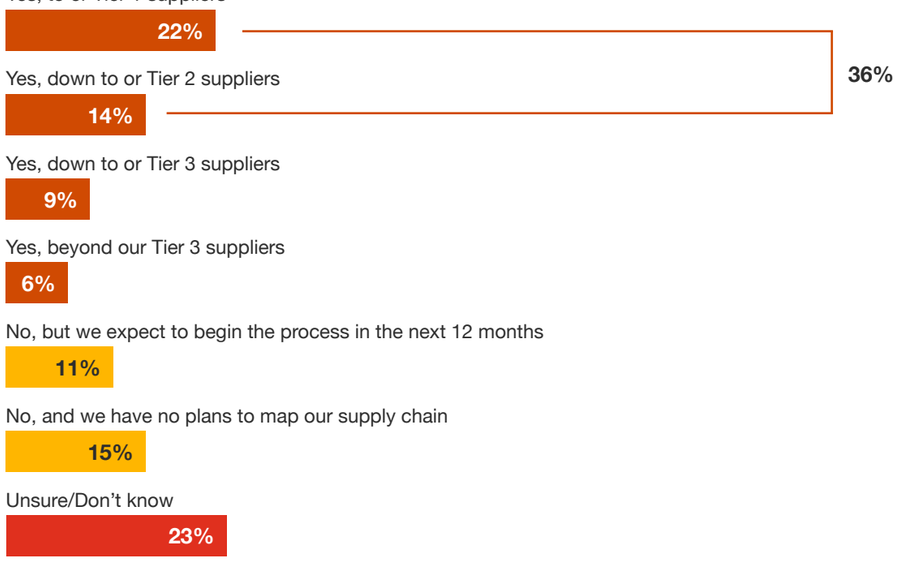
Forced labour risk assessments—a priority? Perhaps too little focus for too many



Q23. Regardless of whether your company is covered or not by the CSRD, do you believe that assessing the risk of forced labour in your supply chain is a priority for your organisation? Base: All respondents = 2446

Unfortunately, our research suggests that not every industry sector with significant forced labour risk is sensitive to it. While 40% of companies in the EUR and 38% in the TMT sectors have done, or are planning to do, an assessment of this risk, companies in the IM sector are lagging. Half (50%) of IM companies say it is either not a priority or that forced labour is an important issue, yet they have no plans to assess their risk.

Supply chain mapping—beginning the journey



Q24. Has your organisation mapped its supply chain? Base: All respondents = 2446

Onsite audits are another tool that can help with understanding the working conditions and practices at a given high-risk vendor. Unlike the momentum around supply chain mapping, a minority is using third-party audits to assess supplier compliance with forced labour regulations. In fact, just 15% of companies conduct such audits regularly, with companies in North America and Western Europe and those with revenues greater than US$ 5 billion leading the way. A greater share of companies in CM (20%) regularly audit for forced labour, and an additional 20% do so infrequently.

So, what would motivate a company to implement a robust third-party audit programme regarding forced labour? Our survey shows the top motives would be a law enforcement or a regulatory investigation of the company or, interestingly, that it is simply the right thing to do. Adverse publicity about the company's supply chain practices is also among the top three. In sum, two of the top three catalysts reported are reactive in nature. Pressure from non-governmental organisations is lowest on the list.

The police are at the door—and other factors that would drive a new approach to third-party forced labour audits

Q26. Which of the following would lead your organisation to implement a robust programme of third-party audits regarding forced labour? (Ranked in top three). Base: All respondents = 2446

The takeaway

Proactive board involvement

Given the scrutiny being placed on forced labour in companies' supply chains, boards of directors should prioritise the issue before it transforms into a crisis to manage in response to external pressure. In practice, this begins with requiring annual updates from management including progress on supply chain mapping. By demanding such updates, boards of directors can demonstrate their level of ambition for addressing forced labour risks and holding management accountable. These updates should include a comprehensive risk assessment of the company's supply chain, prepared by a cross-functional working group and identifying any potential risk factors or red flags that may indicate the presence of forced labour. Reassessments of existing supply chain maps should occur at least annually, and companies would be wise to include contractual language with key suppliers obligating them to update the company regarding changes to at least their own T1 suppliers. All of these efforts will contribute to the first, second and third lines working together to address this risk in an integrated assurance approach.

Through existing supplier relationships, or onboarding processes, companies can collect relevant information, such as the location of manufacturing or processing and the type of workforce involved in the work, and identify potential risks or actual human rights impacts. Furthermore, companies can take proactive measures such as conducting thorough due diligence on entities exhibiting warning signs that may indicate the presence of forced labour or human rights abuses. This should set off appropriate mitigation and remediation actions, such as engaging with suppliers to improve working conditions or seeking alternative suppliers that adhere to ethical standards.

Robust onsite audits

As noted, onsite audits can be a valuable tool to identify potential violations. Exactly which function conducts these audits often depends on the operating model of the business; Compliance or a 'responsible sourcing function' are two common choices. Post-audit readouts should be shared widely, including with the Internal Audit function. The risk owner can vary too, though in more mature organisations the risk is owned by the business.

It is worth noting that this practice should be embedded into a wider supplier risk management framework. By itself, the practice of audits as an assessment for social and ethical standards only represents a snapshot of the assessed workplace at a particular time and place, and often does not paint a genuine picture of daily working conditions. As such, they have severe limitations (e.g., insufficient worker interviews, language barriers, lack of sufficiently deep reviews, practice of subcontracting, etc.), and companies should not place a heavy or sole reliance on these to detect and remedy forced labour. Instead, a broader approach should actively engage suppliers through training, capacity building, worker involvement, strengthened management, and enhanced transparency.

