Combatting fraud in a perfect storm: Calls to action.

ACCA

IN COLLABORATION WITH:

ACFE Association of Certified Fraud Examiners

The Institute of Internal Auditors

ISC2

CISI Chartered Institute for Securities & Investment

airmic

Association of Corporate Investigators

Why these calls matter

Fraud is no longer a side risk – it's a systemic threat amplified by economic distress, regulatory rollback, geopolitical volatility, and artificial intelligence (AI) as a 'truth-bending' machine. While organisations acknowledge the risk, responses remain uneven, fragmented, and often cosmetic. Controls exist on paper, but culture and conduct tell a different story.

ACCA's cluster analysis makes the challenge plain: perceptions of fraud, its drivers, and remedies diverge sharply across professional groups – even within the same organisation. Some see reporting as safe and effective; others see it as futile or dangerous. Ownership is misaligned – boards are expected to lead, yet compliance and audit teams carry the weight. In the gaps, rationalisation thrives: *'a little skimming doesn't hurt'*, *'it's just shrinkage'*, *'everyone does it'*.

Old certainties are collapsing. The social contract between employer and employee is fraying. Reputation risk no longer restrains behaviour in some quarters. AI has blurred the line between truth and fiction, enabling fraud at scale and speed we've never faced before.

In this environment, the cost of inaction is existential. These calls to action move the conversation from awareness to accountability. They are practical, evidence-based, and behavioural at their core. Each answers a simple question: what must change now to make fraud prevention real? They are not a checklist – they are a reset: a way to embed critical thinking into governance, replace 'tick-the-box' with 'test-the-system', and make integrity visible in decisions and outcomes.

Governance and ownership – who owns what and how we know

1. Make fraud a standing board item with decision-ready intelligence

Boards do not need another 600-page pack competing for five minutes of attention. What they need is a clear, repeatable way to see whether the organisation learns fast – intelligence that shows how signals became decisions and decisions became results.

What boards should ask in the first fraud-focused meeting:

- **Foundation:** What fraud did we detect versus report last year – and what's the gap? Was the detected fraud listed in our current register? If not, why did we miss it? Show me our fraud risk assessment (FRA): when done, who contributed, what changed? Use heatmaps to reveal governance blind spots – those areas where everyone assumes someone else is watching – before they become breaches.
- **Capability:** Can finance, cyber, and procurement see each other's alerts, or do they work in silos? Deploy AI or analytics to surface patterns across departments, filtering false positives and revealing genuine threats. Do we have forensic capacity on-call? What percentage of staff had fraud training this year – including deepfakes and how to report?
- **Culture:** How many concerns were raised, what proportion investigated, and do staff know outcomes? When did someone senior last face visible consequences? Can you show evidence that reporting is safe – not policy, but retaliation monitoring and outcome transparency? Track retaliation through patterns in assignments, ratings, and career progression, not just formal complaints.
- **Forward-looking:** What scenario would break us financially or reputationally – have we stress-tested it? What changed since our last meeting that affects fraud risk? Include external benchmarking with similar institutions to learn how they responded to comparable threats.

What the dashboard should show:

One page, one storyline: time-to-acknowledge, triage, decide, and resolve for fraud signals; prevented loss versus control spend; quarterly stress test results (what broke, what was fixed); retaliation checks and speak-up outcomes. The goal is tempo and consequence visibility, not compliance theatre.

The first 48–72 hours determine whether you contain damage or compound it:

Boards need crisis playbooks that answer: Who gets called? Who decides? Who investigates independently? What gets frozen immediately? Include draft templates for regulators, investors, and media to enable rapid, coordinated damage control.

For suspected executive fraud, the playbook should cover: preserve evidence, secure finance systems, appoint an independent incident lead, and temporarily segregate signatory powers if management holds them. Speed beats certainty when containment is the priority.

2. Close the ownership vacuum – publish a one-page fraud RACI and establish a fraud council

Boards can set tone and approve frameworks, but real operational control and resource allocation sit in the first line. If fraud is treated as a compliance or second-line issue, it gets skinny resources and remains reactive.

R	**Responsible** Who is/will be doing this? Who is assigned to work on this task?
A	**Accountable** Whose head will roll if this goes wrong? Who has the authority to take decisions?
C	**Consulted** Anyone who can tell me more about this task? Any stakeholders already identified?
I	**Informed** Anyone whose work depends on this task? Who has to be kept updated about progress?

