REPRINT

risk & compliance

INVESTIGATIONS & WHITE-COLLAR CRIME

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-SEP 2026 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

AZIZ & KAYE
BUSINESS LAW

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com
© 2026 Financier Worldwide Ltd. All rights reserved.

WORLDWATCH

INVESTIGATIONS & WHITE-COLLAR CRIME

PANEL EXPERTS

MEXICO

Carlos García Cueva
Lawyer
Aziz & Kaye Business Law
T: +52 (55) 5985 6689
E: cgc@azizkaye.com

Carlos García Cueva is a competition, risk and compliance attorney at Aziz & Kaye Business Law in Mexico City, with over 15 years of experience spanning government enforcement and private practice. He holds master's degrees from the London School of Economics and King's College London, serves as external adviser to Mexico's National Antitrust Commission and is a professor at Tec de Monterrey.

UNITED STATES

Holly P. Carr
Managing Director, Forensics
BDO
T: +1 (703) 217 1312
E: hcarr@bdo.com

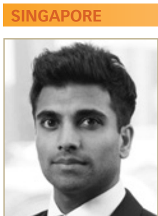
Holly Carr is a managing director in BDO's forensic and investigations practice and co-chair of the firm's global whistleblower task force. Previously an assistant director in the US Securities and Exchange Commission's (SEC's) Division of Enforcement, she advises boards, senior executives and counsel on complex fraud, whistleblower and regulatory matters. Her perspective is informed by a unique combination of experience auditing public companies, preparing financial statements and serving in leadership at the SEC.

SOUTH AFRICA

Tim Smit
Director, Dispute Resolution
Cliffe Dekker Hofmeyr Inc
T: +27 011 562 1085
E: tim.smit@cdhlegal.com

Tim Smit is a director in Cliffe Dekker Hofmeyr Inc's dispute resolution department. He is head of the firm's consumer goods, services and retail sector, and is ranked in Band 3 by Chambers & Global for his corporate investigations expertise.

SINGAPORE



Khushaal Ved
Partner
Hogan Lovells
T: +65 6302 7137
E: khushaal.ved@hoganlovells.com

Khushaal Ved is a partner at Hogan Lovells, guiding clients through sensitive internal and government investigations across Asia-Pacific, from report to resolution. Clients identify Mr Ved as their 'go to resource in the region', and he is globally recognised as a leading cross-border investigations and compliance lawyer, earning accolades from Asian Legal Business, Chambers, Global Investigations Review, Legal 500, The Financial Times and Who's Who Legal for his "excellent reputation" and "authority beyond his years".

UNITED KINGDOM

Simon Airey
Partner
McDermott Will & Schulte
T: +44 (0)207 577 3470
E: sairey@mcdermottlaw.com

Simon Airey focuses his practice on global, cross-border and internal investigations, financial and regulatory crime, bribery and corruption, money laundering, tax and fraud inquiries, data breaches, dawn raids, asset tracing, international enforcement and corporate compliance issues. He acts in associated civil, criminal and regulatory litigation and represents both companies and individuals. He serves as global co-head of McDermott Will & Schulte's investigations & compliance practice.

SWITZERLAND

Marcel Frey
Partner
Prager Dreifuss
T: +41 44 254 55 55
E: marcel.frey@prager-dreifuss.com

Marcel Frey is a member of the dispute resolution and private clients teams. He represents Swiss and foreign clients in court and arbitration proceedings. He also advises private individuals with enforcing civil claims in complex cases of white-collar crime. He regularly advises clients in international judicial assistance proceedings and the recovery of illegally acquired assets. In addition, he specialises in the enforcement of Swiss and international decisions in Switzerland.

JAPAN

Mihoko Nasu
Chief Executive Officer
PwC Risk Advisory LLC
T: +81 80 3313 0746
E: mihoko.nasu@pwc.com

Mihoko Nasu is chief executive officer of PwC Risk Advisory LLC and a partner with PwC Japan Group's forensic services practice, where she helps clients navigate complex investigations related to white-collar crime and regulatory issues. She has been appointed on numerous special investigation committees, particularly investigations of accounting fraud. Furthermore, she has been consistently involved in crisis response consulting, assisting in dealing with regulators and stakeholders, and implementation of remediation measures.

R&C: How are the wider geopolitical, technological and economic currents of recent months collectively reshaping the nature, scale and sophistication of white-collar crime?