'We are seeing a rise in forced labour risks across our clients' global supply chains. The reputational risk associated with these issues is significant and requires proactive management and due diligence.'

Matthew Bruce, Freshfields Bruckhaus Deringer

Insights from leading practitioners

Our Leading Practice Interviewees had further recommendations, including:

Add KPIs for third parties' sustainability.
Companies should consider adding an additional category of third-party risk scoring—the sustainability score. One of our interviewees explained that the company had developed more than 20 specific key performance indicators relating to sustainability for its third parties.

Regularly audit highest-risk third parties.
Onsite audits should be performed on approximately 75% of the highest-risk tranche of third parties at least once every two years.

Keep progressing on supply chain mapping.
Boards should insist on supply chain mapping as an integral part of the company's third-party risk management programme and that management should provide regular updates on the timeline to complete the mapping of the next tier of suppliers until the company has successfully mapped its supply chain.

Weigh local market revenue or production facilities against operational risks.
It may be prudent for companies to evaluate large foreign markets to determine whether the revenue opportunity and operational risks there warrant a supply chain strategy that can be entirely self-sufficient in that country (for example, an 'in China for China' strategy). In other situations, a production facility in a lower revenue market may not be worth the associated operational risk.

Eight complexities that challenge supply chain mapping

Effectively mapping a company's supply chain involves a complex set of challenges that span technical, organisational and data-related areas. Here are some of the technical complexities involved:

Data integration and harmonisation: Combining data from various sources often means dealing with different formats, standards and levels of detail. Ensuring that this diverse data can be integrated into a coherent whole requires robust data harmonisation processes. These data sources include internal sources such as detailed product-level bill of materials and external sources such as aggregated bill of lading databases.

Data quality and accuracy: Quality data collection can be challenging, but it is essential to create a reliable supply chain map. A thoughtful supplier engagement strategy should help to assure that the data collected is accurate, complete and timely. Common challenges include master data management issues with suppliers and fully identifying key business and strategic supply chain relationships.

Scalable and repeatable: A supply chain can be vast and complex, so the technical solution must be scalable enough to handle a large amount of data from numerous sources without performance degradation and the ability to detect significant changes to your supply chain and update accordingly.

Data security and privacy: Supply chains often involve sensitive information with a global footprint. It is vital to understand regional data privacy regulations (e.g., the EU's General Data Protection Regulation) and maintain elevated levels of security to protect data from cyber threats and ensure compliance with various privacy laws and regulations.

Data analytics and visualisation: Analysing the integrated data to extract meaningful insights is a complex task that often requires leveraging advanced analytics and visualisation techniques and can benefit from deploying machine learning or other AI-powered tools.

Legal and compliance issues: Different regions may have different laws concerning data storage and transfer, which can complicate the technical infrastructure required for a robust global supply chain map.

Complex event processing: Recognising patterns and correlations across different data sets and understanding the implications of these patterns for the supply chain require complex event processing capabilities.

Collaboration tools: Effective supply chain mapping requires collaboration between departments within the company and with external partners. The technical solution must support secure and efficient collaboration.

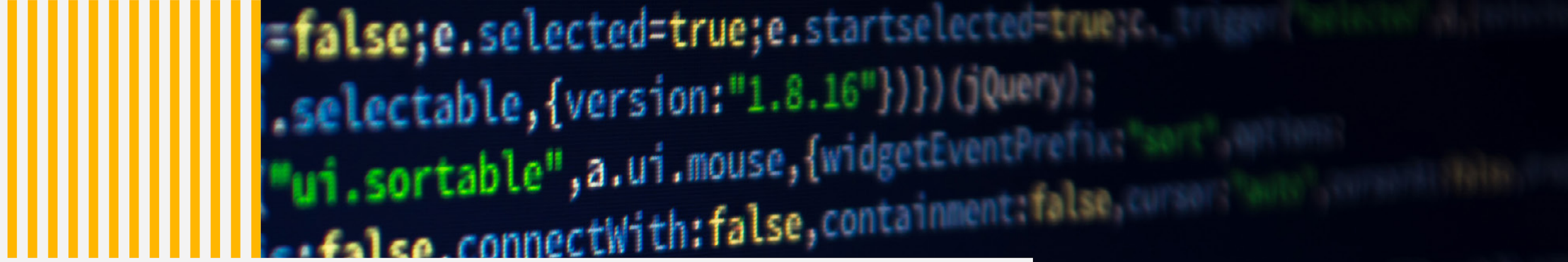
Addressing these challenges typically requires a multidisciplinary approach that brings together expertise in data science, IT, supply chain management and cybersecurity, among other fields.

Do you know the indicators that forced labour is present?

The International Labour Organisation (ILO) has compiled a list of 11 indicators that represent the most common signs or 'clues' to the possible existence of forced labour. As Tom Plotkin of Covington emphasised, 'These indicators aren't necessarily confirmation of forced labour, but they reflect a possible structure or vulnerability where forced labour can arise. These indicators have become critical red flags not only for companies, but for regulators who use them to orient enforcement activity.'