The structural fix is clarity

First line owns prevention and sets operational culture; second line defines standards and monitors risk thresholds; internal audit assures independently; investigations must be firewalled from line management, with clear service-level agreements and consistent board reporting.

Cultural credibility collapses when consequences follow rank rather than conduct. Boards should demand a one-page RACI that names owners for prevention, detection, investigation, and remediation across fraud types, with escalation authority that clarifies not just who acts, but who intervenes and at what point.

Operationalising ownership

A RACI clarifies roles on paper; a fraud council makes them real in practice. This is a small, cross-functional team with explicit mandate and weekly operating rhythm. The mandate is straightforward: hunt for fraud signals, triage responses within defined service levels, own remediation tracking, and escalate to the board when thresholds breach.

- **Operating rhythm:** Hold weekly triage sessions to review alerts, assign ownership, and track closure; monthly deep dives for root cause analysis and emerging threats; and quarterly board reports summarising residual risk, prevention ROI, triage performance, and culture metrics. The council breaks down silos, so patterns become visible before losses crystallise.
- **Board checkpoint:** Does your fraud council have budget authority and transaction-pause power, or must they escalate for permission? The former prevents fraud; the latter documents it. How often do you see reports and how do you know what has changed?

3. Apply 'substance over form' as a living principle – *True and fair* for today's risks

***True and fair* means full visibility.** Directors have a legal duty to ensure accounts give a *true and fair* view – even if that requires going beyond what current accounting standards explicitly mandate. This complements – not contradicts – existing International Financial Reporting Standards (IFRS) principles, especially in areas where material risks intersect with user decision-making. In a poly-crisis environment, material risks like cyberfraud, geopolitical exposure, climate impacts, and AI liability may warrant disclosure in the notes to accounts when relevant to users' decisions. This isn't about adding more reports – it's about integrated thinking, where boards speak with one voice on enterprise value, rather than leaving users to piece together financial and non-financial disclosures.

To support this, build an evidence hierarchy for key judgements – prioritising provenance and independent corroboration. Where risks are material, directors should add decision-relevant context to ensure financial statements remain *true and fair* in a world moving faster than standards. The question is no longer whether every line of the standard is met, but whether the full picture is visible.

4. Put investors and asset owners to work – stewardship with anti-fraud teeth

Institutional investors command leverage but often deploy it passively. Ask for evidence of FRA cadence and maturity, whistleblowing credibility (completion and feedback loops), readiness for AI and crypto risk, and cross-team triage discipline.

Tie engagement and investment decisions to governance changes where gaps persist. When boards see that capital allocation hinges on prevention maturity, momentum follows.

5. Recognise fraud as multinational and tailor controls to jurisdictional reality

The fiction of 'global' fraud frameworks is collapsing. Fraud exploits jurisdictional seams where laws clash with whistleblowing policies, data protection rules differ, and consequence management varies wildly.

What this means operationally: a policy written in headquarters cannot be cut-and-pasted across countries. Boards must demand jurisdiction-specific FRAs that account for legal contradictions within your footprint (Malaysia's fraud laws versus whistleblowing protections; Switzerland's banking secrecy versus beneficial ownership transparency), cultural norms around hierarchy, speaking up, and retaliation (Asia-Pacific contexts where challenging authority is seen as disloyalty; contexts where consequence gaps enable impunity), enforcement capacity (countries with laws on paper but no resources to prosecute), and language and translation of policies into local languages, not just English.

Build playbooks that map jurisdiction-specific speak-up routes, retaliation protections, MLA options, and evidence rules – because fraudsters exploit the gaps one-size-fits-all frameworks ignore.

6. Close the law-versus-reality gap – enforcement lags policy everywhere

From the UK's Economic Crime and Corporate Transparency Act (ECCTA) to whistleblowing directives in the EU and crypto regulations in Asia, the legal landscape is expanding, but enforcement and cultural realities lag.

'There's always a law and the application of the law. These are two different things.'

Mauritius roundtable participant

Jurisdictions like the UK, Australia, and Singapore are extending failure-to-prevent regimes beyond fraud to cover money laundering and cybercrime. ECCTA is now being tested in live investigations, with regulators scrutinising not just policies but evidence of cultural integration. This intensity of corporate liability signals a fundamental shift: organisations can no longer treat compliance as a paper exercise.