MEXICO

García Cueva: Mexico is amid the convergence of extraterritorial enforcement, with an expanding and more aggressive domestic regulatory context. In 2025, the US redesignated major Mexican cartels as foreign terrorist organisations. There is a transversal application of US anticorruption, anti-money laundering (AML) and counter-terrorism financing laws to activities in Mexico. Even conduct that may never be prosecuted domestically can carry exposure and significant liability. In addition, antitrust conduct such as bid rigging frequently involves third-party intermediaries connected to these same networks. Therefore, it is important to assess not only specific risks, but also whether supply chains, joint ventures or key third parties have any exposure. On the technology side, artificial intelligence (AI)-produced content is making certain white-collar schemes such as fraud far more sophisticated. However, cryptocurrency, contrary to popular belief, could rely on blockchain traceability that facilitates enforcement. It is key to enhance prevention frameworks to evolve at the same pace as enforcement.

UNITED STATES

Carr: White-collar crime still comes down to a simple constant: bad actors want what you have. What has changed is the speed, scale and sophistication of how they try to get it, and, increasingly, why. Generative AI (genAI) and agentic AI, deepfakes, voice cloning and false digital personas are making fraud cheaper to launch, easier to scale and harder to detect, often bypassing controls organisations only recently strengthened. At the same time, sustained economic pressure is expanding both motive and opportunity across industries and geographies. The 'why' is no longer

> **"Traditional forms of corporate misconduct remain a persistent concern, typically linked to the well-known fraud triangle of motive, opportunity and rationalisation."**
>
> *Mihoko Nasu,*
> *PwC Risk Advisory LLC*

always straightforward greed; it may also reflect coercion, dislocation, state-aligned interests or basic financial survival. Layer in geopolitical tension, and some conduct that looks like ordinary fraud may also serve broader strategic objectives. The result is a more adaptive, more ambiguous and more dangerous white-collar threat environment.

SINGAPORE

Ved: Recent geopolitical turbulence has materially reshaped the white-collar risk map across Asia. With trade fragmentation, aggressive export controls and tariff volatility, we are seeing an uptick in two distinct categories of misconduct. The first is 'origin washing', that is, misrepresenting where goods come from. Enforcement authorities are uncovering schemes in which Chinese-manufactured goods are routed through Southeast Asian intermediaries like Thailand, Malaysia or Vietnam, with falsified documentation to evade US duties. The second is end-destination concealment, which means misrepresenting where goods are going. This has become acute in the semiconductor space, where possibly restricted technologies are being funnelled through Southeast Asian intermediaries with fabricated end-user declarations. At the same time, genAI is materially lowering barriers to fraud. AI-assisted documentation manipulation no longer requires sophisticated infrastructure. Cryptocurrency layering compounds traceability challenges. White-collar crime is increasingly technologically-enabled and borderless, requiring a fundamentally different response from both companies and regulators.

> **"In Switzerland, voluntary self-disclosure is prevalent in the area of taxes: companies or individuals can file a voluntary disclosure if they reveal tax-relevant facts that were previously undeclared."**
>
> *Marcel Frey, Prager Dreifuss*

JAPAN

Nasu: Amid heightened geopolitical tensions, Japan has seen cases involving exports to sanctioned jurisdictions via third countries and related customs violations. However, tighter monitoring and enforcement by Japanese and foreign authorities, together with Japanese companies' generally cautious approach to export controls and customs compliance, mean that these risks have not materially increased the scale or frequency of white-collar crime. At the same time, rising costs driven in part by the recent depreciation of the yen have raised concerns over practices whereby companies with stronger bargaining power unilaterally maintain transaction prices or refuse to engage in price negotiations. Such conduct has been newly prohibited under Japan's Fair Transactions Act, with regulatory scrutiny increasing. Traditional forms of corporate misconduct, including accounting irregularities, data falsification and employee embezzlement, also remain a persistent concern, typically linked to the well-known fraud triangle of motive, opportunity and rationalisation.

UNITED KINGDOM

Airey: Extraordinary geopolitical pressures are undoubtedly giving rise to more sophisticated incidences of organised crime such as sanctions busting and money laundering, but tariffs, inflated oil prices, tax hikes and the increased cost of borrowing have put huge strain on ordinary businesses all around the world. As a result, managers are under pressure to meet budget, bolster the balance sheet, win market share, secure investment, earn bonuses and cover up mistakes. Experience shows that times like this give rise to higher levels of economic crime and more ingenious ways of concealment. But insolvencies, litigation, investigations, whistleblowers, class action lawyers, non-governmental organisations and investigative journalists follow quickly behind, and a new wave of trigger events and enforcement is expected. Auditors, banks and investment committees are also laser-focused on fraud risk at present, and this will also give rise to a significant increase in investigations and prosecutions.