- Abuse of vulnerability
- Deception
- Restriction of movement
- Isolation
- Physical and sexual violence
- Intimidation and threats
- Retention of identity documents
- Withholding of wages
- Debt bondage
- Abusive working and living conditions
- Excessive overtime

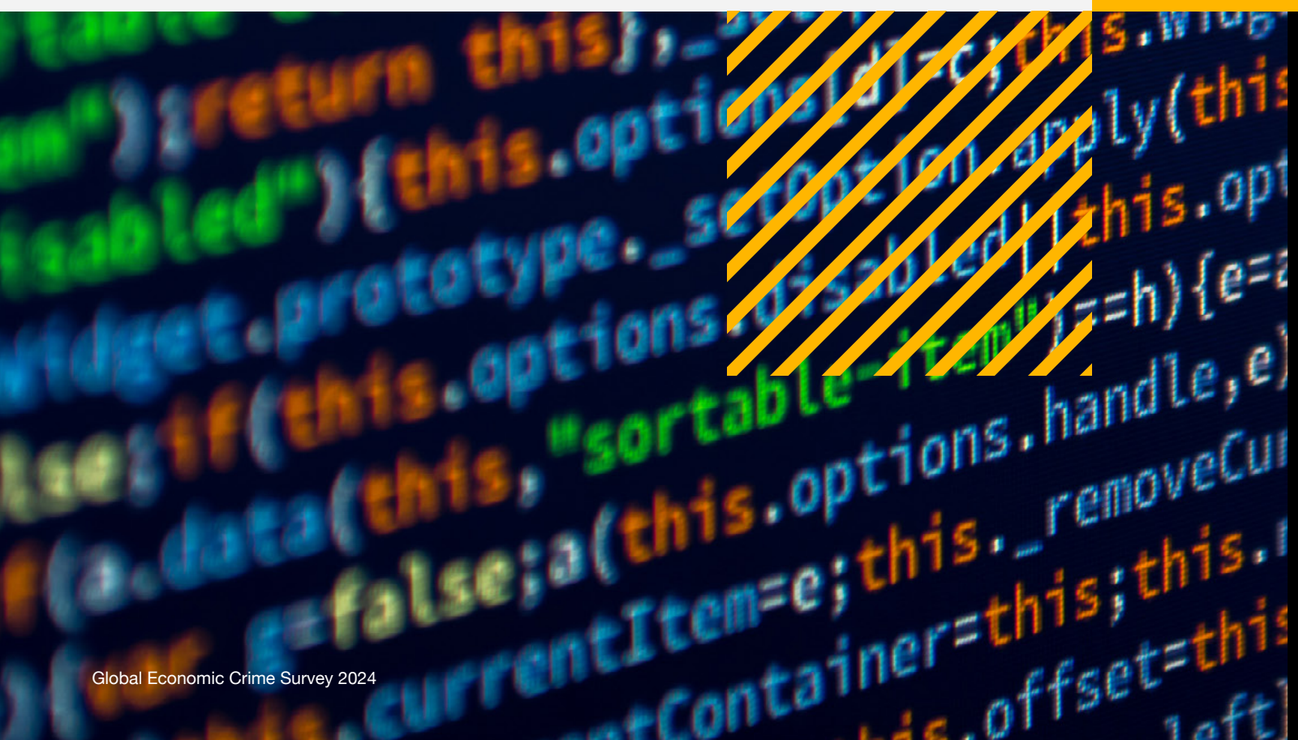
Source, including further descriptions: ILO Indicators of Forced Labour



Export Controls and Sanctions

Cross-border conflicts adding to the complexity of corporate compliance efforts

Geopolitics, including the Russia–Ukraine conflict, tensions between China and the US, and uncertainty in the Middle East, give rise to the export controls and sanctions regulatory environment in which businesses around the world must operate.



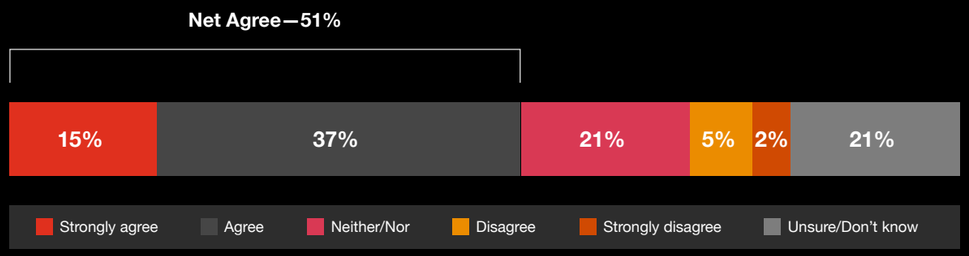
While the US government, including its Departments of Justice, Treasury and Commerce, is driving many of these developments, other countries' alignment with these policies is increasing. Multinational companies, whether they support the underlying policy priorities, have little choice but to heed these legislative and regulatory changes. As Steven Fagell at the Covington & Burling law firm emphasised, 'The Deputy Attorney General and other senior leaders at the US DoJ have noted that corporate boards of directors should be viewing trade controls compliance as an absolute top priority and a key driver of legal risk. Companies are responding by investing in compliance, taking investigations more seriously, and briefing trade controls risks at the board and C-suite levels.'

The pronouncements of the US Commerce Department's Bureau of Industry and Security (BIS) and its Assistant Secretary for Export Enforcement Matthew Axelrod are must-reads for corporate compliance executives worldwide. The close coordination of BIS with Justice and Treasury is exemplified by a series of Tri-Seal Compliance Notes, jointly published by the three departments, which provide important guidance on export controls and sanctions matters.[xvi] Intensifying enforcement efforts are likely. 'In particular, the Commerce and Justice Departments are pursuing expansive, creative legal theories, and hiring dozens of new lawyers and agents dedicated to these cases,' explained Eric Sandberg-Zakian of Covington & Burling. 'Enforcement agencies are seeking larger penalties and imposing more burdensome compliance commitments in settlements.'