Move beyond adequate procedures:

- **Annual FRAs that result in real change:** Conduct FRAs that identify control gaps, allocate resources to high-risk areas, and document changes to demonstrate reasonable procedures under failure-to-prevent regimes.
- **Embed board accountability through fraud KPIs:** Include override rates, investigation closure times, and speak-up outcomes in board packs to ensure oversight effectiveness.
- **Close the cultural gap through visible leadership:** Show leadership commitment through anti-retaliation assurances, transparent case outcomes, and equal consequences for all levels.
- **Localise whistleblowing mechanisms:** Adapt reporting channels to cultural and legal realities, offering anonymous and dual-track options where frameworks conflict.
- **Invest in enforcement partnerships:** Build proactive relationships with regulators and law enforcement and join industry consortia for cross-border intelligence sharing.
- **Leverage technology where regulators can't keep pace:** Use enterprise-grade AI for anomaly detection and behavioural monitoring – not insecure public tools.
- **The ECCTA test case:** Move beyond compliance by embedding prevention into culture and governance, aligning financial and non-financial reporting to withstand scrutiny.

Detection, response and resilience – from reactive to ready

7. Run quarterly reverse stress tests and ghost-hack critical pathways

Organisations that move beyond compliance perform reverse stress tests – asking not *'what might go wrong?'* but *'what would break us?'* – and then red-team those failure points. Blend red-team exercises (tech, social engineering, process abuse) with mystery-customer tests of onboarding, Know Your Customer (KYC), credit, and vendor set-up.

Record deepfake and business email compromise drill pass-rates, time-to-detect, time-to-resolve, and the percentage of critical controls that failed then got fixed – then retest. Regulators in new-bank settings have insisted boards walk through live fraud and cyber scenarios; those sessions reveal not only process gaps but how the board behaves under pressure.

The European Central Bank (ECB) is mandating a reverse stress test on geopolitical risk for all banks under its direct supervision. From 2026, banks will be required to 'assess which firm-specific geopolitical risk scenarios could severely impact their solvency' as part of their internal capital adequacy assessment process.[1]

8. Modernise detection and triage – analytics by default, signals not samples

Deploy full-population analytics (accounts payable, accounts receivable, payroll, expenses) plus behavioural indicators (override patterns, out-of-hours approvals, engagement-performance hotspots). One UK public-sector example illustrates why this matters: a worker held four council jobs simultaneously for years; traditional detection cycles and reviews failed to spot it. Sampling misses patterns; analytics surfaces them.

The fraud council becomes operational here, meeting weekly to triage signals, assign ownership, and track closure. Measure prevented loss, not just incidents closed. Track time-to-decision and time-to-resolution; publish fixes.

Show the business case: Use a simple ROI formula to demonstrate prevention value: Prevented Loss = (Blocked payments + Avoided fines + Recovered assets) – Cost of controls (technology, training, investigation). Example: A €45k fraud prevented vs €3k forensic review = €42k net benefit.

9. Treat geopolitics and insider risk as operational control problems, not headlines

Fraudsters and state-linked networks exploit sanctions loopholes, trans-shipment routes, and disinformation to expose weaknesses boards assume are distant. Map corridor exposure down to country and supplier level, embed beneficial ownership checks and audit rights into contracts, and rehearse cross-border playbooks – from mutual legal assistance to crypto-exchange requests – with forensic-grade documentation that stands up under scrutiny.

Geopolitical tensions also amplify insider and systemic risk. As Derek Leatherdale of Sibylline, a geopolitical risk analysis firm, notes: *'Fraud can easily be enabled by insiders… particularly those who have access to sensitive financial systems or payment authorisation processes. An insider programme can account for this as well as mitigate other insider risks, including those with geopolitical dimensions.'*

The recent Norwegian welfare fraud case showed how criminal networks used identity theft and coercion to manipulate state benefit systems at scale – a reminder that organised actors exploit trust-based digital systems, not just technology gaps.[2]

1 European Central Bank (2025). 'Stress tests in uncertain times: assessing banks' resilience to external shocks', ECB Banking Supervision blog, 5 September 2025. Available at: <https://www.bankingsupervision.europa.eu/press/blog/2025/html/ssm.blog20250905~781d5f81aa.en.html>

2 Rødevand, M. (2025). 'When the Norwegian State becomes the money launderer', LinkedIn post, 5 November 2025. Based on reporting by Dagens Næringsliv and statements by Oslo Police Chief Grete Lien Metlid.

