# Combatting fraud in a perfect storm.

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

# About ACCA.

**We are ACCA (the Association of Chartered Certified Accountants), a globally recognised professional accountancy body providing qualifications and advancing standards in accountancy worldwide.**

Founded in 1904 to widen access to the accountancy profession, we've long championed inclusion and today proudly support a diverse community of over **252,500** members and **526,000** future members in **180** countries.

Our forward-looking qualifications, continuous learning and insights are respected and valued by employers in every sector. They equip individuals with the business and finance expertise and ethical judgment to create, protect, and report the sustainable value delivered by organisations and economies.

Guided by our purpose and values, our vision is to develop the accountancy profession the world needs. Partnering with policymakers, standard setters, the donor community, educators and other accountancy bodies, we're strengthening and building a profession that drives a sustainable future for all.

Find out more at **accaglobal.com**

# About this report.

**Fraud is no longer a technical glitch – it's a systemic risk that undermines trust, governance and value. This report responds to that reality with insights drawn from a global survey of 2,044 professionals across finance, audit, risk, cybersecurity, compliance and investigations.**

To deepen the analysis, we convened 31 regional roundtables and over 30 interviews, engaging more than 250 experts between March and September 2025. These conversations explored where fraud thrives – accountability gaps, governance failures, cultural enablers and the limits of traditional risk assessments.

What makes this report different? It reflects an unprecedented coalition of professional bodies and the formation of a Special Interest Group of experts from our networks. This group shaped the research and practical outputs, including two companion pieces: *Calls to Action*, translating findings into governance steps, and *Thematic Typology*, bringing real-world experiences to life. Together, they aim to move fraud prevention from compliance theatre to operational reality.

# Foreword.

**Helen Brand OBE**
chief executive, ACCA

**Fraud is one of the most pervasive and destructive forces in today's economy. It is not a victimless crime – every fraudulent transaction leaves a trail of harm to people, businesses, and society at large. The losses are staggering: ACFE estimates suggest organisations lose more than 5% of revenue annually to fraud, amounting to trillions of dollars globally.**

According to the Global Anti-Scam Alliance, scammers stole over US$1tn in 2024, while cybercrime costs alone were predicted to rise to and US$10.5tn by the end of 2025, equivalent to the world's third-largest economy if measured by gross domestic product (GDP).[1]

Beyond the financial devastation, fraud acts as a silent killer of trust and organisational value. It erodes confidence in markets, undermines governance, and diverts resources from productive investment to criminal networks that fuel organised crime, corruption and exploitation. This urgency is reinforced by the UK's Economic Crime and Corporate Transparency Act (ECCTA) and similar global regulatory momentum.

At ACCA, we have long recognised that fraud transcends compliance or technical challenges – it represents a cultural and systemic risk that thrives in complexity and complacency. Through our *Risk Culture* series, we have observed how organisations treat fraud risk assessments as tick-box exercises, disconnected from real behaviours and decision-making. We knew we needed to confront this reality, but not in isolation.

We therefore convened a unique global coalition of professional bodies spanning internal audit, cybersecurity, fraud examination, risk management, financial planning and corporate investigations. This global initiative explores what's working, what's failing, and where critical gaps exist. The findings serve as a serious wake-up call: while 62% of respondents agree that fraud awareness training is important, only 57% believe their organisation proactively looks for fraud. Many functions engage only after fraud is exposed. Too few eyes actively seek it beforehand. Prevention remains the 'black hole' our roundtables identified.

The implications are clear: sophisticated modern fraud amplified by new and advancing technologies, economic pressures and shifting geopolitical dynamics cannot be countered by any single profession or jurisdiction. We must embed proactive detection into business operations, strengthen governance and accountability, and foster cultures in which raising concerns becomes safe and expected. Most critically, we must act collectively.

This report serves as both a call to action and a practical guide, reflecting ACCA's commitment to leading with integrity, collaborating across disciplines and equipping our respective members with insights needed to protect organisations, economies and the public interest. Combatting fraud is not optional – it is essential to the trust on which our profession, and society, depends.

1 Global Anti-Scam Alliance (2024) – *Global Anti-Scam Alliance Report,* <https://www.gasa.org/> (page 3).

# Contents.


# 1. The wake-up call our professions cannot ignore

## A perfect storm intensifies

This summary distils the key findings from our global research into what's changed, what's broken, and what's needed to combat fraud in today's environment. From cyber-enabled crimes, AI-driven deception and crypto-related schemes to increasingly pervasive procurement fraud and behavioural schemes such as investment and romance scams, today's threats interact across systems and value chains, creating blind spots that traditional controls fail to address.

Fraud has evolved from isolated incidents to widespread deception that mutates faster than risk registers can capture. We show how the convergence of Web 3.0, accelerating AI and sophisticated global crime networks creates threats that outpace most organisations' ability to respond.

**'Cyber-enabled frauds exploit human errors, deepfakes bypass controls, third-party frauds tear through supply chains and corruption undermines entire markets.'**

Experts consulted in ACCA's earlier work warned we were only scratching the surface of how AI and data analytics could help prevent and detect fraud as digitalisation accelerated.[2]

Cybercrime has become an economy in its own right and is no longer a technology issue; It has become a macro risk that amplifies every other fraud type.[3] The same technologies that scale legitimate business now scale deception, and the same supply chains that create value now transmit loss.

Three forces define today's converging threats:

- Cyber-enabled attack surfaces across payments, identity and data
- Mounting cost pressures normalising shortcuts
- AI collapsing time and amplifying deception.

*'It's time for a collective reset,'* says Dr Roger Miles, a behavioural scientist, former auditor and member of our special interest group.

**'AI is destroying the barrier between truth and fiction and the implication for finance, audit and risk professionals is profound. We've reached a watershed moment where we've got to deeply question the truth of the bookkeeping in front of us.'**

Dr Roger Miles, behavioural scientist and former auditor

## Fraud at scale

Organisations now face well-financed, networked groups operating across borders using the same digital infrastructure that legitimate businesses depend on. Fraud money fuels crime – from terrorism to trafficking – and through our discussions with respective members we can see that state-level fraud remains another harsh reality.

**'Today's fraud is organised crime. And let's face it, it's a lucrative business.'**

UK non-executive director (NED)

The multinational reality of fraud also compounds today's challenges. As another participant in Australia noted: *'We're not living in a global world anymore – we're multinational. Businesses will have to operate multi-nationally, and that's a huge mindset change.'* Fraud exploits jurisdictional seams: whistleblowing frameworks effective in one country could fail in another, not because people care less, but because differing legal frameworks create contradictions and complexity due to inconsistent standards, differing jurisdictional claims, and challenges in applying rules across national borders. Participants also talked about tension when fraud laws and whistleblowing policies clash in practice, particularly regarding corporate responsibility and whistleblower protection.

Regional and national cultural factors create deep fissures. In parts of Asia-Pacific, *'They [the bosses] are very wary of talking about fraud. It's taboo – if you talk about fraud, it's like you are teaching people how to commit it,'* as an internal audit head in Singapore explained.

Meanwhile, in emerging European markets, major shareholders use AGMs to remove directors who ask inconvenient questions. No organisation is immune: fraud doesn't respect borders, and indirect exposure through supply chains means a small to medium-sized enterprise (SME) in a small town faces the same cyber-enabled threats as a global bank on Wall Street.

## The accountability vacuum

These threats are deepened by governance gaps that leave fraud unowned and undetected. Our survey shows how fraud as everyone's issue easily becomes nobody's job – across all functions, there's a gap between current and desired responsibility for anti-fraud. The largest gap is for dedicated anti-fraud units, which many believe should exist but often don't.

**'We have all these different professionals dancing around fraud once it's revealed, but nobody is actually proactively looking for it.'**

Special interest group member

*'Fraud losses are rising four digits, not double, when you factor in direct losses, downtime, brand damage and insurance payouts. It destructs value, though leaders still treat it as a technical issue,'* a European respondent noted.

While our coalition survey analysed fraud perceptions by function, we found that the language of 'functions' can reinforce silos. Roundtables revealed that reframing fraud prevention as a team responsibility

2 ACCA (2020) – *Economic Crime in a Digital Age*.

3 Cybersecurity Ventures – *Cyberwarfare Report*.

– rather than a departmental task – helps change behaviour. When organisations talk about 'cross-functional teams' instead of 'functions', collaboration rises and blind spots shrink. This shift matters because fraud exploits seams between roles; resilience depends on closing those seams through shared accountability.

**'Fraud is no longer a technical issue — it is a systemic risk that demands cross-functional leadership.'**

As a European financial director noted: *'The finance team should be the bridge between IT, compliance and the board because we see all the moving parts.'* Yet another chief financial officer (CFO) in the UK added: *'If we don't do the checks, then everyone asks, "where were the accountants?" We need to stop receiving information and just go out and get it.'*

## Prevalence vs impact

The fraud landscape revealed by our research is not simply a catalogue of schemes. It is a dynamic picture shaped by how often frauds occur, how deeply they hurt and how differently they are perceived by various stakeholders. When viewed through this multi-layered lens, the landscape becomes both more fragmented and interconnected than traditional typologies suggest.

We provide a new axis – prevalence versus materiality – to help our professions avoid simplistic assumptions. Cyber and procurement frauds dominate prevalence rankings, though cyber consistently rates as far more material due to its unpredictable, catastrophic potential.

Through this axis we see how fraud manifests differently across regions and sectors: financial services worry about cyber-enabled identity theft from internal and external threats; healthcare flags procurement fraud affecting patient safety; extractives face bribery and corruption in unstable regions; and professional services prioritise conflicts of interest. These are all amplified by a mix of risks that cannot constitute a single fraud 'landscape', so organisations must navigate sector-specific terrains shaped by multiple pressures and idiosyncratic vulnerabilities.

## Understanding drivers

While 'new technologies outpacing controls' and 'economic stress' lead globally as the top drivers of fraud, 'lack of ethical leadership' becomes the biggest fraud driver in multiple high-risk contexts, making 'tone at the top' the decisive cultural amplifier.

The roundtable discussions also revealed a growing 'disgruntled employee' concern, reflecting the cost-of-living crisis and wider lack of trust.

While fraud risk assessments (FRAs) exist almost everywhere, roundtable discussions show that maturity is not only rare but fundamentally misunderstood. Only integrated, regularly updated FRAs correlate with higher confidence and resilience; static templates deliver comfort, not outcomes. Our regression analysis also shows that organisations that act on FRAs recognise procurement fraud as systemic, while those that do not under-recognise it. Crucially, our survey data proves that you only see what you're trained to look for.

### Top fraud prevalence versus materiality matrix

| FRAUD TYPE | PREVALENCE | MATERIALITY | SECTORAL IMPACT | NOTES |
|---|---|---|---|---|
| Procurement Fraud | High | Medium | Public Sector, FS | Often dismissed as leakage |
| Cyberfraud | Medium | High | FS, Cross-sector | Catastrophic when it lands |
| Authority Abuse | High | Underestimated | Public Sector | Invisible conductor of other frauds |
| Financial Statement Fraud | Medium | High | FS, Large Corporates | Often board-level blind spot |
| Crypto Fraud | Emerging | High | FS, Tech, Global | Low referral rates, cross-border opacity |
| ESG Misrepresentation | Low | Rising | Western Europe, Asia | Silent but serious reputational risk |
| Third-Party Collusion | Medium | High | All sectors | Low visibility, high impact |

## Four distinct perspectives emerge

Traditional approaches treat fraud as purely technical – a matter of controls and compliance.

Our cluster analysis reveals four distinct organisational mindsets – Realists, Cynics, Optimists and Observers – each shaping how fraud is perceived and prioritised.

### Personas Summary

| PERSONA | VIEW ON FRAUD | RISK TO ORGANISATION |
|---|---|---|
| **Overloaded realists** | See fraud everywhere, feel under-resourced | High alert, low action |
| **Cynical insiders** | Distrust leadership, assume compromise | Rationalise misconduct |
| **Optimistic practitioners** | Trust systems, downplay fraud | Vulnerable to systemic shocks |
| **Detached observers** | Think fraud is someone else's problem | Blind spots and disengagement |

Combining that data with our roundtables shows how these differences challenge any single organisational 'fraud narrative'. Low trust in leadership strongly correlates with higher acceptance of fraud rationalisations. People don't just rationalise fraud due to personal pressures. They rationalise it because they believe their leaders do too.

## Professional perspectives, fragmented responses

Detection is rising, but triage is failing. Organisations generate more fraud alerts than they can process, and confidence that reports lead to action is eroding – fuelling the cynicism that drives misconduct. Our coalition approach uncovered tensions – hidden in typical surveys – that help us understand the different perceptions:

- Auditors stress independence gaps
- Cyber professionals focus on structural vulnerabilities
- Risk managers warn of cultural blind spots
- Accountants grapple with cost pressures and role clarity.

The disconnect extends to execution: *'We have skilled people, we have knowledge,'* a Polish board member noted, *'but the system doesn't protect people who ask questions. It pushes into boards people who just say yes.'* This pattern repeats across jurisdictions – qualified professionals sidelined because challenge is unwelcome.

**'One thing we have learned is that fraud brings out seriously deep cultural issues that other risks really cannot do.'**

Canadian participant

## From afterthought to foresight

What most leaders underestimate is not the list of fraud types but the gaps that let them persist. Our survey shows boards believe they should own oversight, yet practical ownership is pushed down to functions without mandate; reporting feels easier on paper than in practice; and fraud risk assessments exist as documents rather than operating systems. Indeed, just over half of ACCA respondents (51%) believe their organisation actively looks for fraud, compared with 57% overall. Those gaps are why 'common' risks like procurement erode resources steadily while 'lower frequency' risks like cyber can prove existential.

The fundamental reframing needed starts with encouraging willingness to speak up because people feel safe and trust their leaders. Organisations that embed proactive fraud prevention and clear accountability frameworks often reap wider risk governance benefits: sharper decision-making, more resilient operations and integrity cultures driving long-term value.

The voices from our coalition show how organisations can move beyond technical compliance and embrace a new era of professional scepticism and behavioural insights – where asking not just more questions, but the right ones, is as critical as finding the right answers. Across all seven professional bodies, behavioural risk management was highlighted as an underused tool – by measuring trust in leadership, tolerance of misconduct and rationalisation tendencies, organisations can identify vulnerabilities before they crystallise into successful acts of fraud.

**'We are good at autopsies and countering fraud after it happens. We are terrible at spotting it before. Behavioural metrics can give us a chance.'**

European risk executive

# Two key messages for leaders:

## Prevention is credibility

It is the willingness to see what you would rather not, and to publish evidence that reporting leads to change. Alex Rothwell, chief executive officer (CEO) of the UK's NHS Counter Fraud Authority states it clearly in an episode of ACCA's risk culture podcast series, *Combatting Fraud in Healthcare*:

**'One of our founding principles is accepting that fraud exists. It's one of the first cultural hurdles that we face as fraud professionals. If you're a finance director, part of your responsibility is to put in place measures to address and mitigate fraud. If fraud is found, it's seen as a failure of control, but it should also promote the concept that fraud exists … because in our experience if you don't look for fraud, it's unlikely you're going to find it until it hits hard.'**

Alex Rothwell, CEO, NHS Counter Fraud Authority, UK

## Maturity is cadence

Monthly residual-risk notes, service levels for decisions and behavioural instrumentation around the controls people actually override. Organisations that practise both do not claim to eliminate fraud; they become hard targets and trustworthy stewards of other people's money.

Boards, policymakers, law enforcement, investors, lenders, educators and professional bodies must treat fraud as a systemic risk – because the storm is only intensifying.

**'You're never going to completely rid the risk because fraudsters are too quick and clever but if we all do our jobs properly and diligently, we will at least reduce it – and probably take ourselves out of the line of sight of the fraudsters because they'll go, *"They're asking too many questions"*.'**

Claire Jenkins, senior policy advisor, Companies House, UK

## What 'systemic fraud' means

**Throughout our research 'systemic' was used frequently to describe fraud risk.**

This is fraud that is not isolated or opportunistic, but embedded in the structures, processes, or culture of an organisation or system, making it harder to detect and more damaging. It often involves:

- Organisational-level compromise: Entire governance or control frameworks can be undermined.
- Cultural enablers: Incentive structures, fear of retaliation, and siloed risk models that allow misconduct to persist.
- Interconnected vulnerabilities: Fraud risk amplified by weak oversight, opaque decision-making, and fragmented accountability.
- Persistence and scale: Unlike one-off incidents, systemic fraud can replicate across units or markets because it's rooted in norms and processes.

As one investigator put it:

**'Fraud has shifted from opportunistic to systematic, where entire organisations can be compromised. Addressing this requires resilience-based thinking that integrates fraud prevention into business decisions.'**

# 2. The interconnectedness and industrialisation of modern fraud

**Today's fraud threats blur the lines between corporate misconduct, organised crime and societal breakdown. Their interconnectedness and scale amplify systemic risk across value chains.**

## Prevalent and pervasive

Fraud is no longer a set of incidents. It exploits shared infrastructure across payments, identity platforms and data ecosystems. These interconnected systems mean a single breach can cascade across multiple entities.

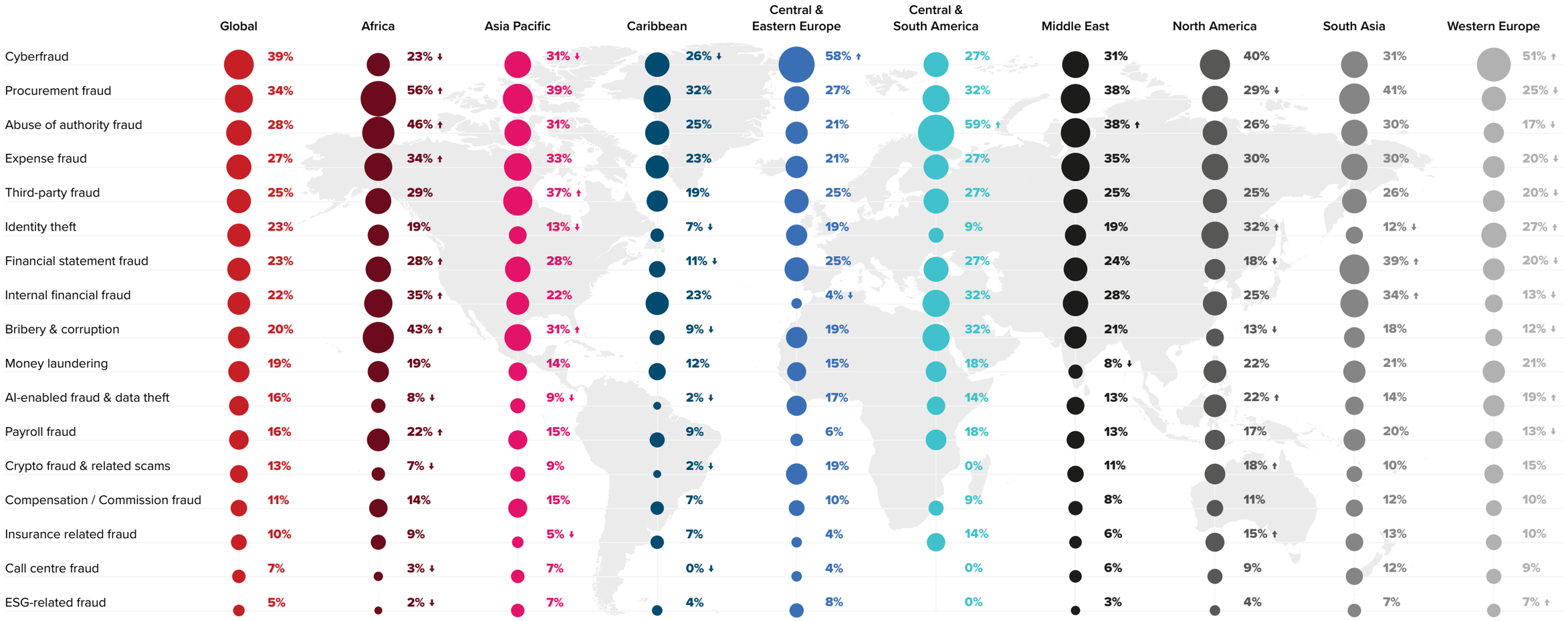
As Figures 2.1, 2.2 and 2.3 show, cyberfraud was the most consistently identified inevitable risk in survey responses and roundtables. What distinguishes today's wave is not novelty but scale and coupling. When operations depend on identity platforms, cloud workflows and outsourced providers, a single breach propagates beyond the entity. A ransomware campaign can shutdown hospitals, airports, power grids, supply chains, and financial systems.