For further evidence of the efforts of the US to spearhead globally coordinated efforts, corporate management and boards would be wise to follow the pronouncements of the 'Export Enforcement Five,' the grouping of the US, Canada, UK, Australia and New Zealand, akin to the 'Five Eyes' intelligence-sharing arrangement. Other bilateral and multilateral efforts include BIS's effort to engage Japan and South Korea in a Disruptive Technology Protection Network,[xvii] aligned to the BIS/DoJ Disruptive Technology Strike Force. Similarly, other countries are strengthening their enforcement capabilities, including the UK's establishment of its Office of Trade Sanctions Implementation with the responsibility to investigate activity by companies that may be seeking to avoid sanctions by sending products through third countries.

Our research suggests that the business community is indeed paying attention to these developments. Among executives surveyed, 59% agree that export controls have grown more complex in the last two years. This percentage rises to 69% for companies with greater than US$5 billion in annual revenue and those in North America. A greater share of companies in the TMT and EUR sectors (66% in each) believe export controls complexity has increased recently.

Enforcement of export controls laws has become more robust



34%	55%	46%	51%	61%	52%	52%
Government and Public Services	Industrial Manufacturing	Financial Services	Consumer Markets	Energy, Utilities and Resources	Health	Technology, Media and Tel-ecommunications

Q27. To what extent do you agree or disagree with the following statements? In the last two years export controls imposed by governments in numerous countries are enforced more robustly. Base: All respondents = 2446

Please note that the percentages do not add up to 100% due to rounding.

Executives also agree that enforcement efforts are on the rise. More than half (51%) believe that export controls are being enforced more robustly than two years ago, with 62% of those in corporations earning US$5 billion or greater in revenue agreeing. While the common perception is that export controls apply primarily to the technology, chemicals, and aerospace and defence sectors, there is a wide array of products across sectors from consumer goods to industrial manufacturing to pharmaceuticals that are controlled so as not to end up in sanctioned countries. And, like the spread of industries for which export controls have relevance, the belief that enforcement is intensifying is widespread. More than half of executives in IM, EUR, CM, Health and TMT agree.

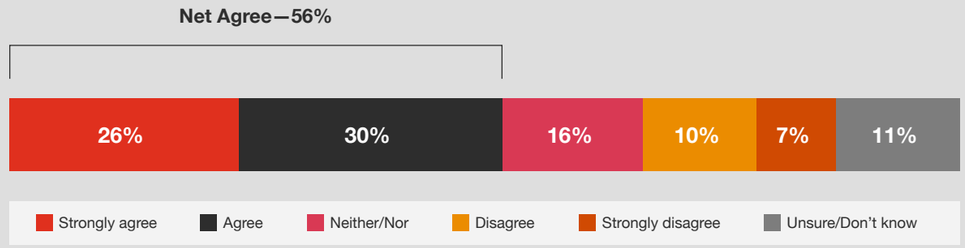
BIS's Matthew Axelrod summed up the intensifying export controls environment for businesses well when sharing his agency's objectives in a recent speech. He said, 'Our goal is to encourage and incentivise investment in compliance on the front end, while also emphasising the financial and reputational cost of facing an enforcement action….And we're equally committed to implementing more aggressive and effective ways to hold companies that don't comply accountable.'

A deeper look

Managing export controls risk isn't just an issue for a few industry sectors. More than half of our respondents (56%) agree it's a priority for their industry, with a greater share of executives concurring in EUR, Health and IM than other sectors. Over half (56%) say managing export controls risk is important to their company specifically, with a greater share in North America (65%) reporting it as a top concern.

China-related restrictions are likely driving Asia-Pacific companies' focus on managing export controls risk (60% say it's a priority), and Central Europe's sensitivity (55% say it's important) may be heightened by the Russia–Ukraine conflict. Large companies (those with more than US$5 billion in revenue) clearly feel the pressure, with 72% saying managing export controls risk is a priority.

Not surprisingly, managing the risk is getting attention



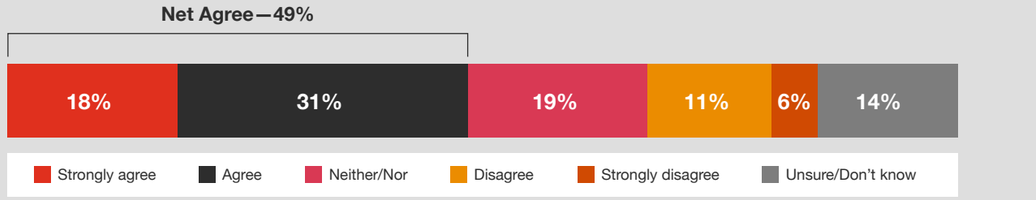
45%	53%	55%	60%	57%	65%
Latin America	Africa	Central and Eastern Europe	Asia-Pacific	Western Europe	North America

Q27. To what extent do you agree or disagree with the following statements? Managing risks associated with export controls is an important priority for our organisation. Base: All respondents = 2446

These large companies also appear to be taking action. Nearly three-quarters say they have a robust export controls risk assessment process that includes participation from Legal, Trade Compliance, and the business in both headquarters and higher-risk jurisdictions. This compares to just half of businesses overall. Nearly two-thirds of companies in North America (62%) report having a strong export controls risk assessment process.