SWITZERLAND

Frey: White-collar crime in Switzerland is becoming more digital, more data-driven and more transnational, due to actors' access to rapid technological advancements and an influx of new international actors being lured to the Swiss economy for its perceived stability. Despite strong levels of competence in major cities, one must acknowledge that the prosecution authorities of smaller cantons are frequently overwhelmed when confronted with technologically superior criminals. Further, Switzerland's alignment with the European Union (EU) in the sanctions regime against the Russian Federation demonstrates its efforts to match its regulation to combat financial crime. The tensions in the Middle East and the restriction in the trade of oil under the EU sanctions regime has added layers of complexity and pressure on companies operating in this challenging industry.

SOUTH AFRICA

Smit: South Africa's white-collar crime landscape is being reshaped by several converging factors.

These factors collectively render white-collar crime transnational, digitally sophisticated and difficult to prosecute. Reported instances of white-collar crime – which includes commercial crimes – have risen by in excess of 50 percent between 2020 and 2025. This increase can be attributed to perceived prosecutorial authority weaknesses, which embolden those perpetrating commercial crimes to persist in their endeavours, as criminal consequences do not always or are very slow to follow. AI-enabled deepfakes and cryptocurrency fraud have industrialised scam operations, with AI-powered schemes proving significantly more profitable than traditional ones. Domestically, the publicised skills shortages in the prosecuting authority and underreporting of crimes have hindered enforcement efforts. The proposed Protected Disclosures Bill of 2026 seeks to bolster whistleblower protections, including criminalising retaliation against whistleblowers, a reform prompted in part by referendum findings that less than 50 percent of individuals would report corruption.

R&C: What recent regulatory or legislative developments have most significantly reshaped corporate compliance obligations in your region – such as those relating to anti-money laundering, sanctions, reporting requirements or whistleblower protections, for example?

UNITED STATES

Carr: Recent developments in the US have not eased compliance pressure; they have made it harder to navigate. The challenge is twofold: knowing and anticipating where the administration may deprioritise enforcement, while also implementing new regulations in hot topics like prediction markets and digital assets. Enforcement priorities have shifted in ways that force companies to revisit established programmes. The Department of Justice's (DOJ's) 2025 reset on Foreign Corrupt Practices Act enforcement is a clear example: anti-corruption risk did not disappear, but the compliance calculus became less straightforward. At the same time, the enacted Guiding and Establishing National Innovation for US Stablecoins Act and the still-pending Digital Asset Market Clarity Act could together finally provide a comprehensive framework for digital assets in the US, fuelling rapid growth in that space. The Financial Crimes Enforcement Network's (FinCEN's) 2026 proposed AML and countering financing of terrorism programme rule pushes firms further toward effectiveness-based, risk-based compliance, which may force companies to rethink existing compliance models and raise the bar for would-be entrants in the digital assets space.

SINGAPORE

Ved: The recent story across Asia is not defined by any single development, but by the simultaneous emergence of distinct regulatory phenomena, for which many compliance programmes are structurally underprepared. The first is the emergence of cooperation frameworks. Singapore's first deferred prosecution agreement (DPA) in the Seatrium case signals that self-reporting and remediation now yield materially better outcomes than contested prosecution, a development that reshapes the disclosure considerations for the region. Many enforcement cases avoid publicity with appropriate management and counsel, so it is often difficult to clearly see the benefits of self-reporting before matters explode. The second is the extraterritorial expansion of enforcement. Domestic regulators in Asia are demonstrating a greater willingness to pursue multijurisdictional coordination to tackle cross-border crimes, and regimes such as China's anti-corruption framework are extending scrutiny to foreign entities with local exposure. The third is the closing of formal transparency gaps. Vietnam, Indonesia and India are advancing beneficial ownership regimes in line with global standards. The resulting risk landscape is that companies are navigating multiple evolving regulatory developments without the benefit of a unified regional playbook. Lastly, Asian regulators are partnering with other international enforcement agencies and increasingly investigating multinational corporations, including US-headquartered companies.