Effective insider risk programmes layer behavioural monitoring, network-vulnerability checks, and cross-agency data sharing to detect both opportunistic and geopolitically motivated activity. Run quarterly simulations – sanctions evasion via trans-shipment, state-linked deepfakes targeting finance leaders, and conflict-driven privilege creep – to test how resilient your controls really are.

10. Fortify third-party and supply-chain integrity

Third-party risk isn't 'outside' – it's 'inside' by contract. Require audit rights, beneficial-ownership transparency, change-of-ownership monitoring, and off-boarding triggers. Continuously test vendor bank-change controls and split-invoice patterns. Value chains fail when the weakest link is exploited; boards should use shared guidance, pre-contract alignment, and packs for partners, raising standards collaboratively rather than waving audit rights after the fact.

'It's not just your entity – it's the whole value chain. If others fail, your purpose fails.'

Special interest group member

11. Work with law enforcement on prevention

Law enforcement faces court backlogs, prison constraints, and a surge in cyber-enabled fraud exploiting AI and anonymity, while resourcing gaps persist globally.

Criminals increasingly target accountancy firms and professional credentials, exploiting the trust ethical professionals attract. Roundtable discussions pointed to a prevention-first model, where professional bodies and law enforcement collaborate to stop fraud earlier. Where authorities publicise arrests and simplify reporting, intelligence flow improves dramatically. Members cited Hong Kong's press briefings and app-based reporting as an example.

Parallels were drawn with child protection reforms: systematic intelligence sharing and real-time vetting close gaps before harm occurs. The same logic applies:

- **Turn near misses into intelligence:** rejected suspicious clients or documents reveal emerging fraud tactics
- **Deploy expert volunteers:** experienced accountants support under-resourced police with forensic and training expertise
- **Enable real-time verification:** confirm credentials and risk profiles before bad actors exploit them
- **Strengthen cross-border cooperation:** leverage global professional networks to track international fraudsters

With the UK's centralised fraud reporting system launching in 2026, the profession should prepare to verify identities, detect credential misuse, and collaborate with law enforcement – starting with training, joint briefings, and intelligence-sharing agreements. This isn't about making accountants investigators – it's about making their expertise a first line of defence.

12. Run joint fraud and cyber drills

Authorisation is the new perimeter. Enforce least privilege and multi-factor authentication (MFA), especially for privileged roles. Apply out-of-band verification and dual authorisation on urgent or executive-style requests and bank changes. Test immutable backups and crisis communications. Track callback adherence and drill pass-rates.

The Co-op's 2024 cyber incident illustrates the value of speed over certainty: the retailer shut down systems quickly to contain the breach, limiting long-term damage despite short-term disruption. In contrast, Marks & Spencer's delayed response to a similar attack led to weeks of disruption, £300m in losses, and reputational damage. The first hours of a breach determine whether damage is contained or amplified.

Know your crown jewels: Boards should require annual CFO–CIO attestation on the location and protection of critical data assets. Cyber incidents show leaders often can't answer *'where is our customer data?'* – one firm lost data after backups were decommissioned without notice. Identify the 10–15 datasets that would cause material harm if compromised, document protection versus risk, and test recovery annually. Under ECCTA, you can't prevent what you can't locate.

13. Shift to active inquiry

Stop waiting for reports – verify and test. Professionals must move from passive receipt of information to active assurance. That means running your own data queries on vendor changes and override patterns, validating critical claims through independent checks like callbacks and out-of-band verification, and stress-testing controls through live exercises such as mystery shopping and red-teaming. If information is available, you have a duty to use it – relying only on what's supplied creates systemic blind spots.

This principle links directly to the 'substance over form' discussion: assurance isn't about paperwork, it's about evidence. The forum highlighted a striking asymmetry –organisations routinely value intangible assets like brand and intellectual property but rarely quantify the intangible risks that threaten them, from reputational collapse to regulatory sanctions. Boards should demand that intangible risk analysis sits alongside asset valuation. If you can't answer both *'what's our brand worth?'* and *'what's the downside if fraud destroys it?'*, your balance sheet tells only half the story.