Given the heightened awareness to export controls risks including the risk that a competitor may report your conduct to the US government, especially in light of the voluntary self-disclosure policy changes in April 2023,[xviii] it's not surprising that BIS has seen a nearly 80% year-on-year increase in self-disclosures and one-third more tips from industry about the conduct of others over the same period.

Establish a robust export controls risk assessment process—get everyone around the table

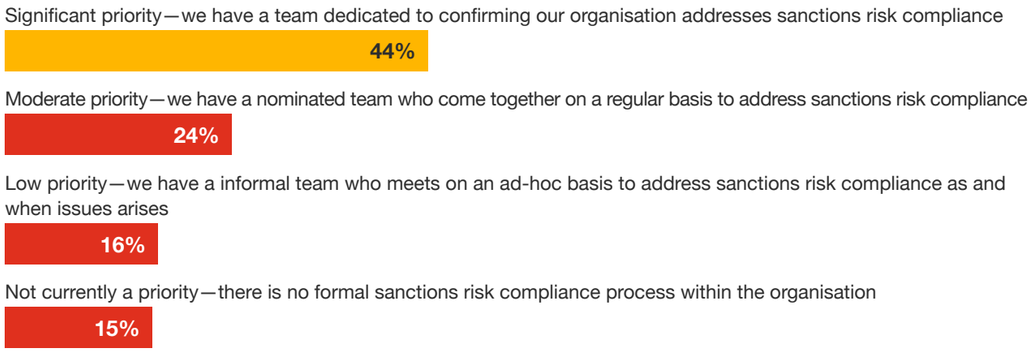


41%	42%	48%	50%	53%	62%
Latin America	Africa	Central and Eastern Europe	Asia-Pacific	Western Europe	North America

Q27. To what extent do you agree or disagree with the following statements? Our organisation has a robust export controls risk assessment process, including participation from the legal function, trade compliance and the business—both at headquarters and from higher-risk jurisdictions. Base: All respondents = 2446

Much like their keen awareness of export controls risk, nearly half of companies (44%) consider sanctions risk compliance a significant priority. Another 24% place moderate priority on the issue. Interestingly, while companies in IM indicated high export controls risk awareness, they rated their sanctions risk compliance priority as lower than the global average.

Sanctions risk compliance receiving serious attention at many organisations

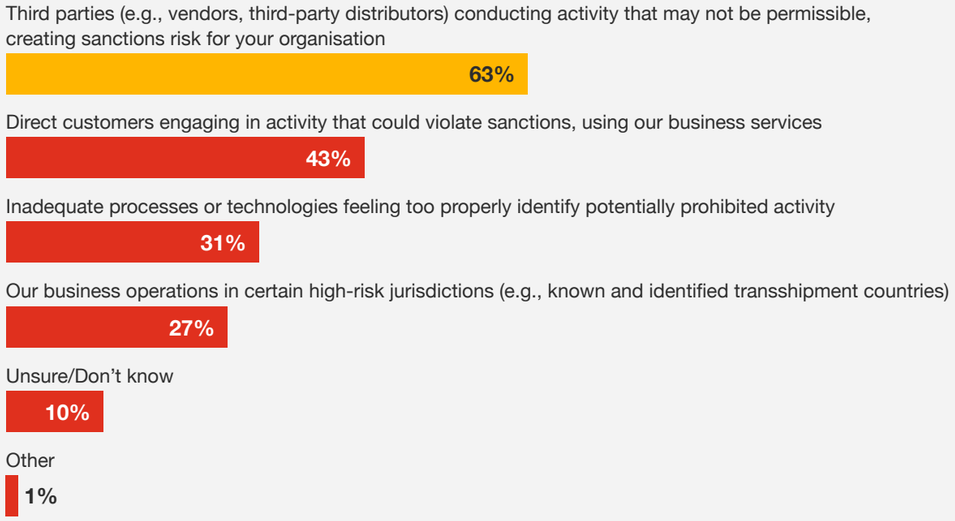


Q28. To what extent is sanctions risk compliance a priority within your organisation? Base: All respondents = 2446

Please note that the percentages do not add up to 100% due to rounding.

Third parties are the primary focus of sanctions compliance risk. In fact, 63% of executives place the possibility of third parties engaging in impermissible activity as a top two sanctions risk, which is a 20-point difference from other risks queried. This finding underlines the urgency of third-party risk management as identified in other sections of this report. Those in North America (74%), Latin America (69%) and Western Europe (67%) feel most strongly about the influence of third parties on sanctions risk. EUR (74%) and Health (71%) sectors appear acutely aware of third-party sanctions risk, while far fewer in IM rank this critical exposure area as a significant risk.