**'We no longer see cyberfraud as isolated. It's infrastructure-level. If payments are paralysed, that is not just a fraud issue, it's a national security issue.'**

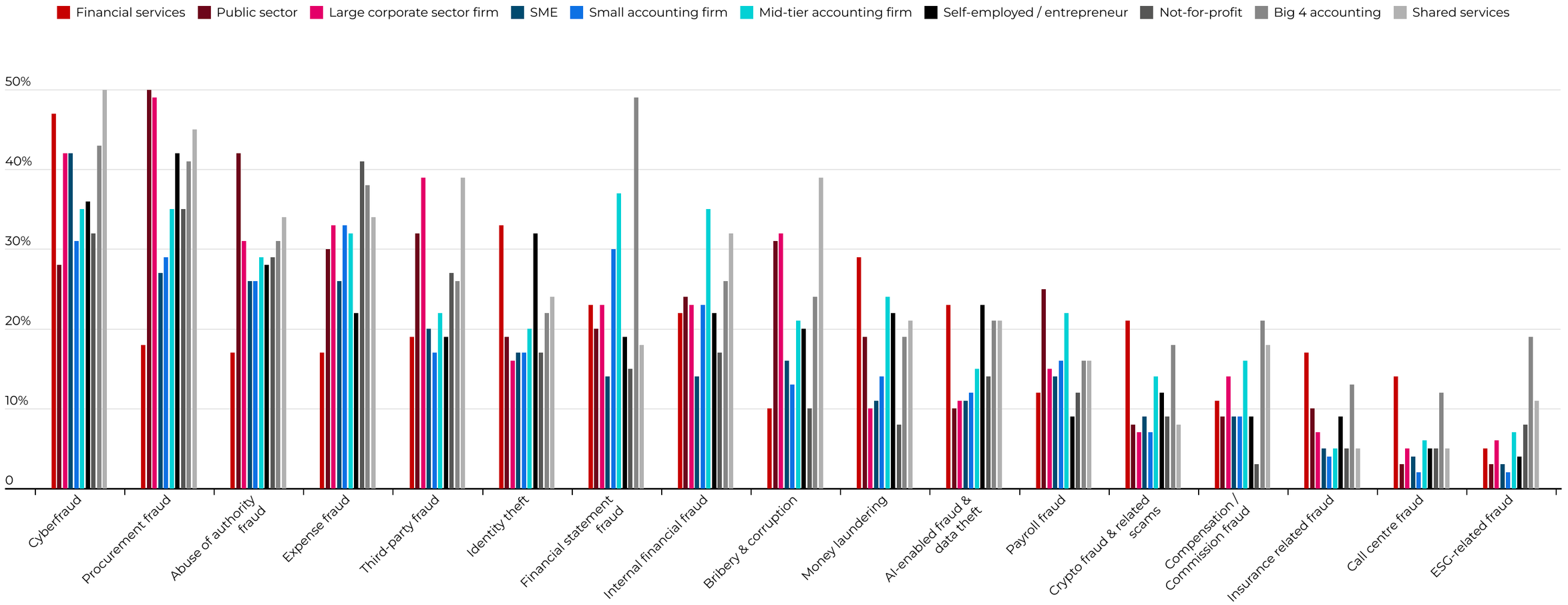
US participant from financial services

*'Now they pull you in. You press 1, then you're talking to a 'FedEx agent'... it's professionally done,'* another respondent from an India-based conglomerate added.

## Figure 2.1 **Cyberfraud dominates globally, while procurement fraud remains underestimated despite high prevalence**

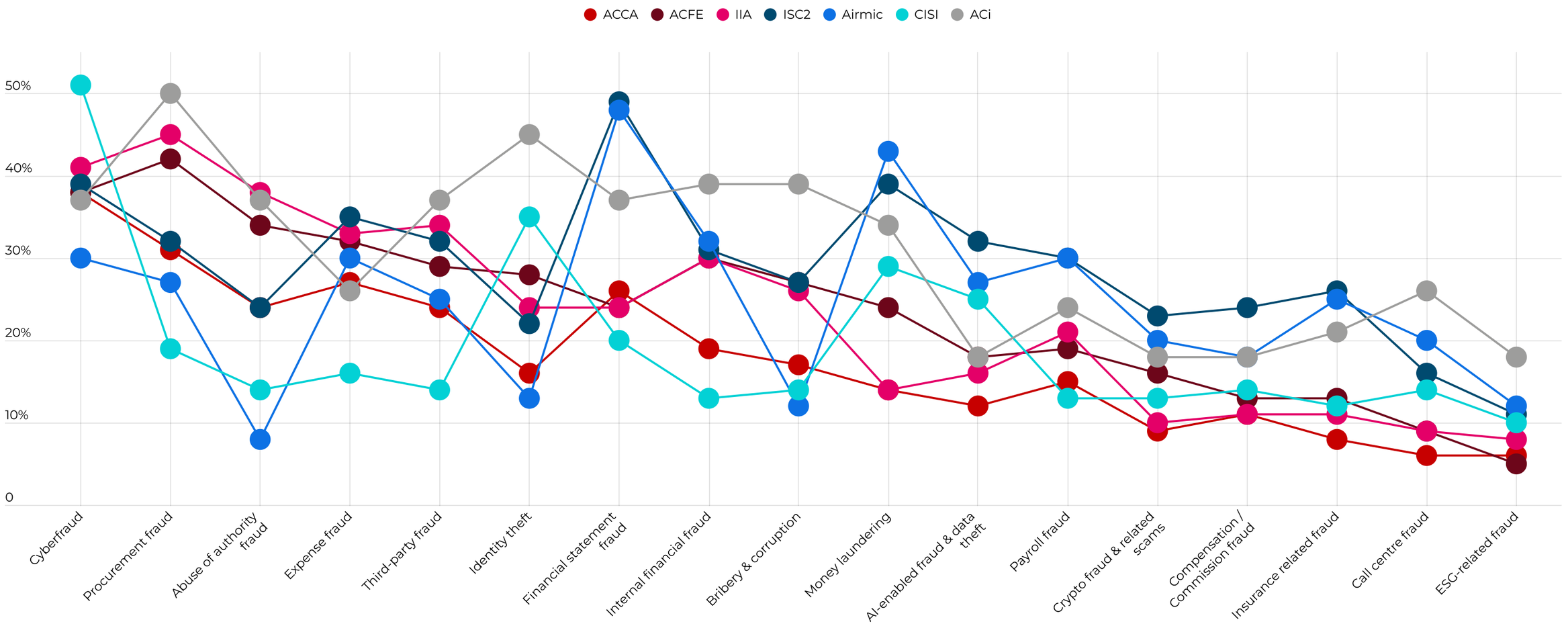


## Figure 2.2 **Fraud prevalence varies sharply by sector: financial services face cyber risk, public sector struggles with procurement fraud**




**Note:** For professional services, 'prevalence' reflects incidents seen across client portfolios, not solely within the firm.

Figure 2.3 **Professional perspectives diverge: cyber risk tops for tech-focused roles, while auditors and investigators spotlight internal and authority-linked fraud**



Furthermore, our regression analysis of the prevalence scores showed a strong link: respondents who rated cyberfraud as highly material were also the most likely to report unclear accountability structures. This suggests that cyberfraud does not simply test technical controls; it exposes gaps in culture, governance and board-level oversight. Threat actors prey on every weakness, not just directly but often through 'back doors' in the supply and value chains.

Regional patterns reveal the scope. In Europe, especially the UK, ransomware attacks are driving cyber insurance premiums to record highs, paralysing supply chains and making cyberfraud a wider resilience issue rather than a narrow IT concern. In the Asia-Pacific, digital payments and super-apps were labelled both *'transformative and vulnerable'*. In Africa, where mobile banking is leapfrogging older infrastructure, members warned of *'first-mover vulnerabilities'* being ruthlessly exploited

**'You need to run frequent vulnerability tests and independent audits or else you're going to be wiped out because you could be sitting on a system while a fraudster is already inside.'**

Ugandan risk manager in financial services

**'Banks run mobile banking, telecoms own the phones, government issues the numbers, and vendors provide systems. They need to work together to close vulnerabilities.'**

Participant in Nigeria

Interestingly, Chinese mainland respondents ranked cyberfraud significantly lower on both prevalence and materiality. Engagements with members suggest this reflects strong state-driven cybersecurity mandates and centralised payment ecosystems, which reduce perceived exposure – though experts across the coalition warned this confidence may mask emerging risks in decentralised finance and AI-enabled deception.

## AI in the fraud arms race – threat and shield

**AI has become the ultimate accelerant in the fraud economy. What once required weeks of planning and specialist skills can now be executed in hours with off-the-shelf AI tools.**

Attackers are using voice and video synthesis, cloned correspondence and hyper-personalised lures to speed deception at a scale and precision never seen before. A Singapore-based chief risk officer (CRO) warned: *'What used to take a fraud ring weeks can now be done in minutes – and it feels personal because it is data-driven.'*

Another participant described a case where a voice-cloned CEO authorised a multimillion-pound transfer during a live call. *'We've seen AI make old scams frighteningly convincing,'* another CRO in Europe added. These tools are not just mimicking voices – they are generating entire identities, complete with synthetic documents and social media footprints, at industrial scale.

On the defensive side, a European auditor explained how anomaly detection had flagged collusion patterns in procurement data more efficiently than humanly possible. In contrast, we found several participants already using AI defensively. A participant from India described AI-driven behavioural analytics as a 'new smoke alarm', sensitive to early warning signs before losses occur.

Yet this transformation comes with caveats. AI is only as good as the governance around it. Without strong oversight, models can hallucinate, embed bias or expose sensitive data. As another CRO in the UK put it, *'AI will amplify whatever culture you have – good or bad.'* The challenge is ensuring that the speed of AI does not outstrip the ethics and controls that keep it in check.

## The grey frontiers

Crypto-assets and stablecoins sit in the grey zone between innovation and opacity. Respondents did not rank them the most prevalent, yet discussions repeatedly linked them to money laundering and organised crime. Several respondents also urged professional bodies to equip accountants and auditors, especially, with guidance on testing crypto-related exposures, warning that without this assurance becomes superficial.

**'Crypto is where fraud and organised crime meet. It's fast, opaque, and cross-border – and regulators are permanently playing catch-up.'**

Middle Eastern compliance officer

**'Lack of basic infrastructure and security in the Web 3.0 space creates significant gaps that fraudsters exploit.'**

Hong Kong fintech participant

Respondents also highlighted the need to treat onboarding and continuous monitoring of third-parties, beneficial ownership changes, and payment instruction changes as fraud controls, not mere paperwork. Organisations that have embedded these checks disrupted loss chains even when incidents originated outside their walls.

## Greenwashing and misallocation

While environmental, social and governance (ESG)-related misrepresentation ranked lower in prevalence, roundtables – mainly in Western Europe and South East Asia – emphasised it as silent and consequential. Misreporting carbon emissions, misuse of sustainability-linked financing and greenwashing claims were all cited.

**'Fraud is not just about stealing money. When companies lie about ESG, they defraud society and misallocate capital. The planet pays the bill.'**

UK contributor

*'Even if it wasn't intentional, we're back to controls again. Who signed it off? Why did someone think that was OK?,'* a risk and compliance lead in Europe professional stressed.

In Africa and Asia-Pacific, respondents linked ESG fraud with procurement fraud, describing cases where sustainability budgets were siphoned off through corrupt contracting. In Western nations, executives worried that political backlash against ESG could create a climate where misreporting thrives in the absence of strong standards.

**'You could also question whether procurement fraud risk is just bad procurement and contract management.'**

Middle Eastern respondent

Whether labelled fraud or not, the market effect is the same: capital misallocation equals reputational damage. The consensus was clear: the right response is parity of assurance – treat key non-financial claims with the same scepticism, sampling discipline and escalation you apply to financial statements. If investors lose faith in ESG reporting, capital may retreat entirely from sustainable projects. This makes the fight against ESG fraud integral to modern-day good governance.

## The convergence effect

Roundtable participants around the world described the same choreography: social engineering primes the request, a compromised credential opens a door, weak supplier hygiene completes the loop and crypto or fast-moving money rails clean the exit. Fraud networks exploit technology, regulatory arbitrage and geopolitical instability to scale operations.

**'Fraud is not a victimless crime. In our context, it pays for guns. It pays for trafficking. It drains our people's livelihoods, their communities.'**

African risk manager working at a non-governmental organisation (NGO)

This convergence of fraud, money laundering and illicit trade turns industrialised fraud into a societal issue. As another European risk manager observed: *'When fraudsters hack your systems or manipulate procurement, it's not just a nuisance, it's part of a global criminal economy.'*

Financial services respondents worldwide also noted a dramatic surge in investment scams driven by highly organised crime gangs deploying sophisticated tactics that fool even experienced investors.

*'The big increase for us and the one we're really nervous about today is investment scams and complex, authorised fraud. Something new is happening and it appears to be properly linked to organised overseas crime gangs. The terrifying thing is just how sophisticated they are. The paperwork that comes back looks so legit,'* a UK retail bank compliance lead commented.

**'The key message from these discussions was that the convergence effect is not only criminal – it's also organisational. Every time our professions work in silos, fraud networks gain another advantage.'**

## The interconnected storm

Fraud is no longer a collection of separate risks, but an interconnected storm system. Cyber tools amplify all fraud types, AI democratises sophisticated attacks, and organised crime networks exploit weaknesses across crypto, ESG and traditional fraud vectors. Our pressions must work together to choose which fraud types to prioritise and build defences against their convergence.

Our research reveals how these interconnected risks propagate through value chains, where a single weak link – whether a supplier, payment processor or identity platform – can trigger cascading failures across multiple entities. Fraud is no longer single entity bound.

### Policy to playbook

**Essential changes are needed:**

- Quarterly fraud dashboards to the audit committee
- Team fraud-risk champions
- Fraud checks before high-value approvals.

**'Interconnected fraud calls for ecosystem governance, shared intelligence, joint reviews and consistent cadence between cyber, finance and operations.'**

Asim Ali Abid, member of both ACCA and IIA, working in the oil and gas sector

Across sectors, we found the interconnected storm could come down to three main areas of discipline:

- **Plan for the blast radius, not just incident response.** Assume systems will be hacked and use ghost-hacker simulations to test resilience across dependent providers.
- **Move from 'trust, then verify' to 'verify, then trust'.** Build this into all decision-making: before acting, always check beneficiary banking details, vendor onboarding and authority to spend through independent channels.
- **Combine fraud, cybercrime, procurement and finance data** so patterns converge in your systems before they converge against you.

### Key takeaways

**Is your organisation treating fraud as interconnected systems or isolated incidents?**

Map how a cyber breach could simultaneously compromise procurement approvals, payroll identity verification, and ESG reporting systems. Audit whether governance structures can respond to convergent threats, assess if teams have the technological literacy to detect sophisticated attacks and leverage predictive analytics, and examine whether behavioural risk indicators can flag cultural vulnerabilities before they become material losses. The fundamental question is whether you're building defences that recognise how fraud exploits shared infrastructure across value chains.

# Financial services – a sector under siege

**Despite heavy investment in controls, financial services faces unique vulnerabilities: valuation fraud driven by incentive structures, ransomware shocks that paralyse operations and the 'specialisation trap' where fraud thinking is outsourced, leaving blind spots in everyday decisions.**

## Cyberfraud dominates materiality rankings

Ransomware can paralyse operations overnight; account takeovers trigger massive losses and data breaches unleash regulatory fines.

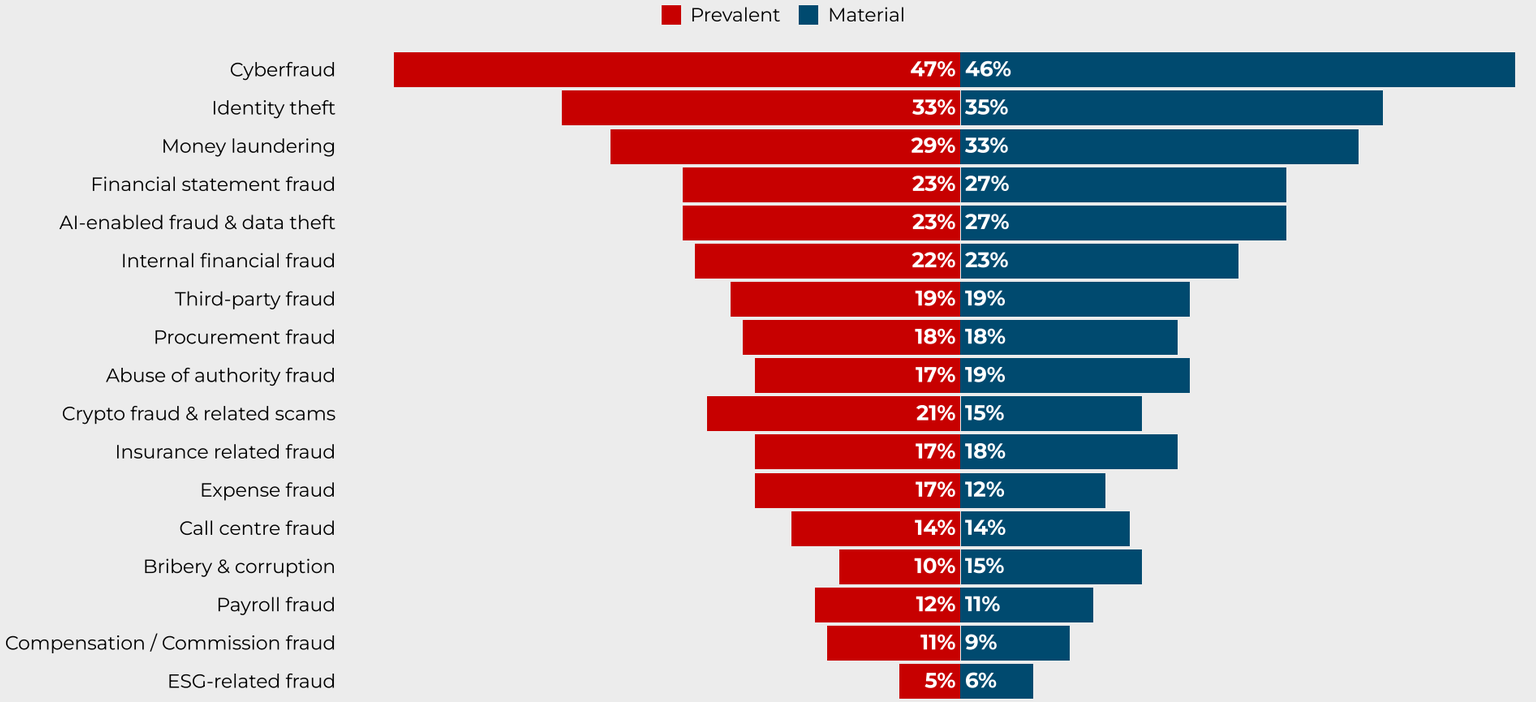
**'Cyberfraud is the only risk where I feel genuinely outpaced. Every time we adapt, the criminals adapt faster.'**

European banker respondent

Siloed recognition creates institutional blindness. Cyber incidents flow through IT departments, recorded in technical logs that finance teams rarely review, creating false comfort. As one US executive admitted: *'We're not focused on preventing fraud. We're focused on detecting it because we can't prevent it. What we try to do right is invest money where we can enhance our controls so that we detect it as quickly as possible.'*

Boards must reframe cyber risk from 'technology challenge' to 'fraud vector', embedding joint fraud-cyber capabilities and ensuring AI-enabled systems monitor payment flows, not just perimeter defences.