Culture, behaviour and voice – reframe speaking up as contribution

14. Build speak-up systems that work

Reporting confidence depends on protection and proof. Credible systems combine simple routes, guaranteed anonymity, independent investigations, and visible leadership follow-through – because staff trust what leaders do, not what policies say.

Organisations need to enable people to raise concerns about conflicts of interest, process flaws, unintended greenwashing, or questionable judgement calls without fear of retaliation. The goal is recognising contribution, not creating a competitive marketplace for fraud detection.

Reward vigilance thoughtfully

Rather than viewing concerns as disloyalty, leading organisations publicly thank employees who identify supplier conflicts of interest, process vulnerabilities, or data misuse. Some use sliding-scale rewards for substantiated cases producing material recovery or risk reduction – though the key risk is creating a culture where employees hunt for dirt purely for monetary gain, turning colleagues into competitors rather than collaborators.

Bounty systems aren't suitable for all organisations, particularly those where regulatory obligations already mandate reporting, such as financial services AML/CTF requirements. They work best in large corporates, supply-chain-heavy sectors, and procurement-intensive public bodies where fraud prevalence is high, but detection is difficult. Smaller organisations under 250 staff may find recognition-only systems more culturally appropriate – public thanks, small gift vouchers, or formal letters of commendation achieve similar effects without complex payment structures.

Firewall investigations to strengthen trust

Separate reporter liaison from investigation. Team A manages intake, welfare, updates, and anti-retaliation monitoring. Team B conducts evidence gathering, interviews, and findings. Both share case ID and audit trail but don't directly interact with reporters.

In one regional bank adopting this model, average acknowledgment time fell from nine days to under 48 hours, substantiation rate increased from 18% to 29%, and a senior-subject case avoided premature closure because the liaison team kept the channel open while investigators escalated to external counsel.

Publicise outcomes to build trust

One manufacturer's quarterly speak-up outcomes note to all staff – showing anonymised case categories, resolution times, corrective actions, and lessons learned – produced a 22% increase in named reports within two quarters. Employees only keep raising concerns when they see action results.

Run witness-protection-style monitoring

Track utilisation, assignments, ratings, and pay for those who raised concerns – to catch retaliation before it entrenches.

What works: four non-negotiables

Credible speak-up systems require four essentials: simple localised reporting routes, guaranteed anonymity, independent investigations firewalled from management, and visible leadership commitment through transparent case reporting – without these, confidence collapses.

15. Align risk appetite from FOFO (Fear of Finding Out) to ‘find out fast’

Without a shareable fraud risk appetite and aligned incentives, people optimise optics, not integrity. They focus on looking compliant rather than being effective, avoiding uncomfortable questions and burying warning signs to protect reputations or hit targets. This is FOFO culture – where the fear of discovering problems outweighs the drive to fix them.

Zero tolerance sounds principled but is operationally dishonest. Every organisation accepts some level of fraud risk, whether they admit it or not. Some level of risk must be accepted for business to function – the key is ensuring proper controls are in place for the risks you choose to take.

Boards must define appetite honestly and test it under pressure. Define no-appetite zones, escalation thresholds, and tolerances for residual risk, then stress-test appetite against threats like deepfakes and supplier failure. Reporting breaches and near-breaches helps boards see how appetite holds under pressure – and whether stated principles match actual behaviour.

Reward blocked attempts, early interventions, supplier off-boardings, and near-miss interceptions. Track breaches and near-breaches openly, not as failures but as intelligence. When leadership sees prevention paying back, momentum holds.