> **"It is likely that the world is on the brink of a new regulatory enforcement cycle. A major economic correction, collapse or financial scandal will likely act as the trigger."**
>
> *Simon Airey,*
> *McDermott Will & Schulte*

JAPAN

Nasu: One of the most significant recent legislative developments reshaping corporate compliance obligations in Japan is the 2025 amendment to the Whistleblower Protection Act, effective from 1 December 2026. The amendment expands the scope of protected whistleblowers to include freelancers and strengthens protections against retaliation. Dismissals or disciplinary actions within one year of a report are presumed to be motivated by whistleblowing, shifting the burden of proof to the employer. In addition, criminal penalties, including imprisonment or fines, have been introduced for retaliatory conduct. These reforms substantially strengthen whistleblower protections and increase enforcement risk. As a result, companies are expected not only to establish formal whistleblowing frameworks, but also to ensure their effective operation through robust governance, investigation mechanisms and safeguards against retaliation.

> **"White-collar crime is increasingly technologically-enabled and borderless, requiring a fundamentally different response from both companies and regulators."**
>
> *Khushaal Ved, Hogan Lovells*

UNITED KINGDOM

Airey: The UK Economic Crime & Corporate Transparency Act 2023 (ECCTA) introduces two seismic changes to corporate criminal liability. The first significantly expands the type of people who can automatically infect a company with criminal liability for a wide range of economic crimes – now anyone who satisfies the statutory definition of being a 'senior manager' can lead to the company being prosecuted for their actions. This provision came into force on 26 December 2023. Separately, on 1 September 2025, the Act introduced a new criminal offence where a company fails to prevent fraud by any of its 'associated persons' including all employees, agents and subsidiaries. Both provisions have extensive extraterritorial effect, applying to people, conduct and companies outside the UK. On 26 June 2026, it is expected that the law will be expanded to cover all crimes committed by senior managers, not just economic crimes. Together, these changes represent the biggest upheaval in corporate criminal liability for over 150 years.

SWITZERLAND

Frey: Three recent topics can be identified. First, the adoption of the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners (LETA), which is set to come into effect in autumn 2026 and primarily introduces new obligations for legal entities with a Swiss nexus – to report the beneficial owners to the transparency register. It is expected that the new requirements will have far-reaching consequences in the areas hitherto considered susceptible to money laundering such as transactions with non-operative companies. Second, the continued effort of the Federal Council regarding its sanctions alignment with the EU targets requires additional diligence from financial service providers and advisers. As for whistleblower protection, it must be noted that neither the EU Whistleblower Directive with its far-reaching impact nor pressure from the Organisation for Economic Co-operation and Development (OECD) has yet resulted in the passing of national legislation to protect whistleblowers. However, some federal departments and cantonal authorities have set an example for the private sector by implementing whistleblowing platforms.

SOUTH AFRICA

Smit: The most significant recent developments reshaping corporate compliance in South Africa have emanated out of South Africa's concerted efforts toward its official removal from the Financial Action Task Force (FATF) grey list in October 2025 – after having completed the bulk of the action plan that included strengthened and widespread AML enforcement by the Financial Intelligence Centre, Financial Services Conduct Authority and the Prudential Authority. South Africa's National Treasury further published the Draft General Laws Amendment Bill of 2025 for public comment, which signalled further legislative tightening. Regulators have adopted a more assertive posture, pursuing high-cost penalties against both institutions and individuals for compliance failures. The crypto travel rule took effect on 30 April 2025, requiring cryptoasset service providers to pass originator and beneficiary information with transfers. South Africa's fifth round FATF mutual evaluation commences in 2026, sustaining pressure on firms to demonstrate compliance outcomes.

MEXICO

García Cueva: The regulatory environment in Mexico has shifted more in the past 18 months than in the previous decade. The US FinCEN designated three Mexican financial institutions as primary money laundering concerns in June 2025, leading to their dissolution. Recent reforms to the Mexican AML law in 2025 are a significant overhaul, expanding beneficial ownership definitions and imposing new reporting obligations for virtual assets and trusts. Tax reforms in early 2026 grant audit powers to verify the materiality of transactions, and false invoice issuance is now classified as a crime warranting pretrial detention. The new antitrust framework reformed in late 2025 maintains cartel conduct as a white-collar crime and imposes heightened administrative sanctions of up to 15 percent of the offenders income. Collusion may be sanctioned if information is exchanged among competitors, not only strictly by engaging in an illegal agreement. In this context, compliance can no longer be compartmentalised.