Third parties in focus once again—sources of concern regarding sanctions compliance

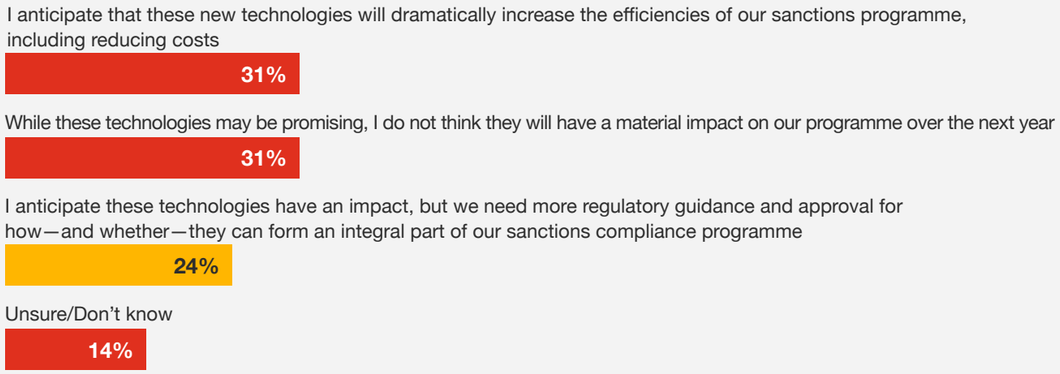


Q29. Which of the following do you think poses the greatest sanctions compliance risk for your organisation? (Ranked in top two)
Base: All respondents = 2446

Despite recognising the risks related to sanctions, many companies have substantial room for improvement in testing the strength of their compliance programme. Just 30% undertake a range of testing steps, such as reviewing policies and procedures, testing to confirm that staff are dispositioning sanctions alerts and cases correctly, and testing sanctions system performance and data lineage. Even in companies with more than US$5 billion in revenue, just 45% test in a comprehensive manner. When viewed by industry, only about one-fourth of those in IM (22%), CM (25%) and TMT (29%) have robust testing. A full 19% of companies do not regularly test their firm's sanctions compliance programme at all.

When it comes to the possibility that new technologies, such as AI, could help considerably with sanctions compliance efficiency and effectiveness, the jury is still out. Nearly a third (31%) of executives agree that these technologies may be promising at some point, but don't believe they will have a material impact in the near term. A quarter (25%) believe more regulatory guidance is needed for how new technologies can become an integral part of sanctions compliance. EUR, CM and FS, in particular, are looking for regulatory guidance relative to other sectors.

Decidedly mixed opinions regarding the impact of new technology solutions



Q32. Thinking about new technologies and systems (e.g., artificial intelligence—including machine learning—or generative AI), what impact do you think they will have on your sanctions compliance programme in the next 12 months?
Base: Those who have indicated there is a sanctions risk compliance process = 2068

The takeaway

Securing board engagement on export controls and sanctions

The priorities for boards and management are clear. First, greater efforts to anticipate geopolitical trends must be matched by enabling businesses to react faster to developments on the ground. These measures will in turn inform higher quality and more useful risk assessments. Second, boards should encourage management to take a 'whole of company' approach to managing the identified risks. And lastly, the technology systems that support both export controls and sanctions efforts must be regularly assessed to be confident that they remain 'fit for purpose.'

'Our clients are horizon scanning for geopolitical risks and potential trade restrictions, especially in relation to China and the Middle East. They are aware of the volatility and uncertainty in the global environment and the potential impact on their operations.'
Ali Sallaway,
Freshfields Bruckhaus Deringer

By tracking and anticipating trends in the constantly shifting landscape of US policies and requirements, as well as those of other countries relevant to a company's operations, companies can more readily integrate these learnings into the design, maintenance, and enhancement of their compliance programmes. Socialising emerging developments with relevant employee stakeholder groups is a critical component to maintaining a strong export compliance programme.

Periodic risk assessment expected

While the relevant US authorities do not mandate precisely how often risk assessments should be conducted, companies should periodically assess the changes to a company's business operations, including mergers and acquisitions, locations, products and services, and third-party interactions. To supplement these internal risk assessments, the Trade Compliance function should conduct export compliance audits. Focus should be placed on key compliance areas, including review of the company's export compliance programme that implements safeguards throughout the export lifecycle, as well as the adequacy of management commitment, support, communications, resourcing, and funding provided to export compliance–related functions.

The Trade Compliance function should also conduct ongoing compliance training to bolster awareness across the company. This may involve specialised training for those business units most affected by export controls (e.g., Engineering, Product Development, Procurement, Legal, Logistics, Human Resources), as well as company-wide training that covers the fundamentals of export controls. Companies must be able to mobilise, reallocate and train resources to match requirements driven by the regulatory landscape.

Export controls compliance spans the product lifecycle and the organisation

Turning from risk assessment to risk mitigation, it is important to note that a company's effort to manage export controls risk often begins with the Research and Development (R&D) function. Companies' Trade Compliance teams should work closely with R&D, especially due to potential risk regarding access to controlled technology. It is important for Trade Compliance to remind the company that blueprints, schematics, photographs, instruction manuals and information regarding sensitive products can fall under the scope of export control laws.

For example, under US law, should an unauthorised individual obtain access to such documents, even if the documents were accessed in the product's country of origin, the product can be 'deemed' to be exported to the foreign national's latest country of residency or countries of citizenship, by virtue of the fact that the unauthorised individual accessed such information.

US authorities place a high importance on access to sensitive items, both in the pre- and post-development stages. Trade Compliance can partner with IT, Information Security, Human Resources and other functions to implement internal controls to monitor who has access to, and the ability to work on, such sensitive products.

Export control implications follow a product throughout its entire lifecycle. Though some companies still prefer to follow the path of transaction-based classifications, meaning that Trade Compliance must classify a product the day it is being shipped, others implement more holistic approaches to classification, meaning that the Trade Compliance team has visibility into both current products and those emerging out of development in the foreseeable future. The product engineering teams are often best placed to address these issues given their centrality to the production lifecycle.