Figure 2.4 **Fraud prevalence vs materiality** (Financial services)



**Procurement and third-party frauds** represent perhaps the sector's most dangerous blind spot. Despite moderate prevalence, financial services' leaders consistently underestimate materiality – a misreading that enables sophisticated attacks. Cultural dismissals of 'it's operational, not strategic' persist until scandals explode.

**'We're still not allocating resources where they hit hardest because we don't fully understand the scale or sophistication.'**

Risk manager in the UK

**Valuation fraud and misstatement risk** emerged strongly from US and Australian respondents. Special Purpose Acquisition Companies (SPACs), private equity, and startup valuations were flagged as *'fabricated or inflated'*, driven by bonus-linked incentives and weak oversight. *'No one trusts what a valuation of a startup is in the US – that's all fabricated always,'* one participant stated bluntly. Another accountancy practitioner in the US added: *'I've walked away from SPAC deals because the inputs and outputs didn't reconcile – $2bn valuations that made no sense.'*

**Internal fraud** suffers from materiality myopia. Expense fraud and payroll manipulation score high on prevalence but low on materiality, dismissed as insignificant versus external cyber shocks.

**'We've actually seen an uptick in internal fraud. A recent interesting one was in payroll where they actually reduced the amount of federal withholdings across employees and then added it to their own.'**

US executive

The specialisation trap compounds the blindness:

**'In some ways, there's a downside to having fraud experts because the more centralised fraud becomes, the less focused individuals become.'**

Chief audit officer (CAO)

When organisations outsource fraud thinking to specialists, line managers often stop thinking defensively, creating exactly the vulnerabilities that internal fraudsters exploit.

**Emerging pressures:** Customer protection expectations are rising sharply: *'We expect the bank to protect your money and if they don't, you won't bank with them,'* an Australian banker commented. The complexity peaks among smaller entities – credit unions, fintechs and payment platforms – which face hybrid risk profiles. *'We're lucky in a way because we're a small community-based cooperative and therefore we do possibly know our members a lot more than [in] a ...retail banking environment'* a respondent from an Irish credit union added. This personal relationship advantage helps with detection but doesn't eliminate sophisticated external threats.

Regulatory and geopolitical changes were also mentioned:

**'We're starting to see an awful lot more sophisticated and technologically sophisticated phishing frauds. I wouldn't say that this is 100% related to geopolitical situations but that surely has a part to play.'**

Swiss insurance executive

A US bank internal audit head was more explicit, drawing from industry intelligence on state-sponsored fraud:

**'What's much scarier to me is how many countries pay people to break into systems and threaten them if they don't succeed.'**

US bank internal audit head

# Public sector blind spots

**Public sector organisations face their own debilitating disconnects between what they see most often and what hurts them most. Our analysis reveals how public bodies struggle with authority abuse as an invisible conductor of other frauds, chronic misclassification of cyber incidents and resource-starved local councils that turn prevention into a distant ideal.**

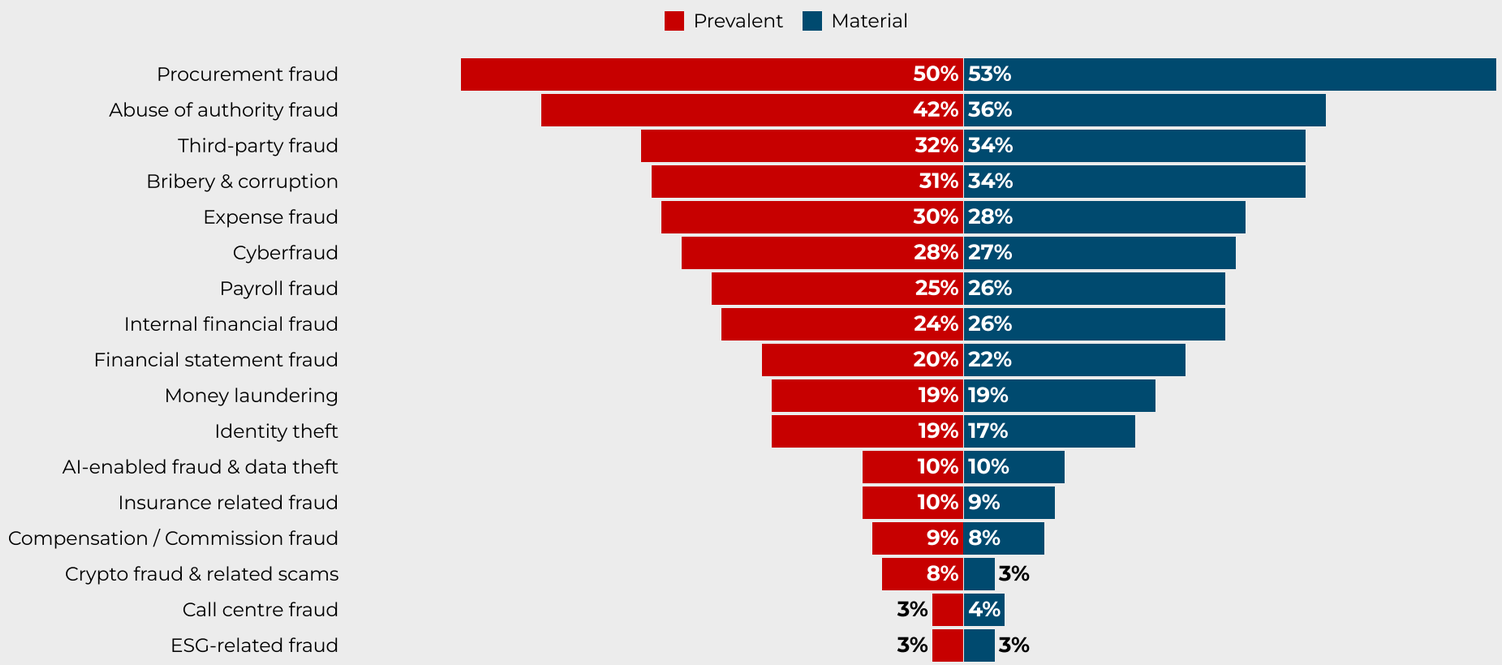
**Abuse of authority** ranks second in prevalence and while materially significant, its impact is often misattributed to downstream categories – procurement leakage, enabling payroll anomalies, and facilitating third-party collusion. This diffusion masks the root cause, so materiality appears elsewhere and the various drivers continue to persist unchecked.

**Cyberfraud** presents a different blind spot. It appears lower in public sector prevalence not because the risk is genuinely smaller, but due to chronic misclassification. Public bodies routinely triage cyber incidents to IT or security rather than fraud. Cyber is the vector that amplifies other frauds – procurement manipulation, benefits fraud, and vendor schemes.

**Procurement fraud** dominates prevalence statistics but remains underweighted on materiality – often dismissed as leakage rather than recognised as potentially catastrophic loss.

**Bribery and corruption** shows the reverse pattern: lower prevalence but dramatically higher materiality when incidents surface.

Figure 2.5 **Fraud prevalence vs materiality** (Public sector)



When leaders allocate resources based solely on frequency – or only on what feels immediately catastrophic – they systematically miss the underlying drivers that enable larger fraud ecosystems. Public bodies need measurement systems that track prevalence-materiality gaps and accumulated losses over time, not just incident counts.

## Local government disconnects

While more national governments increasingly prioritise fraud prevention, local authorities worldwide remain dangerously exposed. The UK illustrates the challenge – central government now operates AI-accelerated risk assessments, but local councils report being *'asked to own fraud without training or tools'*.[4]

UK councils still depend on biennial cross-entity data-sharing exercises – a frequency that costly cases have shown is far too low to catch ongoing procurement abuse or payroll manipulation in real time.

**'In councils, fraud is lumped into audit. Many auditors have never done a fraud risk assessment. We're in the 'Dark Ages' on fraud.'**

A respondent in England

Canadian municipalities describe similar patterns but appear to be making progress. Anonymous hotlines and clear consequence management are gradually changing mindsets. *'One case diverted over $500,000 – reported, investigated and referred to police,'* noted one participant.

Australian participants traced major losses to culture failures. Basic verification calls get skipped despite existing policies, while budget pressures starve back-office systems.

**'If you don't invest in the system, you teach people to bend the rules to get things done.'**

Australian participant

Local government casework shows control gaps can persist for years – for example, one individual holding multiple fulltime council roles undetected – move from biennial spot checks to quarterly payroll/vendor analytics and crossentity data-sharing.[5]

The common thread across jurisdictions: governance confusion (unclear ownership), data limitations (episodic rather than continuous monitoring) and consequence gaps (weak follow-through on detected fraud).

## Prevention as policy

The pandemic forced a reckoning. COVID-19 fraud losses – £10.5 billion in the UK alone – revealed that public bodies were better at counting losses than preventing them. The UK response embedded fraud into spending rules. Under 'Managing Public Money', major programmes must complete an Initial Fraud Impact Assessment before approval. This moved fraud risk from compliance footnote to design-stage question leaders cannot ignore.[6]

Transparency became the second lever. Departments must publish fraud loss estimates, audited by the National Audit Office (NAO). This reframes fraud from embarrassment to performance metric – one that ministers are held accountable for. As one contributor warned: *'No one's going to believe you on ROI* [return-on-investment] *unless you've got good data. Don't be a ghost hunter – be someone with actual evidence.'*

### Key takeaways

Prevention works when it is institutionalised, measured, and enforced. Other jurisdictions can adopt the same principles: mandate fraud impact assessments, publish loss estimates and track avoided costs. Local government delivers essential services directly to citizens, making fraud prevention both a financial and social imperative.

4 UK Cabinet Office (2025) – *Record fraud crackdown saves half a billion for public services*.

5 BBC News (2025) – *Council fraud prevention challenges*.

6 Public Sector Experts Blog (2025) – *Monitoring public sector funding*.

Voices from the coalition – ISC2

# Trust and transparency beyond the firewalls

**As ACCA's survey makes clear, cyber-enabled and technology-driven frauds are widely considered the most material risks. Deepfakes, synthetic identities, and AI-enabled deception are eroding trust and undermining the integrity of markets and institutions. This is the reality, and ISC2 members – especially chief information security officers (CISOs) – must be central to the response.**

The data shows ISC2 members stand out for their proactive stance. They are often more likely than their peers to seek out fraud, to value continuous training, and to recognise that technology-enabled risks are shaping the future of organisational resilience. This is a strength, but leadership today requires more than technical knowledge. Fraud is neither solely a technological problem, nor is it only a financial one. It is an enterprise-wise cultural challenge, and our members' expertise must be part of a wider fabric of collaboration – because collaboration is the only way forward.

Working alongside auditors, accountants, and risk managers in this research has highlighted powerful lessons for our community. First, our peers remind us of the value of shared accountability. Too often, responsibility for fraud is fragmented or only clarified after the fact. To close this gap, ISC2 members should push for joint fraud risk committees that bring together cybersecurity, finance, and audit leaders on a regular basis – not just in the aftermath of an incident. This is how accountability moves from the page to practice.

Second, we have learned the importance of culture and leadership. Technology can highlight anomalies, but only a culture of transparency and ethical leadership will ensure those signals are acted upon. ISC2 members should partner with human resources (HR) and compliance to run joint awareness campaigns, using real-world scenarios to show staff how digital fraud works and what to do if they suspect misconduct. By doing so, we shift from abstract policies to tangible behaviour change.

Third, ACCA's research underscores the need to balance technology and human judgement. Fraud is as much about rationalisation and pressure as about code. To put this lesson into action, cybersecurity teams should sit with finance colleagues during transaction monitoring reviews, helping them interpret anomalies while also learning from their professional scepticism and domain knowledge. Embedding cyber professionals in financial review processes – and inviting finance into cybersecurity drills – creates a mutual learning loop that strengthens both functions.

Fourth, education must expand across the enterprise. The survey data shows many financial professionals remain uncertain about the most common frauds their organisations face. This presents a practical opportunity: ISC2 members can lead cross-functional training sessions where finance staff explain how controls are tested, while cybersecurity professionals demonstrate how AI-generated fraud bypasses those controls. Such exchanges ensure that both technical and financial perspectives are fully integrated into the organisation's defences.

What emerges most strongly from the research is that resilience is collective. ISC2 members bring vital digital skills and foresight, while also gaining from engagement with the perspectives of finance, audit, and risk professionals. By creating standing forums for cross-functional dialogue, embedding cyber expertise into financial control testing, and jointly running simulations of fraud scenarios, we can move from being reactive to proactive.

Our members must be not only defenders of systems but also convenors of trust – leaders who break down silos, strengthen accountability, and help organisations adapt to a world where digital deception is pervasive. The message of this report is clear: combatting fraud in the digital age requires not just technical mastery, but partnership, culture, and shared responsibility.

# 3. Missing the forest for the trees

**Fraud is often instinctively described by classification and case counts. Our research reveals a more complex reality where the real threats often aren't what we think they are. Counting cases is not the same as managing risk.**

Now that we've highlighted the convergence of threats, we explore how fraud's frequency and impact combine to create a landscape that is both more fragmented and interconnected – a dynamic picture shaped not only by how often fraud occurs but by how deeply it hurts and how differently it is perceived.

**'I always have this kind of problem with fraud because it's so broad. I run into a cognitive issue when I try to define what fraud is and is not and I can't because, to a certain extent, everything is vulnerable to fraud and fraud is very much connected to so many other things.'**

Roundtable participant in the US

## Prevalence versus materiality

Our coalition survey data introduces a new two-axis view not found in fraud literature before – how prevalent a scheme is versus how materially damaging it proves when it lands. This distinction matters critically because boards and regulators often focus solely on prevalence while materiality captures the real story: financial loss, reputational damage and operational disruption. These patterns reflect not only different fraud realities but also different professional vantage points. Figure 3.1 provides an overview of overall fraud prevalence and materiality across all demographics.

This unique lens reveals the gap between what happens most often and what causes the most harm, which many respondents had not considered. As Figure 3.2 illustrates, cyberfraud and procurement fraud dominated both prevalence and materiality, but internal frauds such as abuse of authority and expense proved more challenging to detect and report on. Financial statement fraud rounded out the top materiality set despite having a lower prevalence score.

**'Through this data, we could see how boards often mistake frequency for importance – it's the single event that goes undetected, not the frequent small ones, that reshapes trust.'**