R&C: How is technology reshaping both criminal methodologies and investigative techniques related to white-collar crime in your region?

SINGAPORE

Ved: Technology is both a weapon and a solution in white-collar crime today – reshaping not only how misconduct is perpetrated, but how it is detected. The same AI-enabled tools used to detect anomalies are being weaponised by bad actors to commit increasingly sophisticated frauds. Across Asia, encrypted messaging platforms have replaced traditional paper or email trails. Critical evidence is often dispersed across devices, platforms and jurisdictions. But the investigative response has sharpened in parallel. Enforcement agencies such as Singapore's Commercial Affairs Department and the Monetary Authority of Singapore, as well as Hong Kong's Securities and Futures Commission, have increasingly embedded data analytics, AI-assisted tools and advanced digital forensics into their investigative frameworks, enhancing investigative efficiency and capabilities. The implication is a shift in investigative dynamics. As regulatory detection moves upstream, companies have a narrowing window to act first. At the same time, companies that invest in or deploy – often with trusted advisers – analytics and technology to enhance internal controls gain a strategic opportunity to detect and respond to emerging compliance issues.

JAPAN

Nasu: Advancements in digital technologies, particularly AI, have contributed to increasingly sophisticated cyber threats in Japan, including phishing and impersonation attacks. In the context of white-collar crime, however, vulnerabilities within corporate IT environments, such as weak access controls and insufficient monitoring, are expanding opportunities for misconduct. While the widespread use of cloud services has improved data accessibility, deficiencies in access management, sharing settings and audit functions may allow unauthorised employees to access sensitive information, increasing the risk of internal misconduct such as data leaks and insider trading. From an investigative perspective, machine learning is widely used to enhance efficiency by enabling large volumes of data to be analysed and classified automatically. More recently, genAI has further improved investigative accuracy, including in the analysis of low-resolution footage and detection of digitally altered documents or images.

UNITED KINGDOM

Airey: Abuse of cryptocurrencies is heavily implicated in a range of crimes internationally and the speedy movement and concealment of the proceeds of crime. But law enforcement agencies are catching up fast and have developed their own technologies to monitor, detect and prevent related crimes. Technology and dedicated data portals between international law enforcement agencies have improved cooperation, and the ability to intervene quickly. Covert operations are on the increase and formal alliances such as the Prosecutorial Taskforce formed between the UK, France and Switzerland are expected to yield positive results. The death of cooperation with the US DOJ has been much exaggerated – the DOJ remains well resourced, focused and robust. Enhancements to money laundering regulations and AI-assisted capabilities are resulting in huge amounts of data being provided to prosecutors.

SWITZERLAND

Frey: Technology is impacting white-collar crime in Switzerland on both sides of the equation. Criminals now have ready access to the sophisticated tools enabling them to commit financial fraud. The Swiss Banking Ombudsman just recently confirmed that his office is dealing with a high number of cases of fraud involving social engineering. The investigative advances introduced through new technology on the other hand also allow for more efficient and effective responses in corporate investigations with large datasets. AI tools are able to break down and distil large data volumes in less time and minimise oversights. Recent research by Swiss banks and the financial regulator, the Swiss Financial Market Supervisory Authority, has confirmed this development.

SOUTH AFRICA

Smit: Technology is reshaping white-collar crime in South Africa. On one hand, criminals are increasingly employing sophisticated digital and social engineering methods in their criminal campaigns, the use of which makes detection harder. That said, AI and machine learning tools are also being deployed from an investigative perspective to detect anomalies suggestive of fraud, while advanced analytics and digital verification tools are assisting in prevention.

MEXICO

García Cueva: Technology is the great accelerator. On the criminal side, AI-generated documentation is now being used to support fraudulent invoicing at a level of sophistication that renders traditional audit mechanisms obsolete. For companies, best practices in corporate compliance programmes suggest focusing on whether companies have assessed AI-related compliance risks, implemented governance frameworks and trained employees on emerging technology threats. On the enforcement side, we are witnessing a digital transformation across Mexican enforcement agencies. The Financial Intelligence Unit has deployed AI-driven early detection models to detect cross-border money laundering patterns. The Mexican Antitrust Commission has digitalised its information-gathering and is using technology to detect anticompetitive patterns. AI should be leveraged within a framework of strict ethical principles, data governance and firm-wide training. The question is no longer whether to integrate technology into compliance, but how quickly and how responsibly it can be done.