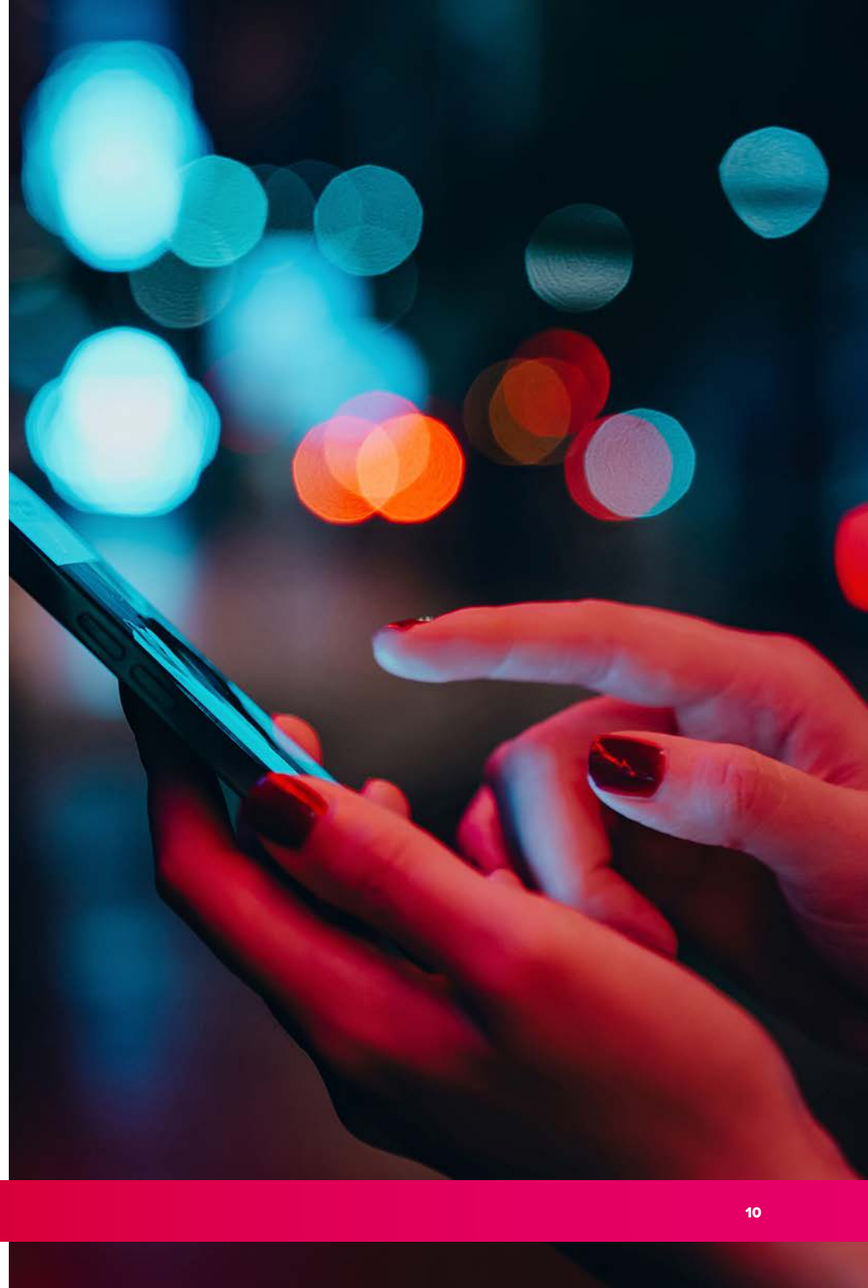
16. Make learning targeted, creative, and measured by outcomes

Gamified fraud awareness – using case-based trivia, puzzles, and incentivised video quizzes – drives real engagement across sectors and countries, unlike generic e-learning which ticks boxes but fails to shift behaviour.

Role-specific, moment-of-need guidance outperforms generic training. A procurement officer facing a suspicious invoice change needs a one-page ‘what-to-do-now’ card, not a 40-slide deck. Face-to-face delivery remains critical for culture-sensitive topics where nuance matters.

Top-down engagement transforms awareness from compliance burden to cultural imperative. Board-member walkabouts, quarterly sessions with police officers and anti-corruption units, and audit-committee sessions dissecting actual fraud cases make materiality visceral rather than abstract. When leadership participates, prevention becomes everyone’s priority.

Measure what matters: near-misses intercepted, callback verification rates, simulation pass-rates, and time-to-decision – not training hours completed.



Professional standards, assurance and capability

17. Make professional scepticism visible across audit functions

Hold the International Standard on Auditing (ISA) 240 – The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements – team discussion explicitly setting aside beliefs about management integrity; document fraud pathways by assertion and show how procedures respond. Challenge '*no fraud this year*' with evidence (FRA cadence, whistleblowing logs, response plans). In higher-risk areas, bring in forensic and data specialists.