Figure 3.1 **Material fraud types strongly correlate with prevalence**

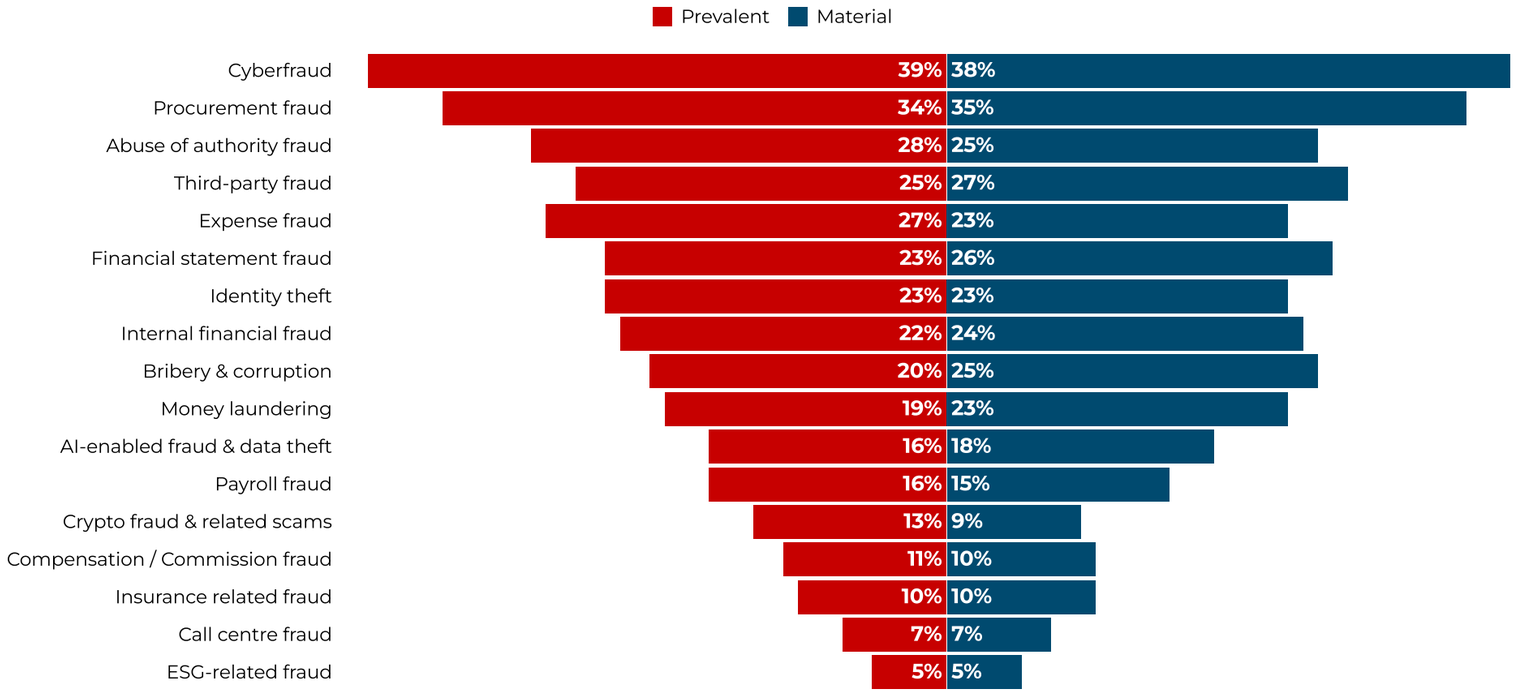
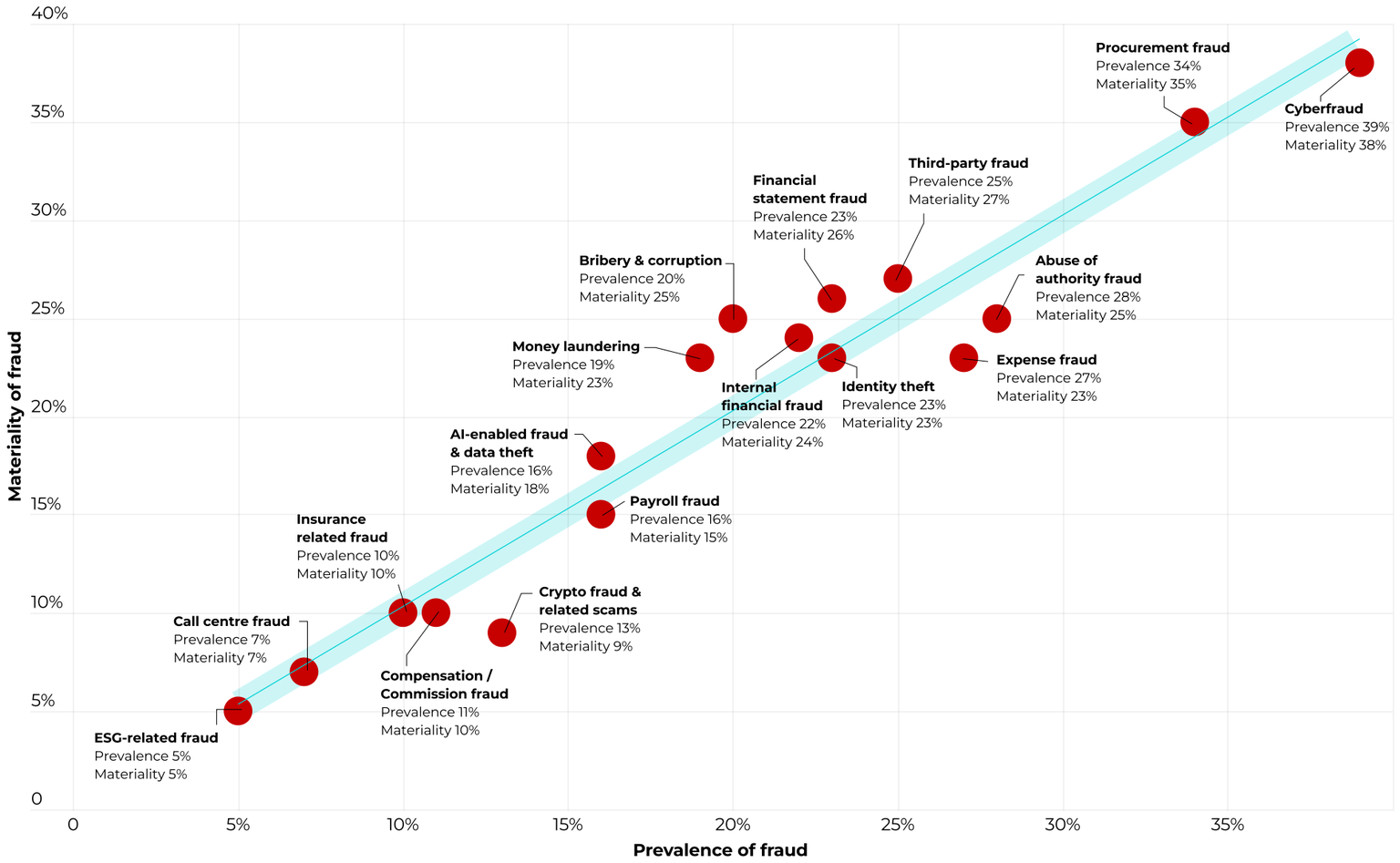


Figure 3.2 **Procurement fraud is prevalent yet underestimated**




## Understanding context

These underlying forces shape every sector differently. Across sectors, procurement fraud and cyber-enabled attacks emerge as universal pain points – but how these risks manifest and are mismanaged varies dramatically by context.

Procurement appears often and is normalised as 'leakage', emerging as more prevalent in public sector bodies, large corporates, and across Africa and the Middle East. Yet individual cases often sit at medium materiality. Left untriaged, their cumulative cost can overshadow more visible risks.

**'Procurement fraud is the easiest way to steal because it looks like business as usual. The amounts are small enough to be ignored, but over time they dwarf cyber losses.'**

Auditor in Africa

Cyber appears episodically and is triaged as 'IT' but when it strikes it is highly material and indeed existential – producing data extortion, prolonged business interruption, cascading losses across third-parties including job losses.

**'Procurement fraud is constant, but it's the cyber-attack you didn't see coming that brings everything down.'**

Participant in the Middle East

The organisations that showed more resilience in our analysis were those that refused to let frequency dictate priority; they asked instead what would damage solvency, service or trust if left unchecked. The two-axis lens helps boards avoid simplistic assumptions: common does not equal catastrophic, and rare does not equal trivial.

## Beyond your walls

By understanding materiality, professionals can ascertain how fraud travels across categories. A business email compromise is rarely 'just an email' – it is a vendor master change, a rushed approval, a payment released without an out-of-band call, and funds that disappear into mixers.

**'We are drowning in cyber alerts. The issue is not detection – it's deciding what is material enough to escalate. And often the real loss is through the supply chain, not our own systems.'**

CRO participant

Today's landscape is more ecosystem-centric, demanding assurance not just over internal controls but also over supplier behaviours, platform data, and identity networks. Without external telemetry, organisations risk proving their controls 'effective' while being blindsided by vulnerabilities beyond their walls.

## The maturity gap

Our regression analysis confirms a critical insight: mature organisations with 'actionable' FRAs were better at recognising materiality than less mature organisations which tended to equate prevalence with importance. This signals a maturity gap in how fraud is prioritised and therefore how decisions around allocating resources are made.

Additionally, we found that the ease of reporting averaged 70% across fraud types even though fraud risk management maturity and trust in anti-fraud measures varied widely by region, sector, teams and seniority.

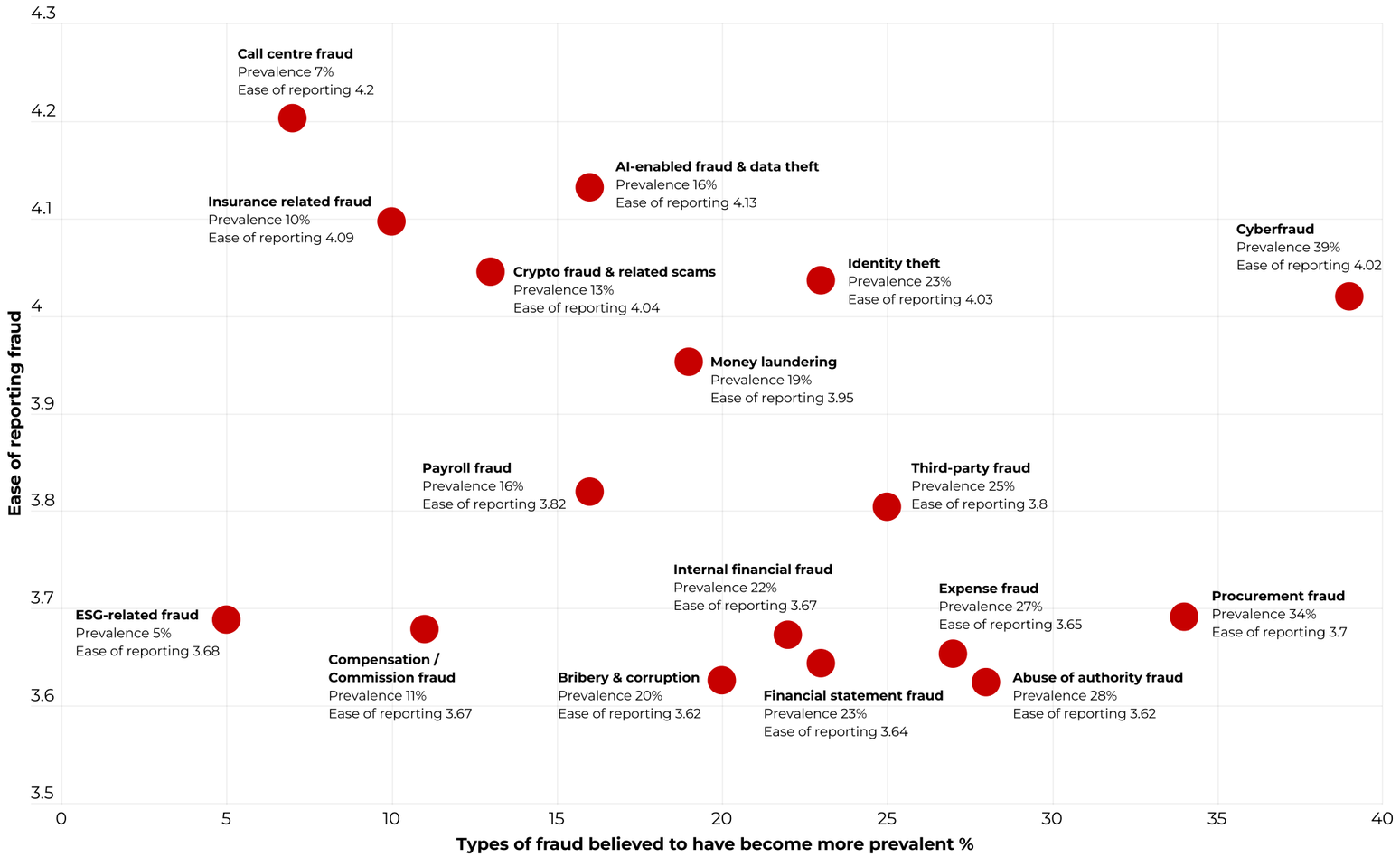
*'We use Ethisphere culture assessments to identify pockets of improvements, but these kinds of frameworks often seem more effective on paper,'* commented one risk professional in India working at a multinational manufacturer.

Comments from regional roundtables reinforce how ownership is unclear, and follow-up is weak.

**'Most companies don't even realise they've been defrauded until it's too late, so how can you report something you don't realise you've been a victim of?'**

Investigator participant

## Figure 3.3 **Internal fraud types are hardest to report**




## Procurement is common, cyber catastrophic

Procurement fraud deserves special attention as the most prevalent for the public sector and many large corporates; however, its materiality was consistently underestimated. The reason? It erodes resources in small but steady increments and can be dismissed as poor management rather than a silent fraud drain. It is also both internal and external.

Figure 3.3 illustrates a critical disconnect – fraud types that are most prevalent, eg, procurement and expense fraud, are often the hardest to report. This reinforces the cultural and hierarchical sensitivities highlighted in our qualitative findings, eg, abuse of authority and the fear of retaliation discussed in our roundtables.

**‘Procurement fraud is almost routine – bid-rigging, split contracts, phantom suppliers. It’s everywhere, but rarely makes headlines.’**

Senior risk officer from the infrastructure sector

This represents fraud seen as ‘part of the system’ – exhausting budgets, distorting competition, and breeding cynicism. Because losses are spread out over time, it rarely triggers the same urgency as high-profile cyber incidents.

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

Bryan Foss, board director and co-founder of the Risk Coalition

Cyberfraud, by contrast, was consistently rated as catastrophic in materiality, even in organisations with advanced controls. Roundtable discussions underscored that cyberfraud rarely exists in isolation. Instead, it converges with procurement fraud (compromised vendor invoices), payroll fraud (identity theft), and money laundering through both cryptocurrencies and cash-intensive sham businesses disguised as legitimate operations.

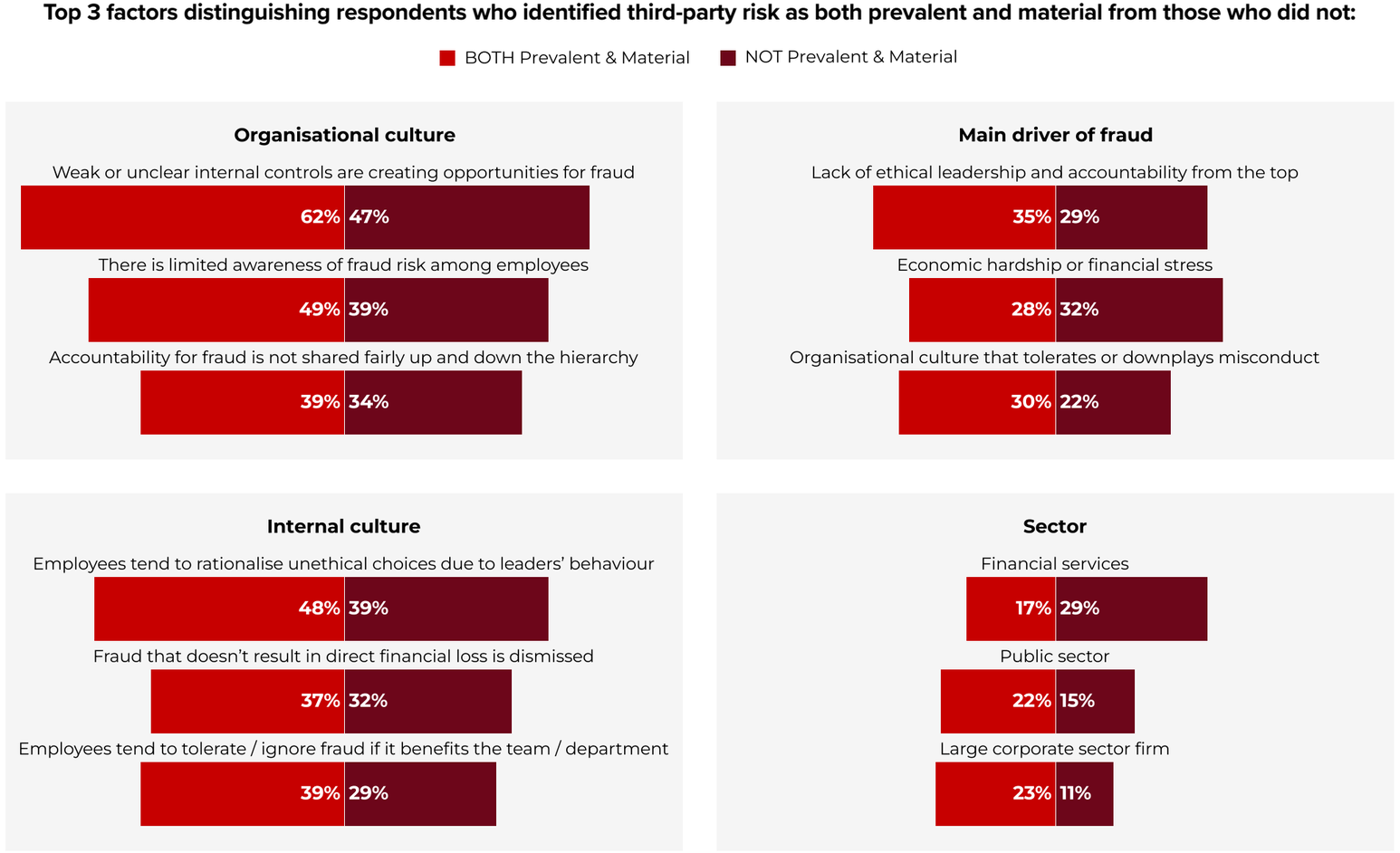
**'It's not just 'know your customer'. All types of firms are rushing into crypto, AI, etc. at all costs when they don't even have basic fraud controls in place.'**

Participant in the Asia-Pacific

## Hidden hazards

Third-party risk was described as an 'inside-out risk' by one respondent in the US. People in large corporates (particularly in technology and manufacturing), the public sector, and internal audit and risk teams ranked it both highly prevalent and material. However, it was one of the lowest scoring fraud types for ease of reporting despite being an external risk. Figure 3.4 explains how third-party fraud, though externally facing, scores below average for ease of reporting. Cultural factors – such as weak internal controls, limited awareness, and unclear accountability – emerge as key barriers.

Figure 3.4 **Third-party fraud scores below average on ease of reporting**



ESG fraud and crypto crimes are two other areas that surfaced as systematically underestimated material risks.

**‘Everybody put ESG-related fraud at only 5% but it is actually rising. Many just don’t investigate ESG matters.’**

Participant in the Asia-Pacific

ESG fraud, especially manipulated carbon credits and false sustainability claims, showed low prevalence but high concern mostly among younger respondents, compliance teams, South East Asians, and Europeans. Crypto and stablecoin fraud appeared more frequently in roundtables than in the survey. Participants, particularly in North America and the wider Asia-Pacific, described them as magnets for organised crime and regulatory blind spots.

**‘We’re fighting yesterday’s war while tomorrow’s criminals are already here. ESG fraud and crypto aren’t tomorrow’s problems – they are today’s blind spots.’**

Accountancy professional in Canada

**‘Decisions about investing in crypto and bitcoins are being made by people who aren’t doing proper due diligence. What could possibly go wrong?’**

Participant in the UK

## The perception problem

Organisations consistently misallocate resources by confusing frequency with impact. Most noteworthy is not the fraud types themselves but the overlooked risks around them. Different demographic responses show that responsibility for detecting and preventing fraud is viewed through contradictory lenses.

**‘Our bias that a fraudster is a certain type of person – age, gender or role – is blinding us to the reality that it’s really not. It’s much wider and opportunism takes lots of forms.’**

Respondent in Australia

Two practical reallocations follow from the data. Move procurement and third-party risk out of the ‘operational’ margins and make them board-visible because they decide competitiveness and integrity. Stop assuming that cyber belongs to technologists alone; it is a fraud vector with profit-and-loss consequences and recovery cycles that boards must demand rehearsing like any other liquidity or continuity risk.

Effective fraud management requires us to learn not just what fraud looks like, but how we systematically misperceive and mis-prioritise it. Recognising this complexity is the first step toward building defences that work in practice, not just on paper. When leaders make those shifts, the whole forest becomes visible again, and the trees fall into place.

## Key takeaways

### Are you allocating fraud prevention resources based on what happens most or what matters most?

Assess whether your risk prioritisation confuses frequency with impact, evaluate if decision makers include diverse perspectives that counter systematic blind spots, and determine whether resource allocation is forward-looking or reactive to last year’s incidents. The fundamental question is whether you’re building defences based on risk triangulation or just responding to the fraud that scares you most.