UNITED STATES

Carr: AI-enabled fraud is faster, cheaper and more scalable than anything we have seen before – and bad actors are deploying it without regard for public safety, putting both organisations and financial markets at risk of destabilisation. It is already outpacing most organisations' ability to detect and respond, which means risk is evolving faster than governance. At the same time, the volume of data in investigations is set to double or even quadruple over the next two to three years, driven by both human and machine-generated evidence, including synthetic identities and activity trails. Investment in new tools – or access to them – is non-negotiable in today's environment. A major challenge is that organisations must respond at the speed of the threat while still balancing cost, governance and security requirements. The result is growing friction across compliance, cyber security and investigative teams as they try to apply yesterday's controls to today's threats.

R&C: What trends are you seeing in the use of voluntary self-disclosure by corporates? How do enforcement bodies in your region incentivise or discourage such disclosures?

JAPAN

Nasu: In Japan, incentivised corporate voluntary self-disclosure mechanisms primarily operate in two areas. One is the leniency programme under the Antimonopoly Act. Where a company voluntarily reports cartel conduct and cooperates with the Japan Fair Trade Commission, administrative surcharges may be reduced or eliminated depending on the order of application and the degree of cooperation. Disclosures made after the commencement of an investigation are also eligible, encouraging both early reporting and substantive cooperation. The number of leniency applications declined during the pandemic but has increased significantly in recent years, suggesting that the programme remains an important mechanism in practice. By contrast, the surcharge reduction regime under the Financial Instruments and Exchange Act is narrower in scope, offering a uniform 50 percent reduction only for voluntary disclosures made before an investigation begins. Recent policy discussions have considered introducing a more flexible, cooperation-based framework like the antitrust model, indicating potential expansion of incentives.

> **"South Africa's fifth round FATF mutual evaluation commences in 2026, sustaining pressure on firms to demonstrate compliance outcomes."**
>
> *Tim Smit,*
> *Cliffe Dekker Hofmeyr Inc*

UNITED KINGDOM

Airey: The decision by a company to make a voluntary disclosure of criminal conduct remains one of the most difficult decisions it may ever make. In the UK, the incentives for making a disclosure are often very difficult to balance with an assessment of the risk of getting caught and various challenges associated with the current regime relating to DPAs. Companies are hugely concerned about the collateral damage that often follows from related civil litigation, the prosecution of individuals, reputational damage, impacts upon banking and insurance relationships, and so on. Recent guidance issued by the UK Serious Fraud Office has attempted to introduce more clarity into the process and emphasises the importance of early and full disclosure, cooperation, remediation and the importance of a comprehensive compliance programme. The new guidance effectively offers a guarantee that the SFO will not prosecute and will instead issue an invitation to negotiate a DPA unless 'exceptional circumstances' apply.

“White-collar crime still comes down to a simple constant: bad actors want what you have. What has changed is the speed, scale and sophistication of how they try to get it, and, increasingly, why.”

Holly P. Carr, BDO

SWITZERLAND

Frey: In Switzerland, voluntary self-disclosure is prevalent in the area of taxes: companies or individuals can file a voluntary disclosure if they reveal tax-relevant facts that were previously undeclared. The key condition is that the tax authority must not already know about the issue and the company or individual must cooperate fully. Back taxes and interest remain payable, but the penalty may be waived. For companies, careful review is essential because incomplete disclosure can jeopardise the protective effect. In practice, the disclosure is usually submitted in writing and at an early stage, often with tax advice. In criminal law, voluntary self-disclosure by companies can result in a reduced punishment. Also, under antitrust law, the first party to voluntarily disclose information may be exempt from penalties if their cooperation is deemed sufficient.

UNITED STATES

Carr: Voluntary self-disclosure remains an important feature of the US enforcement landscape, but companies still approach it cautiously because the benefits are not always clear at the outset. The DOJ has worked to reduce that uncertainty through its revised 2025 'Criminal Division

Corporate Enforcement and Voluntary Disclosure Policy' and, in 2026, the first-ever Department-wide Corporate Enforcement Policy, both of which signal a more standardised commitment to rewarding timely disclosure, full cooperation and effective remediation. The Securities and Exchange Commission (SEC) remains more discretionary, but emphasis by Paul Atkins, chair of the SEC, on the SEC's core mission and on greater predictability, fairness and due process in enforcement signals an effort to bring greater consistency to the agency's approach. The harder variable for organisations considering self-reporting is often the states, where attorneys general take less uniform approaches that can shift meaningfully based on the current political and policy priorities of a given jurisdiction.