For internal audit, assess whether controls really do stop bad outcomes (for example, AI and deepfake drills, regions with opaque beneficial ownership structures). Enable junior staff to escalate around hierarchy when *'something feels off'*. Report culture metrics (speak-up integrity, retaliation checks) alongside control tests. The goal is to make scepticism operational, not just a talking point.

18. Cross-team fluency for today's fraud

Modern fraud moves faster than governance structures. Environmental, social and governance (ESG)-related fraud, though understated in our survey, is rising sharply and spans sustainability, finance, legal, and governance domains. A shortage of forensic capacity compounds the risk. Professional bodies should co-develop training modules, shared typologies, and sector-specific forums where compliance officers, auditors, forensic experts, and technologists build mutual fluency.

Specialist certification is essential. Just as data protection laws drove formal training for data officers, the rise of whistleblowing legislation demands case-management expertise. Role-fit matters: finance teams need behavioural red flag and analytics training; procurement needs tools for ownership screening and collusion detection; HR and ethics officers need interviewing and psychological safety frameworks; IT and security need legal knowledge on evidence and cross-border cooperation. Continuing professional development should include simulations – deepfake payment requests, collusive bids, ESG data manipulation – where cross-functional teams practise triage, escalation, and decision-making under pressure.

19. Close the regulatory enforcement gap – lift standards at stock exchanges

Most exchanges require listed companies to have whistleblowing policies and mechanisms – but that's where scrutiny ends. Exchanges could lift standards by requiring annual attestation by the audit committee chair that internal channels are independent, protected, and board-visible; collecting confidential whistleblowing metrics such as volume, closure times, and retaliation complaints; mandating periodic external assurance of reporting systems for larger issuers; applying sanctions for issuers found to suppress or retaliate, with public censure for repeat offenders; and including whistleblowing oversight in mandatory director training.

This approach mirrors how exchanges drive governance improvements in other areas –using listing requirements to create minimum standards that regulation alone cannot enforce. When capital markets demand evidence of fraud prevention maturity, boards respond.

20. Prepare for the skills exodus and update standards continuously

Our research revealed a serious reality that some institutions have disbanded geopolitical risk functions as part of cost-cutting structures. At the same time, some governments are planning selective conscription of technology and engineering skills for national defence purposes. This creates a double crisis: current skills disappear as major advisory firms exit specialised fraud, cyber, and geopolitical risk services, whilst future skills won't develop because training pathways are being dismantled.

Professional bodies can develop specialised certifications in fraud case management, geopolitical risk assessment, and cyber-fraud investigation. Create apprenticeship and secondment programmes that build practical experience. Convene workshops where accountants, auditors, risk managers, and cybersecurity professionals learn each other's languages. Build repositories of case studies, typologies, and lessons learned that survive beyond individual practitioners.

Geopolitics as fraud's operating system

A perspective from **Dr Roger Miles**, behavioural risk specialist and member of ACCA's combatting fraud special interest group

This research has shown we're witnessing something unprecedented: the foundation of business trust – the assumption that most people follow the rules – is eroding at an alarming rate. This isn't just about individual fraudsters or rogue organisations. It's about the geopolitical architecture that either enables or constrains fraud, becoming fundamentally unstable.

The 65% threshold: a fragile social contract

My research with the Dutch Justice Ministry (Justitie) and subsequent work across financial institutions points to a critical tipping point: societies and organisations need approximately 65% of their population to spontaneously comply with rules for the system to function.[3] This isn't about enforcement – it's about an intuitive respect for legitimacy. When that baseline drops toward 50%, we enter dangerous territory where 'most people don't care either way' becomes the prevailing sentiment, and deviant behaviour legitimised.

We're seeing this threshold tested globally. In jurisdictions where the rule of law has become inconsistently applied, the question isn't whether fraud will flourish, but how brazenly it will operate and whether professional standards can be maintained.

Legitimacy erosion and the fraud ecosystem

The gap between what rules say and what actually happens has always existed. But something has shifted. We're moving from wilful blindness – where people look away from infractions – to something more corrosive: structural normalisation. When institutional accountability mechanisms weaken across multiple jurisdictions, it sends a signal cascading through every organisation operating within those spheres: reputation risk carries reduced weight, rules become negotiable, and consequences become optional.

This pattern appears across diverse contexts. Where verification systems are under-resourced – whether through design or neglect – manufactured ignorance becomes possible. When company registration processes prioritise volume metrics over verification, they create perverse incentive structures that enable rather than prevent money laundering and fraud.