Procurement plays a critical role in export controls compliance. This is because some third-party products, including both hardware and software, may require additional safeguards and export licence requirements before shipment to a company's sites and offices, and integration into a company's already-existing products.

The role of technology in export controls

Finally, it is critical that the technology tools and platforms that enable broader risk management efforts—including those that support restricted party screening and export control classification processes, as well as end-to-end transaction life cycle management—are contributing to operational efficiencies and are helping to deliver sustained compliance.

Not surprisingly, ERP solutions incorporate several of these capabilities. Available modules within ERP solutions support companies with automation and integration of various global supply chain and related processes, including classification and export licence determinations and decrementation, embargo and restricted party screening for shipments, and determining *de minimis* eligibility.

Trade Compliance executives would be wise to consider technology capabilities to securely store export-controlled information (e.g., 'offline' or 'on premises' database(s) vs. 'cloud' storage) and should be actively involved in discussions that span the technology lifecycle, including throughout the pre-implementation, implementation, and post-implementation tuning stages. As with other parts of an export controls compliance programme, technology platforms and automated solutions should periodically be evaluated to confirm they are 'fit-for-purpose' in accordance with the company's current risk profile, complexity of business operations, and types of products and services.

The board's role in furthering the compliance agenda

Like export controls risk management, effective sanctions compliance requires active involvement of the company's board and senior executive management. Senior management—including the board as necessary and appropriate—should receive regular briefings to ensure they have visibility into, and are ultimately accountable for, sanctions-related risks.

Briefings should include key risk indicators (KRIs, e.g., open issues, significant increases in sanctions alerts or levels of exposure) as well as KPIs (e.g., meeting service level agreement–defined timelines for reviewing and clearing sanctions alerts).

Companies that use third parties such as re-sellers or redistributors to sell products and services should have in place mechanisms by which they assess and understand the sanctions compliance programmes of those third parties. US regulatory authorities, in particular, have pursued enforcement actions in recent years where US persons sent products to redistributors who subsequently sold those products to sanctioned jurisdictions or persons. Companies should test resellers' and redistributors' compliance programmes on a regular or sample basis, including reviewing the design of those programmes and analysing specific transactions. This mitigates sanctions regulatory risk both by limiting the likelihood that the company is working with an entity that is providing goods or services to sanctioned persons or jurisdictions and by limiting legal exposure if the reseller or redistributor is in fact engaging in such activity.

Insights from leading practitioners

Our Leading Practice Interviewees had further recommendations, including:

Stay alert to conflicts of interest.
Companies should be alert to the fact that trade compliance violations can start with conflicts of interest, including receiving personal benefits from parties and/or individuals in sanctioned countries.

Conduct crisis simulations.
Boards should encourage management to conduct crisis simulations focusing on geopolitical scenarios and, where applicable, potential for countersanctions from other countries. It is important to apply the lessons learned to the company's export controls and sanctions compliance programme and its broader business continuity plans.

Use sales data to identify diversion.
Companies need to intensify their efforts to leverage sales data to identify possible instances of diversion to sanctioned countries by third parties in neighbouring countries. Identifying specific products that are likely to be of higher value to the sanctioned countries may help focus the company's data analytics efforts.

Recognise geo-blocking limitations.
Companies should be aware of the limitations to geo-blocking, particularly with respect to sanctioned territories that exist within non-sanctioned countries (e.g., Crimea) and to efforts by individuals to use virtual private networks to defeat geo-blocking IT systems.

Monitor social media.
Companies that produce physical, branded products should monitor social media for images of its products being used in sanctioned countries.

Governments aren't likely sources of company-specific guidance.
Companies should not necessarily expect governmental authorities to provide guidance to individual companies on best practice outside the context of a regulatory enquiry or investigation. External legal counsel and other consultants, who often appear before these authorities, should be familiar with the expectations of law enforcement and regulators and should be able to be of assistance.

Sanctions compliance hinges on timely and accurate data

Testing of sanctions screening systems should include data lineage, data quality, list ingestion and overall system performance. If a company is not properly screening the data it has on customers and counterparties—either because the data is not feeding properly into the screening system or the screening system is not using updated sanctions lists—the likelihood of doing business with a sanctioned person or in a sanctioned jurisdiction increases significantly.

To the extent possible, companies should ensure they collect all relevant information from customers and counterparties, that data collected is accurate and complete, and that the data makes its way in a complete and traceable manner to the sanctions screening system. In addition, companies should ensure that the sanctions screening system is properly updating, in a timely manner, the relevant sanctions lists each time regulatory sanctions updates occur.

Where to from here

Supply chains. Markets. Competitors. Regulators. Law Enforcement. Technological change. Complexity does not have to be your adversary.

Take risks intelligently. Develop even greater confidence in compliance.

Here are questions to ask yourself and your team—before your board or regulators ask you:

1 Is your board adequately engaged on your issues?

Sustaining strong board interest, especially after a high-profile investigation or regulatory matter has concluded, can be a challenge. Emerging issues like the need to comprehensively map your supply chain to better deal with the risk of forced labour can struggle to get time on a crowded meeting agenda. Issue-specific briefings for select directors can help. Refreshed data visualisations of key risk management data are worth exploring.

2 Does your risk appetite match that of your CEO?

With earlier and more proactive strategic engagement with your CEO, the risk function can help close the disconnect with senior leadership that can sometimes exist. See PwC's recent Global Risk Survey and Global Internal Audit Study for more information.