MEXICO

García Cueva: Voluntary self-disclosure is one of the areas that could have the most strategic value in Mexico. In antitrust, the Mexican leniency programme for cartel cases is the most structured voluntary disclosure instrument available, providing pathways for leniency from criminal prosecution and very significant penalty reductions. In the financial crime space, recent reforms recognise spontaneous compliance as a mitigating factor. In anticorruption, administrative responsibilities law contemplates reduced sanctions for companies with integrity policies. The more disruptive incentive structure is now external but with impact in Mexico. The US DOJ corporate whistleblower programme covers tips related to cartel-connected violations. This creates powerful incentives for those inside Mexican operations to report directly to US authorities. Crafting robust compliance mechanisms including internal reporting channels, before they are needed – not in the middle of a crisis – is one of the most important decisions.

SOUTH AFRICA

Smit: South Africa does not have a formal, generalised voluntary self-disclosure regime for white-collar crime akin to the DOJ's Corporate Enforcement Policy. Investigations may be triggered by voluntary self-disclosures, but the National Prosecuting Authority does not offer a structured declination or leniency framework for corporates that self-report. Mandatory reporting obligations under Prevention and Combatting of Corrupt Activities Act and the Financial Intelligence Centre Act create statutory disclosure duties rather than voluntary incentives. Post-greylisting reforms, including the permanent Investigating Directorate Against Corruption and proposed Public Procurement Bill, signal increased enforcement capacity, which may indirectly encourage proactive corporate disclosure as prosecution risks rise. However, the absence of guaranteed leniency for voluntary self-disclosure remains a notable gap.

SINGAPORE

Ved: Voluntary self-disclosure in Asia is complicated. Unlike in the US or UK, the regional framework is fragmented and unpredictable. Disclosure to one regulator does not insulate companies from enforcement by others – risking piling-on and possible expansion of the matter – and managing parallel processes across incompatible frameworks creates significant risk. Recent DOJ guidelines introduce a new variable: prosecutors must now consider whether a foreign regulator is already investigating the same conduct, creating an incentive to disclose to a local regulator first. In Asia, Singapore's framework is the clearest development – the Seatrium DPA demonstrated that genuine cooperation yields tangible benefits. However, often these regulatory investigation cases take years to close. Elsewhere, the picture is uneven. India offers a pragmatic settlement mechanism for securities matters but lacks formal frameworks under corruption and money laundering laws. In China, blocking statutes and state secret laws make parallel processes particularly challenging. Cooperation credit is real in this region, but disclosure strategies must be carefully considered and deployed.

R&C: What practical steps should companies take to strengthen their compliance frameworks, enhance risk management, improve their ability to detect and deter internal white-collar crime, while also preparing for the next wave of regulatory expectations?

SWITZERLAND

Frey: Swiss companies must stay abreast of recent legislative developments such as the new obligations that will be coming into effect with the LETA, such as reporting their beneficial owners, by checking whether they fall within the scope of the Anti-Money Laundering Act and by tracking changes to the sanction's ordinance. In addition, internal risk management systems must be introduced, and employees must be regularly trained to raise fraud awareness across the entire workforce. Where a company falls under the scope of LETA, it however may also benefit from access to the transparency register to obtain comfort as to the averments of their clients. The upcoming new regulatory framework remains challenging and requires stringent preparation to stay ahead.

MEXICO

García Cueva: Whether for multinationals entering Mexico for the first time or Mexican companies expanding internationally, prevention is cheaper than remediation, and functional compliance is cheaper than crisis management. The standard that prosecutors and regulators apply is clear: is the programme well-designed, adequately resourced and does it work in practice? 'Paper compliance', policies that exist on a shelf but are disconnected from operations, creates a false sense of security. It is important to base any compliance effort on an objective assessment of the company's specific risk profile, context and key instruments. Aligning a compliance programme adapted to the company's reality, both in the approach and mechanisms chosen, will contribute to risk prevention and mitigation. And technology must be central: AI-driven monitoring, data for anomaly detection and digitalised processes deliver a competitive advantage. Organisations that invest in prevention today position themselves to thrive in Mexico.