# Closing the fraud gaps together

**Across the results of ACCA's coalition survey, two things stand out. First, we're not surprised that procurement, insider/authority-linked, third-party and cyber-related risks dominate as the most prevalent and material frauds. Our respective professions emphasise different focal points in the fight against fraud, and that's precisely where proactive collaboration can raise the bar from detection to prevention.**

Regarding materiality, ACFE respondents put procurement fraud slightly ahead of ACCA and rate bribery and corruption and third-party fraud higher than ACCA, reflecting ACFE's proximity to field investigations and case resolution. ACCA respondents, by contrast, elevate cyberfraud and financial-statement fraud more strongly – consistent with finance's responsibility for reporting integrity and systems exposure.

In terms of prevalence, both professions rank procurement and cybersecurity near the top, whilst ACFE respondents rank abuses of authority and internal financial frauds higher than ACCA members, indicating an investigative lens with unique insight into the human factors behind fraud. ACCA respondents rank financial-statement fraud higher in prevalence than ACFE, which aligns with its assurance roles.

## The whistleblowing reality

It's also unsurprising to see different responses when it comes to measures to encourage speaking up.

**'Almost half of frauds I see are detected by whistleblowing or people having the courage to speak up.'**

ACFE member in Australia

This investigative reality underscores why ACFE respondents prioritise protections and independence: anti-retaliation and ensuring investigations are carried through are notably stronger preferences than ACCA respondents.

The same member also cautioned: *'Often the police aren't interested, they're not experienced in it. Fraud is not sexy enough.'* This pragmatic view of enforcement gaps explains why both professions must help organisations build internal capability rather than relying solely on external authorities.

Figure 3.5 **Which of these statements do you agree with?**

## Cultural and control

Perceived fraud driver responses tell the cultural story. ACFE respondents indicated that insufficient enforcement and the belief that fraud won't be detected are more prevalent than ACCA respondents. This result reflects anti-fraud practitioners' scepticism regarding the consequences of fraud and the capacity for detection.

Both ACCA and ACFE respondents call out lack of ethical leadership and economic stress at similar levels – shared ground for a single message to boards. One participant, who is both ACFE and ACCA and working with major corporates in the US, added candidly: *'I've worked in some organisations where there's been an absolute absence of internal controls, and this has been big international household names... It's quite surprising how many organisations have abysmal internal controls.'*

## What drives modern fraud

The motivational landscape has shifted dramatically:

**'More than 15 years ago, in every fraud I investigated gambling was the motive. Now it's lifestyle and it's living beyond people's means, and they see all the advertisements and go, *"That's what everyone's doing and I'm not doing that. I want a piece of that".*'**

ACFE investigator

This evolution reflects changing societal dynamics that both professions must address in prevention strategies.

## Strategic collaboration

**Fuse independence with simplicity for improved fraud reporting.** The ACFE community can lead on independent case handling and anti-retaliation assurance, whilst ACCA can operationalise this into clear, simple reporting processes and role-specific training that actually reaches first-line staff. Pairing these respective strengths tackles both willingness and ability to report.

**Make prevention measurable.** ACFE's field insight into insider/authority-based typologies and third-party collusion risks should inform finance-led risk assessments and dashboards (override rates, vendor/beneficial ownership change analytics, time-to-decision). ACCA's systems view should be leveraged to ensure those measures are embedded in controls and approvals, not just noted in policies.

**Close the consequences gap.** With ACFE respondents noting enforcement gaps and detection scepticism and ACCA spotlighting technology control drift, a unified call to boards and regulators can link culture and capability – emphasising independent investigations, publishing aggregated outcomes and investing in defensive analytics where risk is highest (procurement, insider, or third-party).

**Speak with one voice about leadership.** Since both groups flag poor tone at the top, we should jointly press for failure-to-prevent-ready programmes: live evidence files of procedures, tests and outcomes – across financial and non-financial metrics – so leadership accountability is visible, auditable and real.

**'The ACFE is made up of a lot of different people, including accountants. Embrace the multidisciplinary nature. Don't think you have to do everything yourself.'**

ACFE member in the Asia-Pacific

In the end, we observe the same issue from various perspectives. ACFE members excel at independence, consequences and human factors, ACCA at systems, controls and assurance. By integrating these perspectives, we can turn potentially fragmented efforts into measurable prevention – the outcome that ultimately matters most.

See Appendix A on how to optimise anti-fraud measures by using both the ACFE's Fraud Tree and the coalition typology together.

# Crypto fraud – why it's hard to stop

**Cryptocurrency and decentralised finance (DeFi) present a unique frontier for fraud that traditional controls struggle to address. Our survey data showed that despite rising prevalence, only 10% of crypto fraud cases are referred to law enforcement – the lowest referral rate of any fraud type (Figure 3.6). This gap reflects both the technical complexity and jurisdictional challenges that make crypto fraud exceptionally difficult to detect, investigate, and prosecute.**

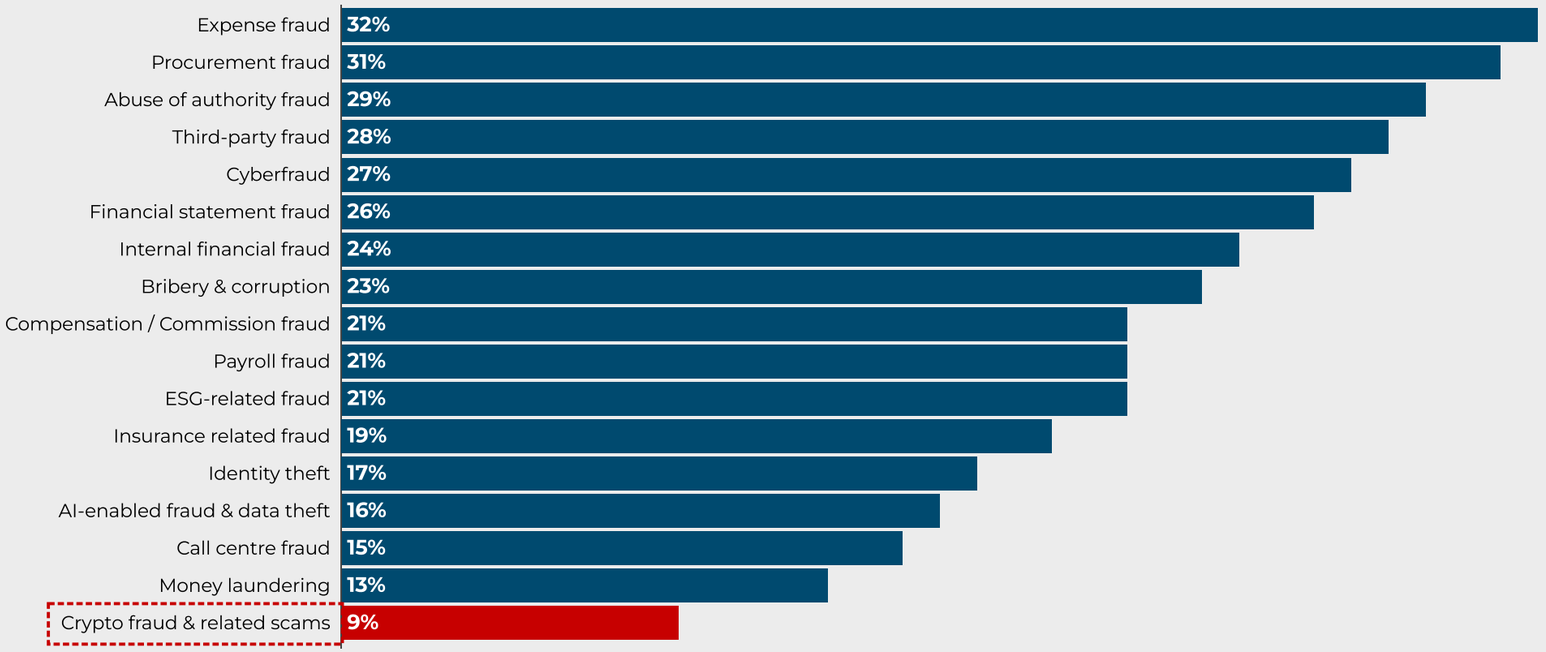
## Why crypto fraud differs

Traditional fraud controls assume reversibility, intermediaries, and jurisdictional clarity – assumptions that blockchain technology fundamentally eliminates. Once funds leave a wallet, they're irreversible. Blockchain's pseudo-anonymity makes perpetrators hard to trace, and cross-border flows occur in seconds, exploiting regulatory fragmentation. As one respondent noted:

**'Stolen funds move across jurisdictions in minutes. Enforcement varies wildly – Asia-Pacific is a prime example. That makes recovery almost impossible.'**

Our survey reveals that crypto fraud and money laundering are significantly more prevalent in financial services despite having some of the lowest referral rates to law enforcement for the sector, 9.3% and 13.3% respectively.

Figure 3.6 **Respondents reporting referral of incidents to law enforcement**



## The regulatory landscape

Fragmented crypto regulation creates arbitrage opportunities for fraudsters. PwC's global analysis highlights that regulatory fragmentation continues to enable this, especially in jurisdictions where crypto-assets are not yet fully integrated into financial services regulation.[7] While frameworks are emerging – Hong Kong's Securities and Futures Commission (SFC) licensing requirements, the EU's Markets in Crypto-Assets (MiCA) regime, the UAE's Virtual Assets Regulatory Authority (VARA), and the US Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act – enforcement capacity lags behind.[8]

A review by the International Organization of Securities Commissions (IOSCO) found that while most jurisdictions have frameworks for fraud and market abuse, enforcement authority often does not extend beyond crypto-asset service providers, leaving significant oversight gaps.[9] As Figure 6.1 shows, 21% of respondents cite 'insufficient enforcement or fear of consequences' as a main fraud driver. IOSCO warns that without consistent implementation, investor protection and market integrity remain at risk.

## Common schemes to recognise

### Phishing and social engineering:

Fraudsters use deepfake video and voice to impersonate wallet providers, exchanges, or colleagues and obtain private keys or seed phrases.

### Rug pulls and exit scams:

Token founders attract investment, then drain liquidity pools and disappear – DeFi's permissionless nature enables this with minimal oversight.

### Smart contract exploits:

Code vulnerabilities allow attackers to drain funds. The 2022 Ronin Network (US$625 million) and Poly Network (US$611 million) breaches demonstrate the scale of risk.[10]

### Pump-and-dump schemes:

Coordinated groups artificially inflate token prices through social media, then sell at peak, leaving retail investors with losses.

### Ransomware payments:

Criminals exploit crypto's pseudo-anonymity and irreversibility.

## Red flags for finance teams

### Transaction patterns:

- Unrealistic returns, fake endorsements, or pressure to 'act fast'
- Rapid crypto-to-fiat conversions via unregistered Virtual Asset Service Providers (VASPs)
- Dormant accounts with sudden abnormal volumes
- Structuring transactions below reporting thresholds
- Deepfake-based impersonations in payment requests.

### Operational warning signs:

- Urgent crypto payment requests bypassing standard approvals
- Wallet address change requests without independent verification
- New counterparties insisting on crypto-only payment
- Vendors unable to explain custody and security arrangements
- Firms operating without proper licensing or adequate Know Your Customer/Know Your Transaction (KYC/KYT) procedures.

7 PwC (2025) – *Global Crypto Regulation Report 2024*.

8 Hong Kong SFC – *Virtual Assets Regulatory Framework*; European Securities and Markets Authority – *Markets in Crypto-Assets Regulation (MiCA)*; UAE Virtual Assets Regulatory Authority – *Crypto Regulation Overview*; US Congress – *Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act*.

9 IOSCO (2025) – *Crypto-Asset Markets: Regulatory Approaches and Enforcement Challenges*.

10 Merkle Science (2022) – *Analysis of Ronin Network Exploit*.

## Controls that work

### Cold storage and multi-signature wallets:

Keep most assets offline; require multiple authorisations for transactions above materiality thresholds.

### Out-of-band verification:

Mandate callback verification for wallet changes or large transfers using separate channels. Deepfake attacks exploit single-channel communication.

### Transaction monitoring:

Deploy blockchain analytics tools flagging suspicious patterns: rapid wallet movements (layering), known high-risk addresses, or unusual timing and amounts.

### Segregation of duties:

Separate custody, initiation, and approval functions. No single individual should control private keys and authorisation.

### Essential compliance:

- Enhanced due diligence with robust KYC/KYT procedures
- Real-time transaction screening using blockchain analytics and AI
- Regular audits and employee training
- Incident response plans for crypto-related anti-money laundering (AML) and counter-terrorism financing (CTF) breaches.

## Forensic capabilities

While blockchain transactions are pseudo-anonymous, they're recorded on public ledgers. Specialist firms like Chainalysis, Elliptic, and CipherTrace can trace fund flows, identify address clusters, and flag sanctioned addresses. However, this requires expertise most finance teams lack. Organisations should establish relationships with blockchain forensics providers before incidents occur.

## When to involve law enforcement

Despite low referral rates, certain crypto fraud warrants immediate escalation:

- Material losses (jurisdiction-dependent thresholds)
- Evidence of organised crime or terrorist financing
- Ransomware payments (may be legally reportable)
- Insider fraud involving corporate wallets
- Cross-border schemes affecting multiple victims.

### Key takeaways

**Crypto fraud is not a niche risk.**

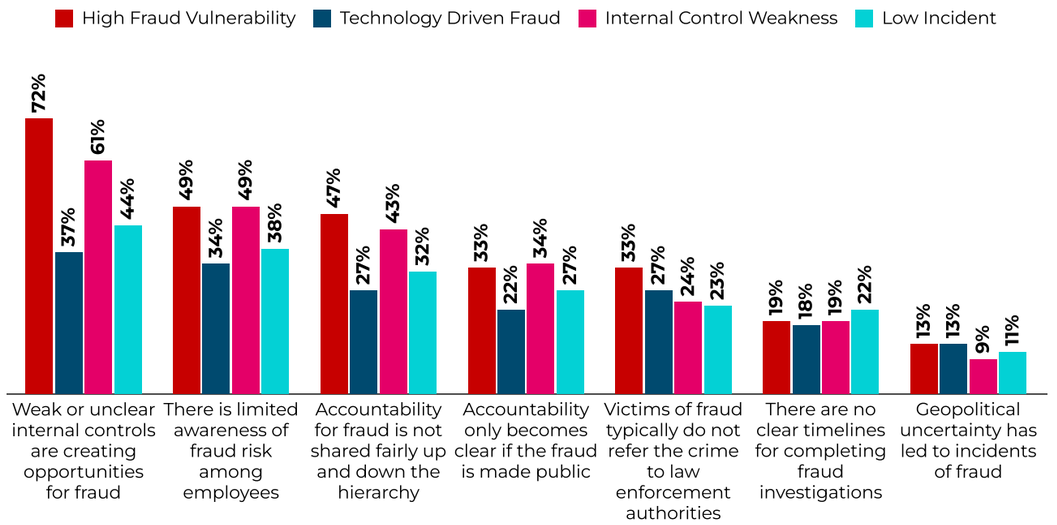
Organisations accepting crypto payments, holding crypto treasuries, or operating in Web 3.0 spaces face material exposure. Traditional fraud controls assume intermediaries and reversibility that crypto eliminates. Finance professionals must understand these differences, implement crypto-specific controls, and build relationships with specialist forensic and legal advisers before losses occur. The 10% referral rate suggests most organisations discover crypto fraud too late, after recovery options have evaporated.

# 4. Putting perceptions into context

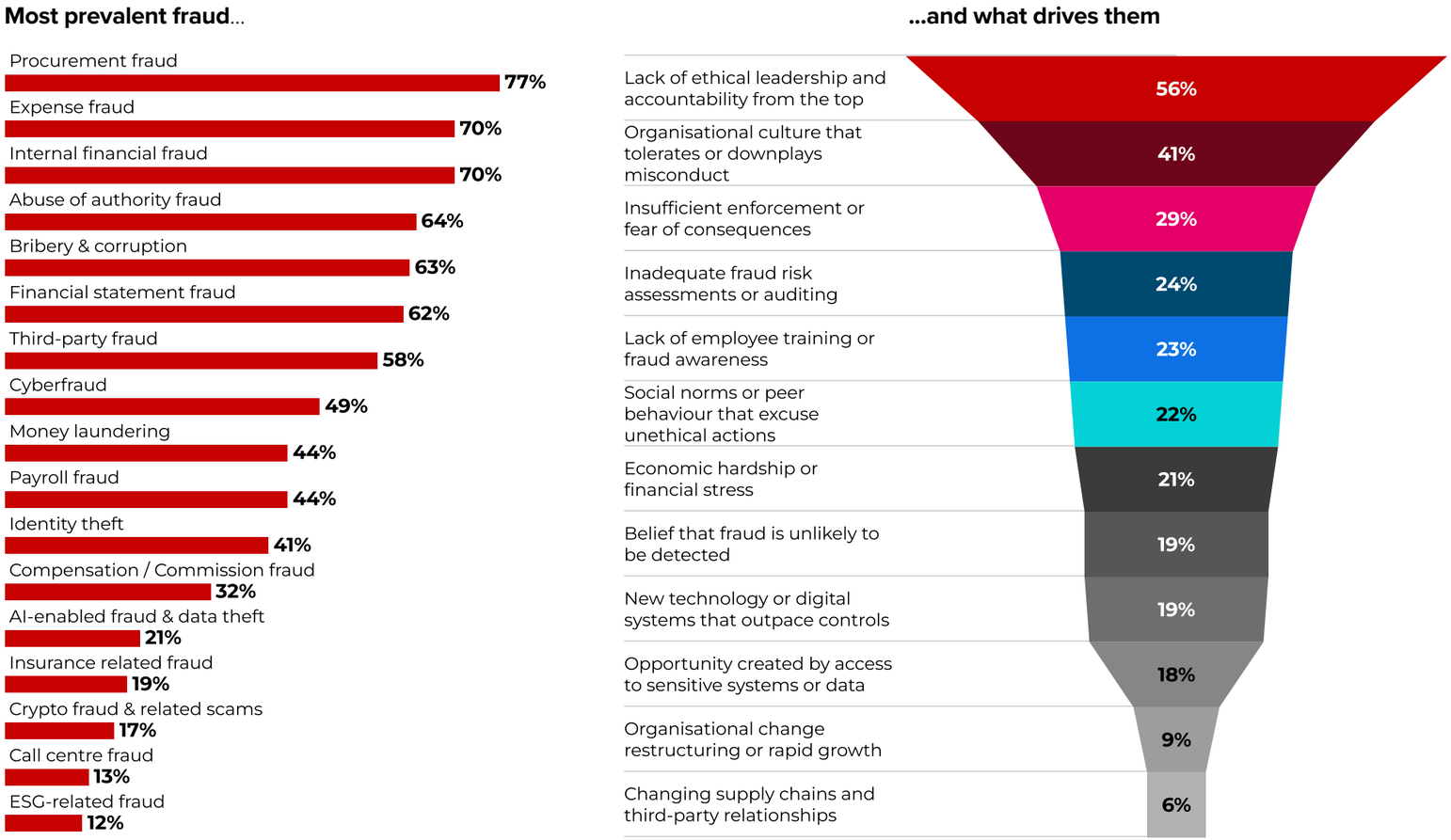
**Fraud is about not only the risks themselves but crucially how different stakeholders perceive them. In this section, we show how perception gaps across personas and professions create blind spots that undermine prevention.**

As Figures 4.1 and 4.2 show, our cluster analysis of our coalition survey data explains why fraud looks so different depending on whom you ask.