The organised crime calculus

A troubling insight from criminology: sophisticated organised criminals understand that they can only operate successfully when legitimate business is flourishing. They're parasites on a functioning host. The criminal ecosystem traditionally self-regulated to stay 'just below the radar' – pushing systems as hard as possible without destabilising them entirely. Complete collapse would eliminate their operating environment, so they maintain a careful balance.

But we're approaching a point where that balance may no longer hold. When AI-enabled fraud requires minimal investment, offers massive returns, and operates frictionlessly across borders, the traditional constraints evaporate. A distributed attack infrastructure has no supply chain to disrupt, no physical evidence trail, no opportunity cost to failed attempts. It's venture capital logic applied to crime: a 0.1% success rate still generates astronomical returns.

Jurisdictional arbitrage and the compliance reality

The uncomfortable truth from my conversations with accountants globally: in many jurisdictions, fraud isn't investigated because authorities lack resources, mandate, or institutional capacity. This creates what I call 'compliance deserts' – jurisdictions where formal rules exist on paper, but enforcement has become performative rather than substantive.

3 Diane Vaughan (1996): 'Risk, Work Group Culture, and the Normalization of Deviance', in *The Challenger Launch Decision*, chapter 3; Roger Miles (2017): 'The roots of misconduct: Why don't people behave even worse?' in *Conduct Risk Management*, chapter 5.

Geopolitics as fraud's operating system

Transparency International's Corruption Perceptions Index reveals this starkly.[4] As you slide down that scale, professional bodies face an impossible question: to what extent should we operate in jurisdictions where our ethical standards fundamentally clash with local institutional reality? Where signing off on accounts might implicate practitioners in systemic governance failures?

This isn't about judging individual jurisdictions. It's about recognising that fraud doesn't respect borders, and professional liability increasingly hinges on understanding where verification infrastructure remains robust enough to support assurance.

The manufactured legitimacy crisis

What alarms me most is the deliberate erosion of what we might call 'truth infrastructure'. When clock towers across a country are synchronised, it signals something profound about social coordination and shared reality. When they all tell different times, it signals fragmentation. AI hasn't just blurred the line between truth and fiction – it's obliterated the infrastructure we used to rely on for verification.

This compounds across contexts. In environments where digital authenticity has become contested – where deepfakes, manufactured documents, and information warfare are tools that sophisticated actors deploy – how does an auditor verify anything? We need not just new technical tools but a fundamental reimagining of what 'standard of proof' means when any artefact can be convincingly fabricated.

The professional response

The question isn't whether we've reached the end of the trust-based economy. The question is whether we can rebuild that trust intentionally, rather than watching it collapse and scrambling to respond. This requires something unfashionable: moral courage at institutional scale.

'Professional bodies, firms, and practitioners need to establish clear boundaries about which jurisdictions, clients, and practices remain compatible with professional integrity. This isn't about jurisdictional superiority – it's about honest assessment of whether verification infrastructure exists to support professional assurance.'

Industry cannot wait for coordinated international responses that may never arrive. The alternative – accepting a reality where rules exist only as aspirational statements while practice diverges fundamentally – serves no one's long-term interests, including sophisticated criminals who ultimately need functioning systems to exploit.

The path forward

We stand at a critical juncture. The patterns described here aren't inevitable – they're the result of choices about enforcement priorities, resource allocation, and tolerance for institutional drift. Recognising these patterns is the first step toward rebuilding verification frameworks that can withstand determined attack.

Professional standards bodies should:

- Establish clear criteria for jurisdictional risk assessment that includes institutional capacity, not just legal frameworks
- Develop shared intelligence on where verification infrastructure has degraded beyond professional tolerance
- Create escalation protocols for when practitioners face impossible conflicts between local reality and professional standards
- Build collective capacity to say certain contexts are simply incompatible with assurance, regardless of client pressure

As ACCA's research shows, fraud has changed fundamentally. Our response must match that scale – not with apocalyptic warnings, but with clear-eyed assessment of where trust infrastructure remains viable, and honest acknowledgment of where it has failed. That clarity serves everyone except those who profit from confusion.

4 Transparency International's Corruption Perception Index methodology is here: <https://www.transparency.org/en/news/how-cpi-scores-are-calculated?utm_source=chatgpt.com>