3 Are your risk assessments overdue for an assessment of their own?

It's time for a fresh look at geopolitical risk assumptions, new regulatory obligations and cross-border enforcement trends.

4 Will better visibility, inside and outside your company, to past incidents of employee misconduct, and your efforts to hold people accountable and mitigate the risk of future problems, help deter aberrational behaviour today?

More frequent, short surveys of employees on matters relating to ethics and compliance can provide useful data points for the second and third lines of defence. Benchmarking your communications strategy against the leaders, including firms outside your industry, is a worthwhile exercise.

5 Are the investigation capabilities at your disposal going to establish the facts as quickly as you need them?

Upskilling the data analytics and AI capabilities of your team, including the tools they utilise, is a sound investment. Critical decisions—whether about the veracity of a whistleblower or the benefits of self-reporting—are informed by the quality of the data analysis.

6 Are you measuring fraud losses adequately and getting to root causes?

Perhaps a wider perspective is required to be more confident that similar risks aren't lurking in other parts of the business.

7 Is your third-party risk management approach up to the challenge?

You may have access to the data you need today, but the data *you want* is a different story. Stronger teaming between Compliance, Internal Audit and Procurement could secure the data lake and analytics capabilities you need to unlock compliance insights.

Endnotes

i www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-keynote-remarks-american-bar-associations
ii www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#:~:text=The%20Foreign%20Extortion%20Prevention%20Act%20(FEPA)%2C%20which%20criminalizes%20the,from%20certain%20individuals%20and%20entities
iii www.justice.gov/opa/blog/criminal-divisions-voluntary-self-disclosures-pilot-program-individuals
iv Securities and Exchange Commission Office of the Whistleblower Annual Report to Congress for Fiscal Year 2023, www.sec.gov/files/fy23 annual-report.pdf
v www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-announces-new-safe-harbor-policy-voluntary-self
vi www.legislation.gov.uk/ukpga/2023/56/enacted
vii www.tribunal-de-paris.justice.fr/sites/default/files/2023-03/Guidelines%20on%20the%20implementation%20of%20the%20CJIP PNF January%2016%202023%20VD.pdf
viii www.gesetze-im-internet.de/hinschg/BJNR08C0B0023.html
ix www.bafa.de/DE/Lieferketten/Multilinguales_Angebot/multilinguales_angebot_node.html
x www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7055
xi Non-Prosecution Agreement Letter from the U.S. Department of Justice, Criminal Division to Courtney Trombly & William Barry, Re: Albemarle (Sept. 28, 2023), www.justice.gov/opa/file/1316796/dl?inline.
Deferred Prosecution Agreement, United States v. Corporacion Financiera Colombiana S.A., No. 8:23-cr-00262-PJM (D. Md. Aug. 10, 2023), www.justice.gov/media/1311296/dl?inline.
Plea Agreement Attachment A-2, United States v. Telefonaktiebolaget LM Ericsson, No. 1:19-cr-0084-LTS (S.D.N.Y. Mar. 20, 2023), www.justice.gov/media/1283591/dl?inline.
Order, In re Koninklijke Philips N.V., Securities Exchange Act Release No. 97479 (May 11, 2023), www.sec.gov/litigation/admin/2023/34-97479.pdf.
Order, In re 3M Co., Securities Exchange Act Release No. 98222 (Aug. 25, 2023), www.sec.gov//litigation/admin/2023/34-98222.pdf ['Aug. 2023 3M Order'].
xii www.europarl.europa.eu/doceo/document/TA-9-2024-0329_EN.html
xiii eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464
xiv www.govinfo.gov/app/details/PLAW-117publ78
xv www.cbp.gov/newsroom/stats/trade/uyghur-forced-labor-prevention-act-statistics
xvi There are numerous other multi-agency announcements on export controls and sanctions-related topics. For some of these announcements, see the following links: www.justice.gov/nsd/compliance-notes
www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Notice_US_Export_Controls_FINAL508.pdf
xvii www.bis.gov/press-release/departments-justice-and-commerce-launch-disruptive-technology-protection-network
xviii www.bis.gov/speeches/remarks-prepared-delivery-assistant-secretary-export-enforcement-matthew-s-axelrod-biss

PwC Forensics Global Network Contacts

Ryan Murphy
Global & US Forensics Leader,
Partner, PwC US
ryan.d.murphy@pwc.com

Justin Offen
Global Forensic Technology Leader,
Principal, PwC US
justin.m.offen@pwc.com

Marcos Panassol
Brazil Forensics Services Leader,
Partner, PwC Brazil
marcos.panassol@pwc.com

Claire Reid
UK Forensics Services Leader,
Partner, PwC UK
claire.reid@pwc.com

Anita Kim-Reinartz
Germany Forensics Services Leader,
Partner, PwC Germany
anita.kim-reinartz@pwc.com

Sirshar Qureshi
EMEA Forensics Services Leader,
Partner, PwC Czech Republic
sirshar.qureshi@pwc.com

Puneet Garkhel
India Forensics Services Leader,
Partner, PwC India
puneet.garkhel@pwc.com

Mihoko Nasu
Japan Forensics Services Leader,
Partner, PwC Japan
mihoko.nasu@pwc.com

Alex Tan
South East Asia Forensics Services,
Partner, PwC Malaysia
alex.tan@pwc.com

Jane He
Australia Forensics Services Leader,
Partner, PwC Australia
jane.a.he@au.pwc.com

Chris Costa
GECS Research Lead,
Managing Director, PwC US
chris.costa@pwc.com

www.pwc.com/gecs