> **"Mexico is amid the convergence of extraterritorial enforcement, with an expanding and more aggressive domestic regulatory context."**
>
> *Carlos García Cueva,*
> *Aziz & Kaye Business Law*

SOUTH AFRICA

Smit: South African companies must employ a multilayered approach to strengthening their compliance and risk management frameworks. Key steps include establishing a dedicated compliance function that reports directly to the board, implementing robust whistleblower mechanisms and fostering a culture of ethical conduct through regular training. Also important is to conduct periodic fraud and corruption risk assessments and map vulnerabilities across procurement, finance and third-party relationships, with particular attention to the Companies Act and the Prevention and Combatting of Corrupt Activities Act. Companies should also deploy data analytics and continuous monitoring tools, strengthen their internal audit capabilities and implement effective segregation of duties within the organisation. Developments from bodies such as the Financial Sector Conduct Authority and the Companies and Intellectual Property Commission should also be monitored. Finally, companies are well-advised to engage proactively with emerging environmental, social and governance and beneficial ownership disclosure requirements, benchmarking frameworks against established governance principles.

SINGAPORE

Ved: The gap is growing between companies that construct sophisticated compliance systems and those running legacy compliance controls. This is widening across Asia. Regulators are making that gap consequential. Detection capability is now the differentiator: companies able to present a regulator with a completed internal investigation retain strategic control of the narrative, but those that scramble after a dawn raid lose that advantage. Are complaints or evidence of misconduct being reported? And are they being reported internally or leaking into commercial business, creating unsustainable revenue and irreparable short-term reputational damage? In my experience, detection in this region most often fails because of overreliance on local management to self-report risks – notwithstanding the obvious disincentives to disclose underperformance or personal misconduct to headquarters. This is the same local management who were given increased autonomy in the pandemic years, and where and when business seemingly flourished. The fix is not more policies but independent visibility: centralised AI-driven transaction monitoring, accessible whistleblower channels that bypass local management and audit rights that headquarters actually exercise. Companies should also stress-test their incident response now – identifying trusted local counsel, establishing privilege and document preservation protocols, and mapping internal response procedures for crisis governance – rather than improvising those during a crisis.

UNITED STATES

Carr: Companies need to move faster – much faster. Annual, check the box governance reviews are not built for a threat environment that is accelerating by the minute. Controls that still depend heavily on manual processes should be reassessed now, with a plan to move, where appropriate, toward secure automated continuous monitoring. But the conversation cannot stop at AI. AI is already making fraud faster, cheaper and easier to scale. Quantum computing presents a different but equally serious strategic threat to data confidentiality, authentication and operational resilience, including through 'harvest now, decrypt later' scenarios that could turn yesterday's data theft into tomorrow's crisis. Amid all of this technology-driven pressure, the human element matters more, not less. Companies will not manage these risks effectively if the issue stays trapped in compliance or IT. The organisations best positioned to respond will be the ones that can communicate risk clearly, build alignment across the board and C-suite, and make decisions at the speed this threat environment now demands.

UNITED KINGDOM

Airey: As a result of various issues, it is likely that the world is on the brink of a new regulatory enforcement cycle. A major economic correction, collapse or financial scandal will likely act as the trigger. Aggressive activity by the press, politicians and the public will result in renewed activity by prosecutors. At such times, companies should not be economising on their compliance efforts. The reality is that the same pressures that lead to misconduct often mean that resources are squeezed. Companies must therefore carefully assess risk and target resources wisely. AI technology and skilled compliance professionals can assist, but senior management has a huge part to play. Many of the provisions of the UK government guidance relating to ECCTA put a sharp focus on top-level commitment to preventing crime. To this extent, compliance, like accountability when things go wrong, ultimately starts and ends in the boardroom.

JAPAN

Nasu: In Japan, the next phase of white-collar crime regulation is likely to be characterised less by new legislation than by the gradual strengthening of enforcement under existing frameworks. A key example is the anti-bribery regime under the Unfair Competition Prevention Act (UCPA), including the 2023 amendment – effective from 2024 – which increased penalties and expanded extraterritorial reach to cover overseas misconduct by non-Japanese employees of Japanese companies. The UCPA remains subject to OECD monitoring, with a phase five evaluation scheduled for 2028 expected to assess enforcement in practice. Against this backdrop, companies should strengthen risk-based compliance across group entities, ensure employees understand applicable laws across jurisdictions, focus on high-risk areas and maintain effective whistleblowing mechanisms supported by clear senior management commitment. R&C

Enjoyed this article?

Join our community for free to access more expert insights.

Join Now - It's Free