Figure 4.1 **Personas differ sharply on cultural and structural drivers**



## Figure 4.2 **High Fraud Vulnerability clusters* reveal distinct fraud risk profiles and drivers**




* High Fraud Vulnerability cluster: this group faces higher risks of traditional fraud and reports the highest prevalence across many fraud types.

**‘One of the biggest problems is that we have been so obsessed with controls, but ignore the different behaviours that cause fraud.’**

So explained Ashu Sharma, chief strategy officer at the Association of Corporate Investigators (ACi) and group investigations lead at Anglo American, in ACCA’s Risk Culture podcast episode, *Fraud Thrives Where Culture Fails*. He emphasised:

**‘Fraud no longer knocks on the front door. It’s built into the architecture.’**

Ashu Sharma, chief strategy officer at the ACi and group investigations lead at Anglo American

In our research, we analysed all the demographics and crucially also *how* people think and behave when it comes to fraud. As part of our cluster analysis, we identified four distinct personas, each shaped by sector, seniority, and cultural context.

## Persona 1: Overloaded Realists

These respondents recognise fraud as serious but feel overwhelmed and under-resourced. They are most common in small and medium-sized entities (SMEs), public sector organisations, and regions with limited enforcement.

**‘Fraud is everywhere, but we’re stretched so thin it feels impossible to do more than firefight.’**

Operational risk director at an NGO in Africa

This group of respondents highlighted procurement fraud, third-party risks and lack of bandwidth to pursue root cause analysis or act on fraud once detected. For them, fraud is a constant background pressure.

## Persona 2: Cynical Insiders

These respondents distrust governance and assume systems are compromised. They are more common in environments where corruption is endemic or where leadership has been seen to cut corners.

**‘If the board doesn’t follow its own policies, why should anyone else?’**

Internal auditor in the private sector in the Asia-Pacific

This group is also more likely to rationalise fraud, reflecting our regression analysis findings that showed low trust in leadership correlates with higher acceptance of rationalisation. Cynical Insiders see fraud as ‘part of doing business’ – not because they endorse it, but because they believe leadership sets the tone.

## Persona 3: Optimistic Practitioners

These respondents, working mostly in financial services and large corporates, trust systems, controls and compliance frameworks.

**‘We’ve invested in systems. Fraud isn’t our biggest worry.’**

Senior compliance officer from a multinational bank in Europe

They often underplay fraud prevalence, assuming that investments in technology and governance are enough. The risk is complacency: being unprepared for systemic shocks such as cyber-attacks or major procurement scandals.

## Persona 4: Detached Observers

This group treats fraud as somebody else’s problem. They are often in roles not directly tied to governance, such as finance managers or operational leads.

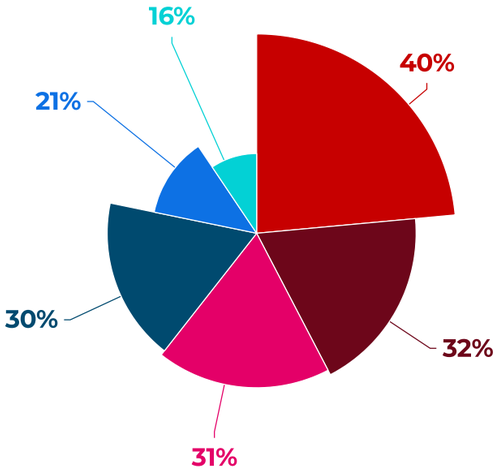
**‘Fraud isn’t really my area – others are handling it.’**

Survey respondent working in finance in the US

This group poses a particular risk because disengagement itself creates blind spots. They are least likely to speak up, least aware of drivers and most vulnerable to being blindsided by fraud.

Our survey shows that employees rationalise fraud differently: some excuse it if it benefits the team, others dismiss non-financial misconduct entirely – patterns that correlate with leadership tone and cultural norms. Figure 4.3 shows rationalisations of fraud overall.

Figure 4.3 **Rationalisations of fraud**




- Employees tend to rationalise unethical choices due to leaders' behaviour
- Fraud that doesn't result in direct financial loss is dismissed
- Employees tend to tolerate or ignore fraud if it benefits team / department
- Fraud is being rationalised due to perceived unfairness*
- Fraud involving digital systems (eg bots AI manipulation) is overlooked
- Certain types of fraud could be justifiable due to pressures felt

*(eg pay gaps lack of recognition)

## Professional and generational patterns

Our cluster analysis reveals why the fraud landscape looks so different depending on perceptions. Figure 4.4 illustrates the fraud perceptions by profession and generation.

- **Overloaded Realists** (often in SMEs and public sector) see procurement fraud everywhere but feel powerless to fight it.
- **Optimistic Practitioners** (financial services, large corporates) downplay prevalence, trusting in systems until a shock hits.
- **Cynical Insiders** focus on leadership failures, treating fraud as inevitable in corrupt environments.
- **Detached Observers** underplay fraud entirely, assuming someone else has it covered.

Together, these perceptions explain why the same fraud can be dismissed in one context, tolerated in another and treated as existential elsewhere.

**'Fraud is not one risk but many risks, depending on whom you ask. That's why policies that look neat on paper fail in practice.'**

Participant from the Asia-Pacific

The personas also correlate with generational and seniority differences:

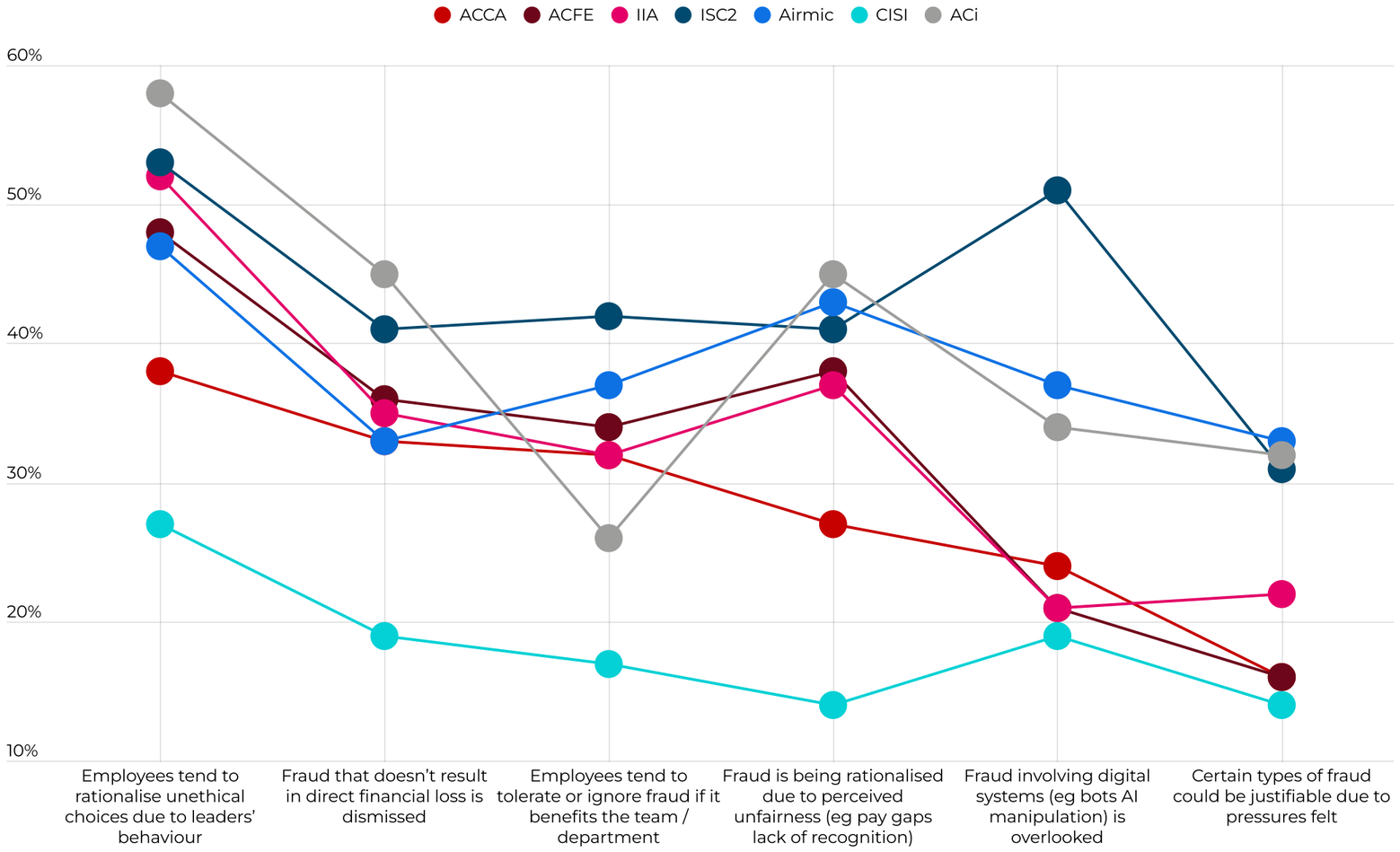
- **Younger professionals** tend to align with Overloaded Realists, aware of risks but lacking influence.
- **Senior leaders** often resemble Optimistic Practitioners – confident in systems but sometimes detached.
- **Middle managers** often fall between Realists and Cynical Insiders, feeling accountable but under-supported.

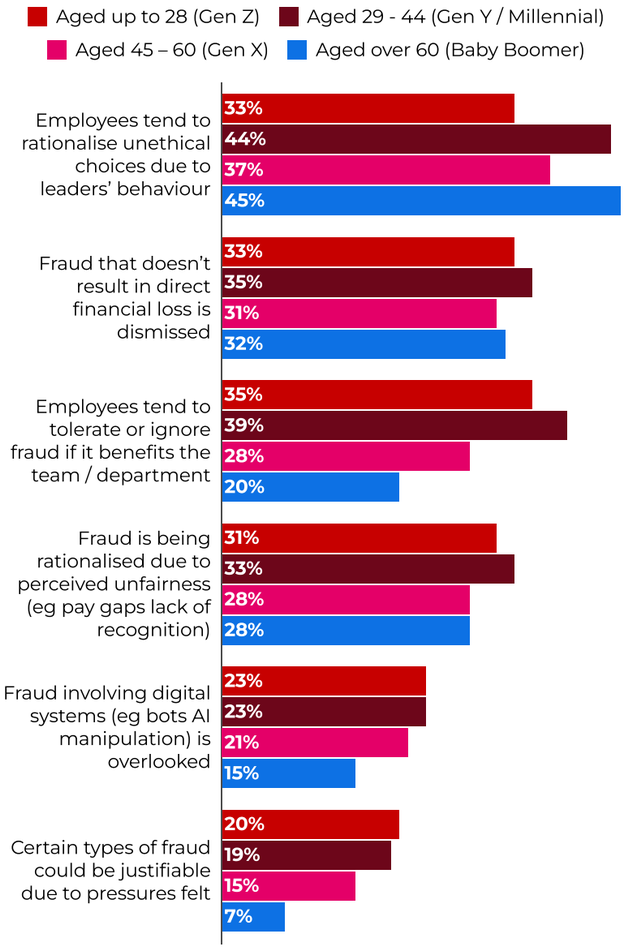
These personas help us understand other governance fractures: optimism at the top, anxiety in the middle, and disengagement at the edges. Because this research draws on multiple professional bodies, we can also see how the various professions perceive fraud differently:

- **Accountants** emphasise financial pressure and misaligned incentives.
- **Risk managers** highlight governance gaps and unclear accountability.
- **Cyber professionals** focus on infrastructure vulnerabilities and organised crime.
- **Auditors** worry about credibility gaps and the limits of assurance.

For example, survey results on 'ease of reporting' showed that Airmic respondents rated their organisations significantly lower than ACCA respondents – evidence of how professional orientation shapes lived experience of fraud.

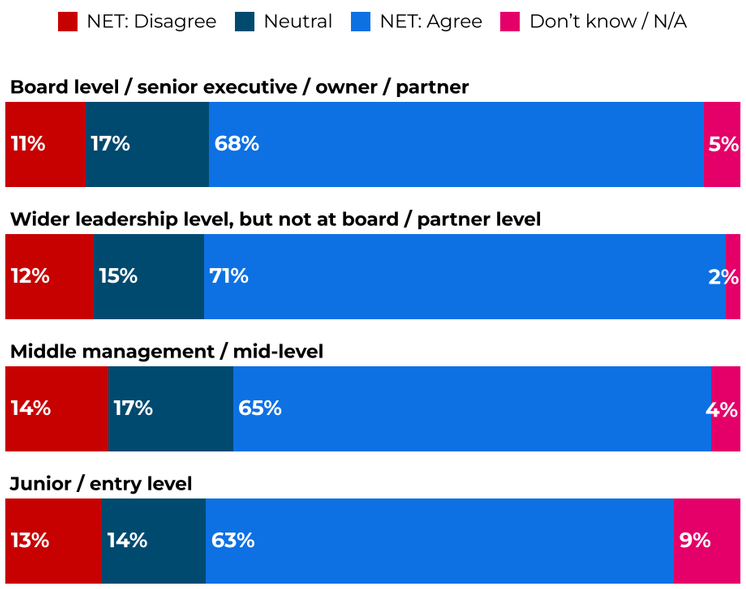
## Figure 4.4 **Professional and generational divides shape fraud perception**



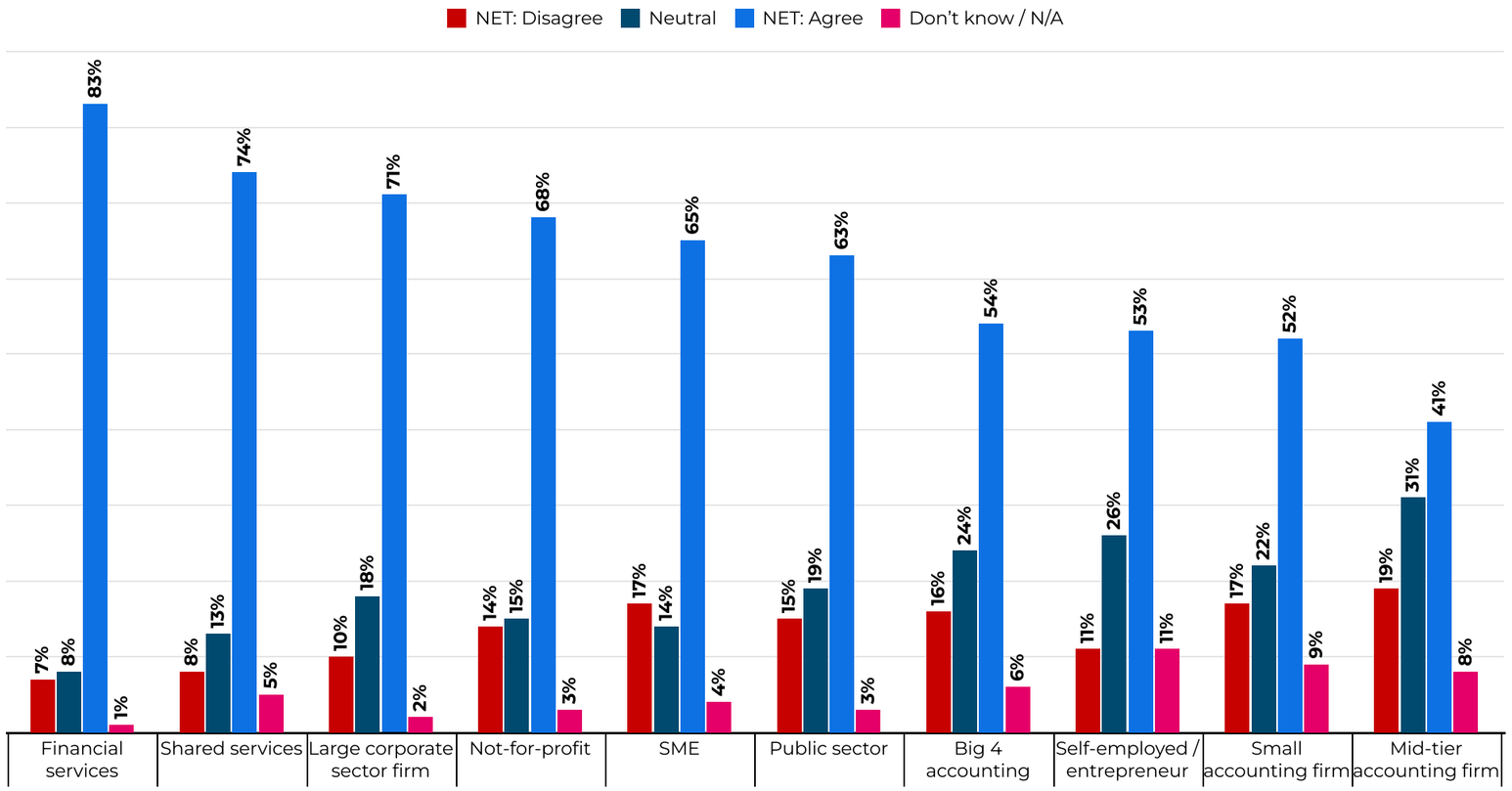



Our survey data analysis ties perception gaps to practical consequences, Figures 4.5 and 4.6 show how the ease of reporting varies sharply by seniority and sector (internal and external roles), with frontline staff least confident – an asymmetry that deepens perception gaps and undermines early detection.

## Figure 4.5 **Ease of reporting improves with seniority**




## Figure 4.6 **Ease of reporting by sector**




**Note:** Accountancy firms, including the Big 4, report greater difficulty in escalating fraud concerns. Independence constraints and commercial sensitivities may contribute, alongside ownership models that blur escalation pathways. This pattern links to elevated financial statement fraud prevalence (Fig 2.2) and external audit's low ease-of-reporting score (Fig 7.3).

## From personas to policy

These personas are not academic – they have practical implications for governance, training, and FRAs. Recognising them gives boards and regulators a powerful diagnostic tool to identify stakeholders' attitudes: urgent, resigned or detached.

The first step to building effective defences is to synthesise a shared view. Without that, organisations will remain fragmented, chasing different risks with different assumptions – and leaving gaps wide open.

### Key applications:

- **Communications must be tailored:** messages for Cynical Insiders won't work for Detached Observers.
- **Training must account for different rationalisations:** realists need tools, optimists need reminders, cynics need leadership trust, observers need engagement.
- **Boards must understand their signals shape rationalisations:** they need to ask not just more questions but the right ones and demand more proof of monitoring.

**'It's not that people don't care about fraud. It's that they're all looking at it from different angles. The challenge is bringing those views together.'**

Participant from a large corporate in the Middle East

There is neither a silver bullet nor a one-size-fits-all solution. Policies that work for one group may fail in another. Training, governance, and communication must be tailored to personas, sectors, and cultures. Fraud risk management that recognises these differences moves beyond compliance into culture. It treats people not as abstract roles, but as distinct actors whose perceptions shape outcomes.

## Who sees fraud – and who acts?

**Fraud may be universal, but our research shows its meaning shifts dramatically across organisational layers.**

Boards often claim oversight yet treat fraud as a reputational footnote, surfacing only when scandals erupt. C-suites frame the risk through optics – litigation, investor confidence – but shy away from transparency that could dent short-term image. Middle managers, by contrast, live in the hazard zone: they see procurement anomalies and control overrides daily, yet feel squeezed between responsibility and authority, unsure whether escalation will be supported. At the other end, younger professionals bring a broader ethics view, linking fraud to AI misuse, data privacy and social responsibility. They are more willing to speak up, but far less confident they'll be protected.

These fractures matter. When optimism at the top collides with anxiety in the middle and ethical urgency at the edges, prevention strategies misfire.

Closing the gap means boards owning fraud as a strategic risk, leaders signalling transparency over optics, and organisations embedding protections that turn willingness into action.

**'Fraud isn't in our board packs unless it explodes.'**

Board participant

**'We know the risks are there, but who really has our back?'**

Middle manager

**'Fraud isn't just theft – it's misuse of trust.'**

Younger professional

## Key takeaways

**Do you consider the different personas in your organisation, and designing responses accordingly?**

You cannot address fraud effectively when your board shows optimistic confidence while middle management displays cynical distrust and operational teams feel overwhelmed – each group needs different engagement approaches. Are you building defences based on your professional view alone or integrating multiple perspectives? Assess if your fraud risk assessments incorporate insights from all relevant functions and determine if leadership signals are interpreted consistently across levels. Fragmented views create the exact blind spots that sophisticated fraudsters exploit.

Voices from the coalition – ACi

# Why investigation must sit at the table

Association of Corporate Investigators

**The ACi responses in ACCA's coalition survey reveal a critical insight – fraud is no longer an exceptional occurrence, it's embedded within modern business operations. However, most organisations still treat it as an isolated anomaly rather than integral to enterprise risk design. This cognitive disconnect represents perhaps the most significant barrier to effective prevention.**

## The structural vulnerability

Corporate trends towards decentralisation – siloed workforces, complex supply chains, disconnected digital ecosystems – have fundamentally altered the fraud risk equation. Remote working arrangements have expanded attack surfaces whilst reducing informal oversight mechanisms. Third-party relationships create extended networks of trust that sophisticated actors exploit. These structural changes demand distributed, intelligence-driven approaches that can adapt to modern operations, not localised defences designed for yesterday's threats.

## The skills gap

As financial crime becomes more sophisticated, traditional investigation functions must evolve. The complexity of contemporary fraud schemes requires professionals who can navigate not only accounting irregularities but also digital evidence trails, cryptocurrency transactions, and cross-jurisdictional flows. Forensic accounting – the convergence of financial expertise and investigative acumen – is becoming essential, yet increasingly rare.

Critically, these capabilities must be deployed during monitoring and investigation, when threats emerge, not relegated to post-incident audits. Early detection requires the right people doing the right work with the right authority.

## The collaboration imperative

Perhaps the most significant insight from ACi members is that effective fraud prevention requires unprecedented cross-functional collaboration. Traditional silos separating finance, compliance, legal and investigative functions prove counterproductive when fraud schemes exploit the seams between organisational disciplines.

ACi practitioners emphasise learning across professional boundaries – investigators seeking accountancy skills, accountants wanting investigative perspectives. This collaborative imperative extends beyond individual organisations to encompass professional bodies, regulatory authorities, and industry associations. The partnership across seven professional bodies in this research exemplifies the cross-institutional cooperation essential for addressing the systemic nature of modern fraud risk.

## From mindset to action

The path forward requires courage to challenge established practices, wisdom to learn from multidisciplinary perspectives, and commitment to treating fraud prevention as strategic imperative rather than compliance obligation. Organisations must:

- Embed investigative thinking into risk assessment, not just incident response.
- Create cross-functional teams with genuine authority and resources.
- Invest in hybrid skills that combine financial, digital, and investigative expertise.
- Treat fraud as a structural design challenge, not an operational exception.

Only through collective engagement – across functions, professions and institutions – can organisations build the resilience necessary to combat evolving fraud threats and make business safer for all.

**Ashu Sharma**, Chief Strategy Officer, Association of Corporate Investigators

# 5. The accountability vacuum – when everyone's job becomes no one's job

**Fraud is both a financial risk and a governance test. This section exposes a glaring reality – governance gaps actively drive fraud risk, creating vacuums that turn fraud from hazard into inevitability.**

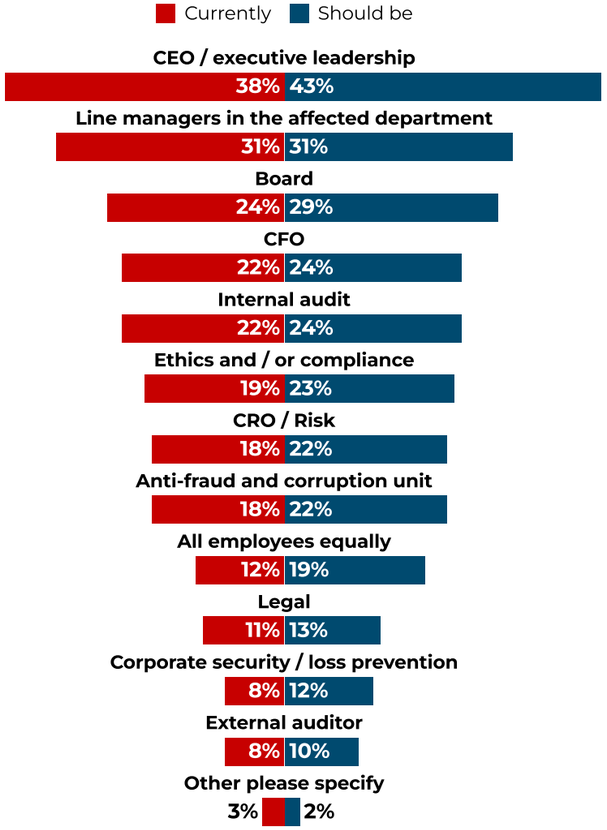
## When ownership disappears

Our survey data and roundtables reveal how easily accountability disappears and misconduct thrives. We found that accountability for fraud remains fragmented, with responsibility pushed up, down and sideways depending on roles and circumstance. Figure 5.1 highlights a critical misalignment: respondents believe anti-fraud responsibilities should extend beyond current allocations, with internal audit and ethics/compliance most often cited as under-assigned. A similar gap exists for senior executives. Instead, responsibility gets dispersed across audit, compliance, or risk functions – none of which have full authority to drive organisational change.

**'Fraud accountability in our company is like pass the parcel – everyone thinks it belongs to someone else.'**

UK roundtable participant

Figure 5.1 **Fraud oversight: Board and C-suite show the largest accountability misalignment**




**Gap in anti-fraud roles:** Survey shows a mismatch between functions tasked and those that should be.

The board's role was often raised in the roundtables. *'Are they wilfully blind or conveniently ignorant?'*

**Some cited the Fear of Finding Out – FOFO.**

*'They don't want to know... because if I want to know, then I'll probably have to resign. And that 'don't want to know' creates a beautiful, dark corner that grows and grows,'* another UK roundtable participant said.

This poor coordination creates a dangerous vacuum, and our regression analysis reinforces it – respondents who said their organisations had clear governance ownership of fraud were twice as likely to express confidence in managing it. Where ownership was blurred, confidence fell sharply.

Boards can set tone and approve frameworks, but real operational control and resource allocation sit on the first line.

*'If fraud is recognised as material, the chief operating officer* [COO] *must own it because they control the resources'*, explains Bryan Foss, board director and co-founder of the Risk Coalition. If fraud is treated as a compliance or second-line issue, it gets 'skinny resources' and remains reactive. Foss, a member of our special interest group, said that the COO, as the operational lead, is the only role with authority to shift people and budgets quickly.

**'If the COO's plan and KPIs [key performance indicators] don't include fraud prevention, the work starves. The risk management doesn't work.'**

Bryan Foss, board director and co-founder of the Risk Coalition

## FOFO as governance failure

Roundtables surfaced this pattern that formal governance codes don't name but practitioners recognise instantly: FOFO – board-level reluctance to probe fraud risk because discovery triggers obligations, reputational damage or personal liability.

FOFO manifests as strategic myopia where boards focus on growth whilst treating fraud as a 'compliance problem' – selective scepticism that accepts management assurances without demanding evidence, and consequence avoidance that refuses to investigate senior figures because 'it would damage the share price'.

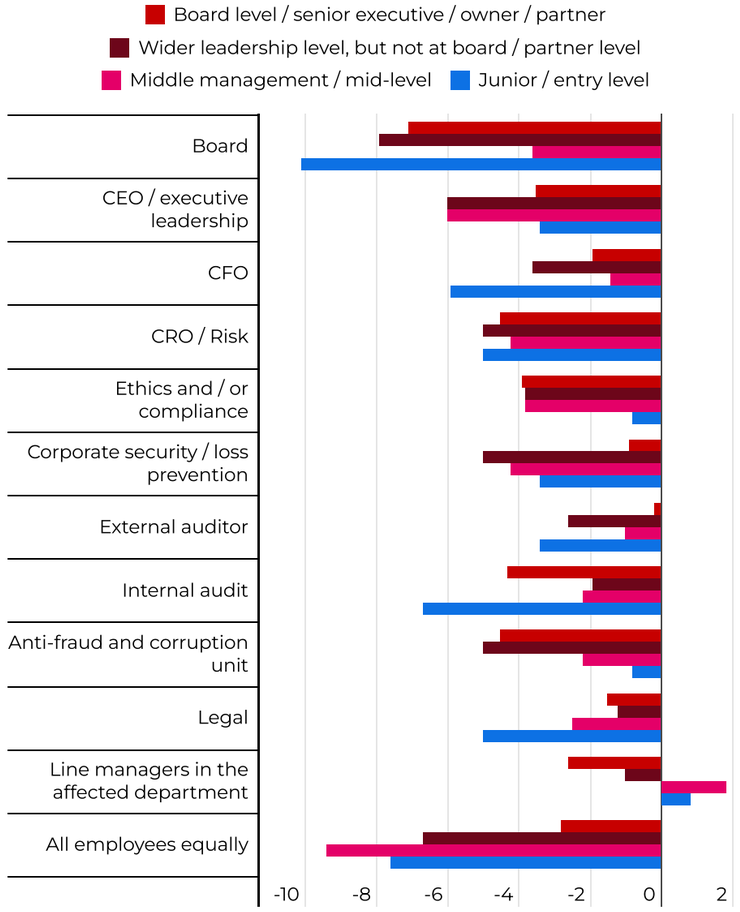
Breaking the FOFO cycle requires institutionalising curiosity: making fraud a standing agenda item normalises uncomfortable questions, rotating audit committee chairs prevents regulatory capture, and mandating external fraud assessments surfaces issues internal teams may have overlooked.

## Professionals reveal deep misalignments

Figures 5.2, 5.3, and 5.4 illustrate the misalignments between current and desired accountability across seniority, functions and professions. The board and C-suite show the most significant gaps, especially in risk management and cybersecurity. This suggests either fundamental misunderstanding or deliberate de-prioritisation of fraud risk at the highest levels.

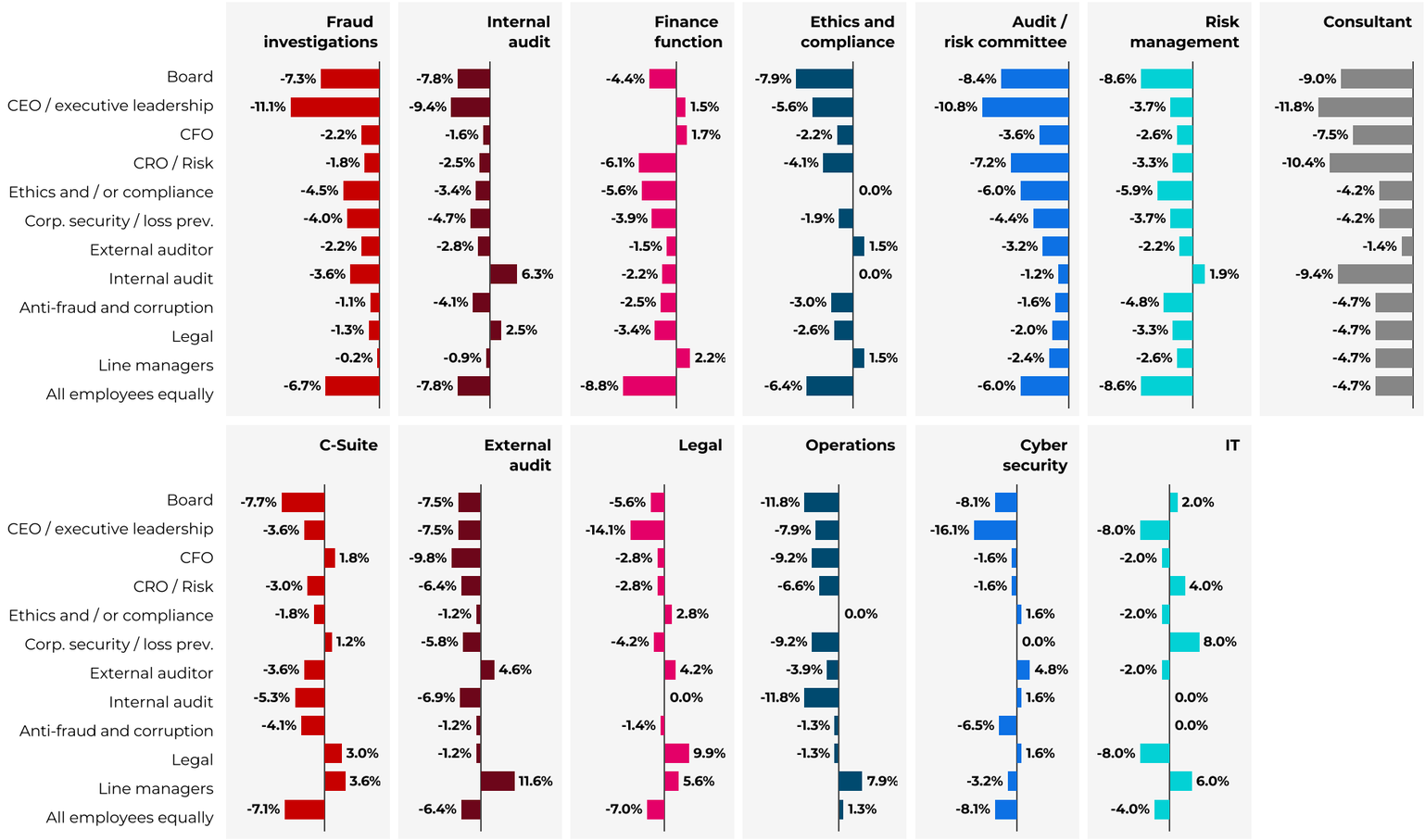
Professional body perspectives are also telling: Airmic shows the greatest misalignment for board and CEO accountability, suggesting deep dissatisfaction with leadership among risk professionals. ACCA aligns best with CFO roles, while ACi aligns with external auditor functions.

## Figure 5.2 **Misalignment persists across levels**



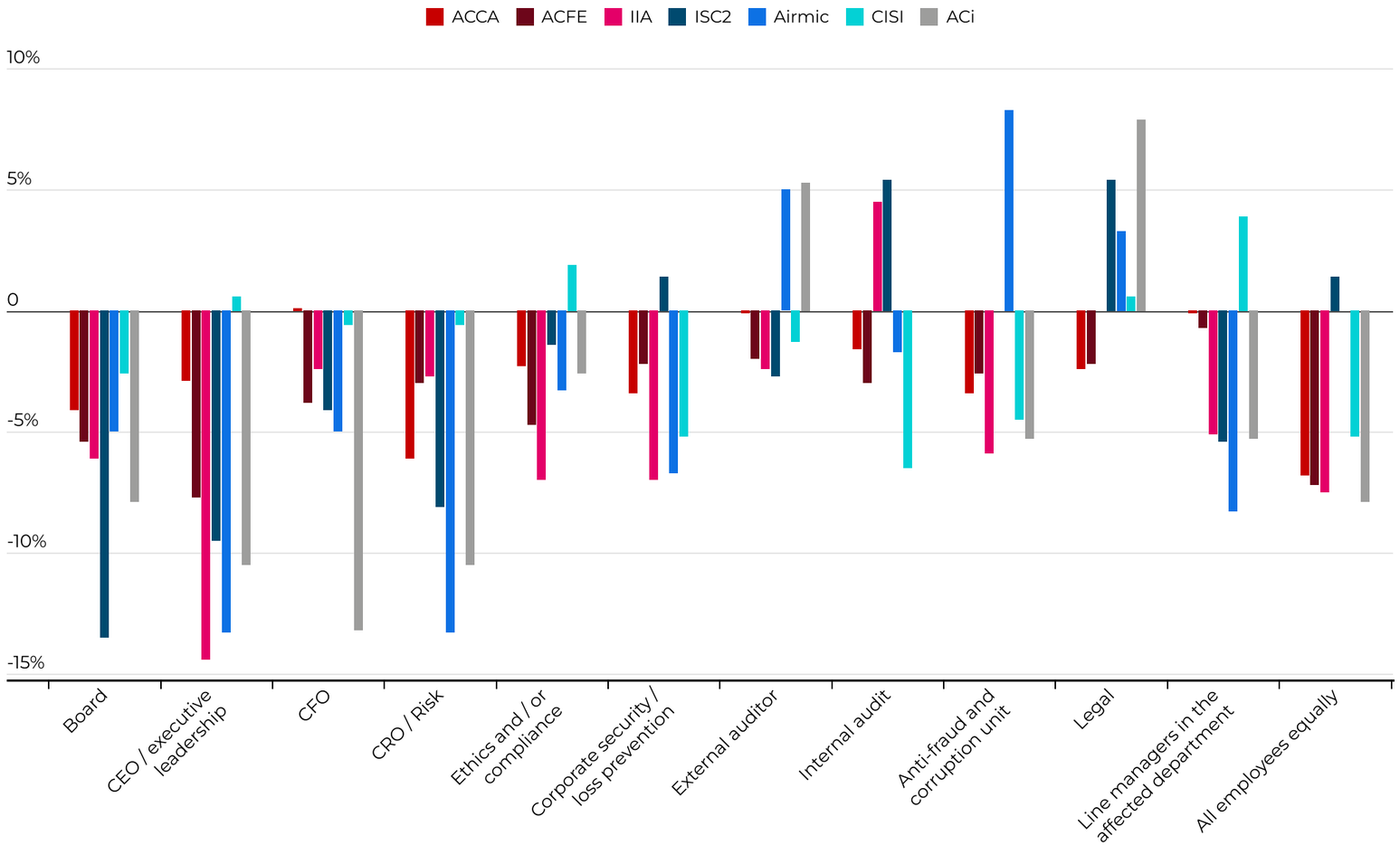

**Note:** Current vs. expected responses for fraud oversight diverges sharply.

## Figure 5.3 **Accountability misalignments are widespread – but most pronounced at the top**




**Note:** Boards and executives fall furthest behind expectations for fraud accountability.

Figure 5.4 **How different professions view fraud ownership — and where gaps persist**




**Note:** Professionals disagree on who should own fraud, revealing fractured accountability.

The question of who owns fraud risk appetite – particularly the CRO-CFO relationship in operationalising it – remains contentious (see Airmic's commentary). This operationalisation challenge – moving risk appetite from board statement to decision-making tool – fundamentally shapes whether fraud signals become action or noise.

Most concerning is the consistent under-resourcing of training across all functions, highlighted by negative alignment values throughout. Education and awareness remain chronically under-prioritised despite being universally recognised as essential for fraud prevention.

## Audit committees without substance

Audit committees represent the board's intended sharp edge for fraud oversight, yet roundtables revealed they often lack focus, frequency and depth.

**'What assurance does the audit committee give you? They meet infrequently, and when fraud exposures are presented, you get five minutes. Then it's on to the next item.'**

Participant in the UK

Many committees confine themselves to narrow financial reviews rather than serving as the board's conscience on fraud. They tick boxes rather than asking what organisations are losing – directly, indirectly, and culturally.

**'The most sought-after board members are those who sign everything and ask nothing.'**

Risk manager in the Middle East

Practical improvements for providing more meaningful oversight:

- Requiring fraud cost–benefit analysis in committee papers, showing savings from prevention as well as comparing cost-cutting savings with accumulative losses due to fraud
- Commissioning root cause reviews after fraud incidents, not just case closures
- Challenging whether risk assessments reflect behavioural vulnerabilities and not just control gaps.

Several roundtable participants advocated for 'active assurance' – deploying ethical hackers or simulated customers to test whether fraud defences and due diligence processes work in practice.

This approach, widely used in cybersecurity as red teaming, is now being adapted for financial crime prevention.[11] Banks and regulators already use mystery 'shoppers' to check compliance with KYC and fair-lending rules; extending this to fraud and credit-risk controls could uncover blind spots before criminals exploit them.

## Who owns data for fraud?

### We consistently heard leaders ask, 'How do we value data, so people look after it?'

When it comes to fraud, accountability fails when data ownership is nobody's job. A pragmatic split emerged in our forums:

- **Board/audit committee** – demands decision ready reporting on data risks (lineage, quality, use), not just IT status.
- **COO** – owns operational data readiness for fraud controls (join keys, access, reconciliation, retention).
- **CFO** – treats data as a financial control surface: valuation assumptions, reporting data, and model inputs must be auditable.
- **CDO/CIO** – stewards' architecture, lineage, access, and model registries; certifies data quality thresholds for fraud analytics.

Clarifying fraud-related data ownership through a RACI matrix helps accelerate triage and move governance from theory to practice — turning data into a first-line fraud control rather than a back-office afterthought.

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

11 In cybersecurity, red teaming involves the use of 'ethical hackers'.

## The expertise and independence deficit

Survey results on ease of reporting confirm this credibility gap: financial services respondents scored relatively high on reporting confidence, but public sector and professional services showed far lower trust. This suggests committees in some sectors lack the authority and expertise to provide meaningful oversight.

Many audit committee members lack training beyond financial reporting basics, with some senior board members still equating fraud with petty theft while overlooking procurement, cyber and ESG risks. As one South Asia board member participant explained: *'Maybe a stronger line to the audit and risk chair, and a dotted line to the CFO because in one of the cases I had, it was the CFO that was the problem.'*

Committees must strengthen their independence and equip themselves with external forensic support, especially when internal functions are conflicted. As one board committee member in the United Arab Emirates (UAE) explained: *'The Securities and Commodities Authority has introduced requirements for external independent board evaluations. Every listed entity must now meet benchmarks for how the board performs their fiduciary duties. This kind of regulatory mandate helps ensure boards actually understand their oversight responsibilities, not just sign documents.'*

Participants noted that some corporate governance codes call out fraud duties explicitly, while others rely on 'best practice', leaving enforceability gaps. In our Calls to Action, we recommend board charters and committee terms of reference to name fraud explicitly.

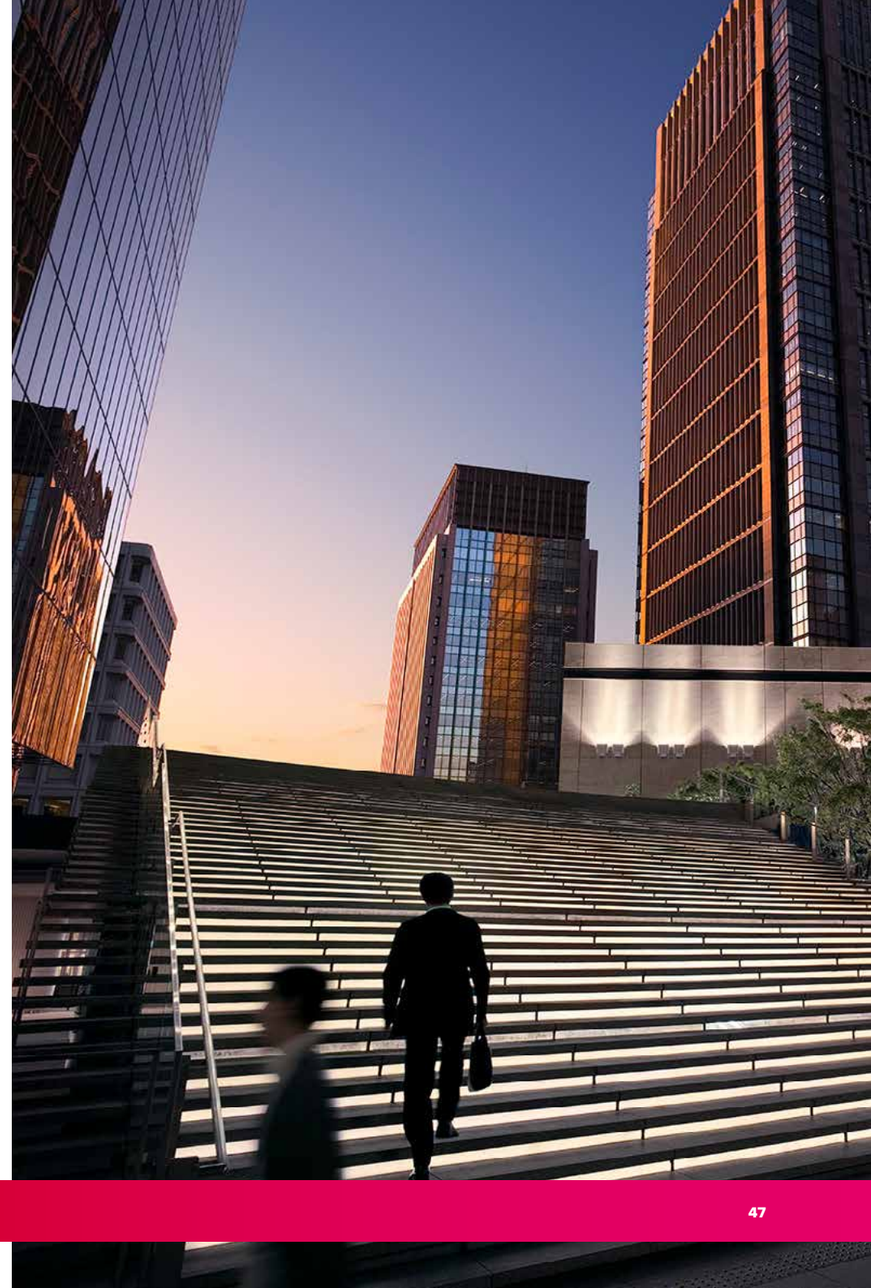
## Accountants can transform board understanding

Accountants and auditors provide the critical link between fraud risk and board comprehension, yet respondents across sectors described reporting as overwhelming rather than enlightening.

**'I get 5,678 policy documents, but I don't have time to go through them. I need the data that tells me what's really happening, what's missing, and what decision you need from me.'**

European board member

This highlights an urgent need for all our professions to provide concise, decision-oriented analysis rather than voluminous compliance reports. The principle of *'true and fair'* must extend beyond numerical accuracy to include integrity in context. If boards only hear only about confirmed fraud cases, it's already too late. They need early warning signals of unethical behaviour, gaps in consequence management, and cultural drivers of misconduct. See our *Risk Culture* podcast series episode exploring how the *'true and fair'* requirement can help directors understand the full story of an organisation's risk profile.



## Fixing the silo cracks

A recurring problem is that fraud data (risk data in general) often sits fragmented across departments: compliance logs cases, cyber teams track incidents, procurement holds vendor red flags, finance sees anomalies, but these datasets rarely integrate. Breaking down these silos requires not only data integration but also embedding investigative thinking into risk assessment from the outset, rather than deploying investigation only after incidents occur.

**'Fraud thrives in the gaps. We had three departments with pieces of the same puzzle, but no one put them together until it was too late.'**

US healthcare head of internal audit

**'It's the decentralisation that makes fraud easy… nothing centralised, including whistleblowing platforms and information sharing about them.'**

Participant in Malaysia

Resilient organisations treat fraud data as an enterprise resource, not departmental property. Boards should require cross-functional fraud reporting where information flows seamlessly across compliance, risk, audit and finance functions.

**'Identification of fraud is one thing. Then what happens? Because who cares about identifying if you're not going to do something about it. We don't want processes. We want impact and effectiveness.'**

CRO participant in Europe

In practice, fraud risk amplifies not only because of divided ownership but because cross-functional issues take longer to escalate than single function risks – the time delay between detection and decision is the real governance vulnerability.

## Cultural context shapes accountability

Culture profoundly influences how accountability operates. In Asia-Pacific, raising concerns can be viewed as disloyalty, undermining whistleblowing frameworks. In Africa, weak consequence management requires both carrots and sticks, rewarding staff who raise concerns while penalising misconduct. In Europe, fraud definitions are expanding to include behaviours that are legal but unethical, such as misusing customer data.

Accountability cannot be copy-pasted across cultures. Governance structures must adapt to local realities while maintaining universal principles of transparency and consequence.

Our data reveals clear stakes: where governance is transparent and committees are active, confidence is higher and losses are lower. Where ownership is blurred, fraud becomes normalised and easier to commit. Boards and audit committees must own accountability, accountants must present complete pictures that go beyond compliance, and organisations must break down silos that allow fraud to thrive in the gaps.

**'Ask all directors the scope of these ethics policies. How group-wide are they? Whistleblowing lines are not group-wide unless you've made them so.'**

Tina Mavraki, FTSE 100 board director and member of ACCA's risk culture special interest group

See Figures 5.5 and 5.6 for the factors that shape willingness to report and how confidence varies by organisation type and leadership culture — closing the loop between perception ('who owns fraud?') and outcome ('do people feel safe to report?').

**'Structural supports and cultural levers matter most: leadership commitment and shared accountability lift confidence, while weak controls and limited awareness shut it down.'**

## Figure 5.5 **What raises or lowers employees' willingness to report suspected fraud? Leadership and protections matter most**

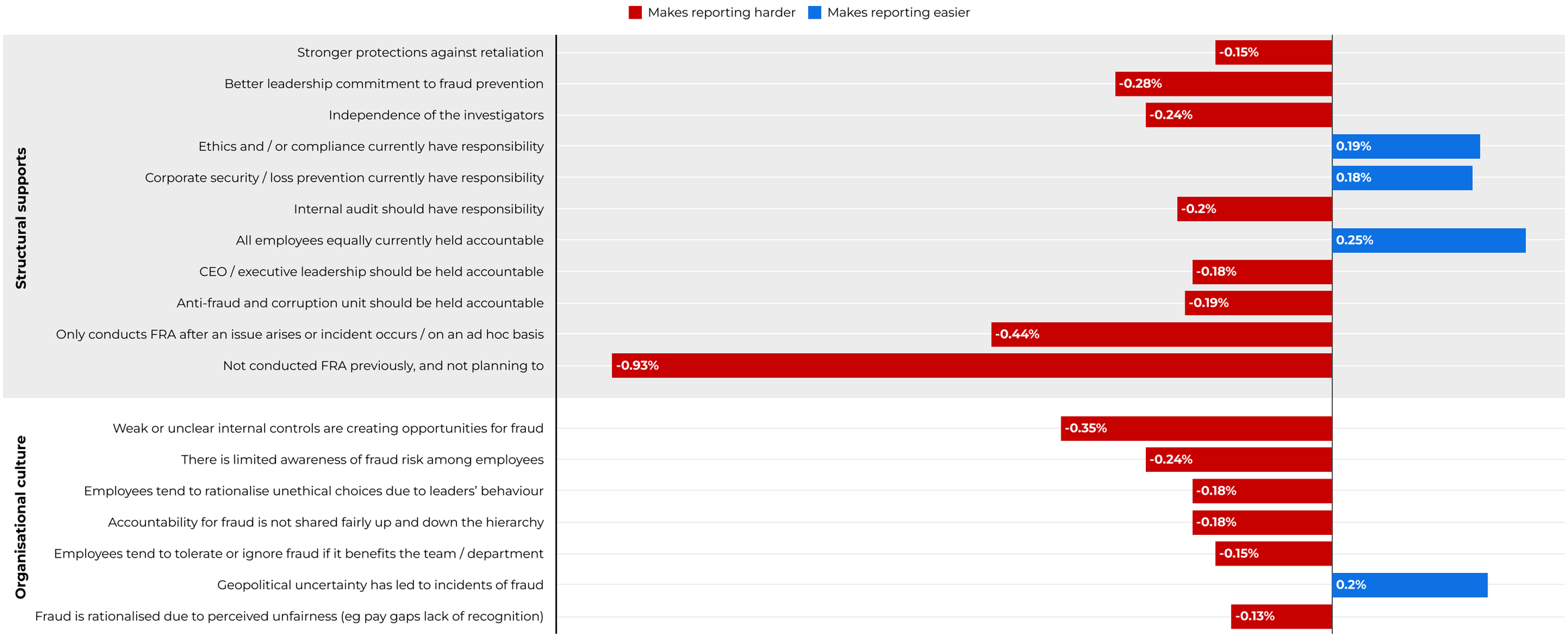
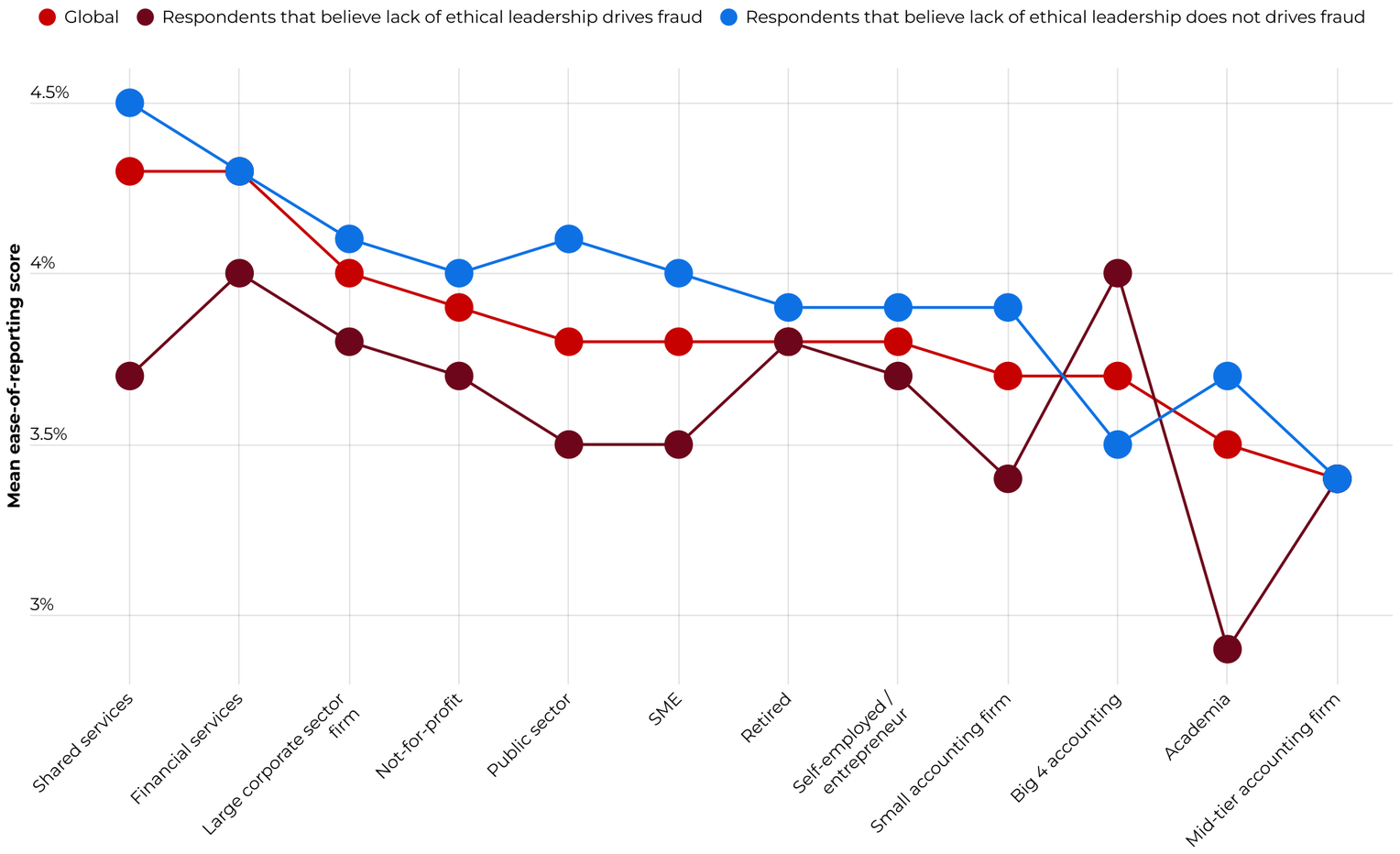


Figure 5.6 **Who feels least able to report? By sector**




**'Reporting confidence is structurally uneven. It is lowest in SMEs and smaller firms and drops even lower in organisations that lack strong ethical leadership.'**

## Key takeaways

### Are your governance structures creating real accountability or just shuffling responsibility?

Does your board truly own fraud oversight, or is it delegated down while authority remains fragmented? Audit whether your committees have the expertise, independence, and time to provide meaningful oversight while adapting to local cultural contexts. Assess if your reporting gives boards decision-ready intelligence rather than compliance volumes, determine if fraud data flows across functions or remains siloed, and evaluate whether accountability frameworks are proactive rather than reactive. The fundamental question is whether your governance prevents misconduct before it occurs or creates gaps where fraud thrives.

## Ownership cracks and how to pin them

**Fraud thrives in ambiguity.**
**When roles blur, accountability collapses.**

Our research shows how the four lines model offers clarity: first line owns operations, second line ethics and risk, third line assurance, and a fourth line – the board – that tests independence and demands decision-ready reporting. This isn't ceremonial oversight; it means asking uncomfortable questions early, not after losses mount.

One audit chair told us candidly:

**'We removed the word 'material' from our terms of reference because you can't know if it's material until you investigate.'**

That change licensed earlier, bolder inquiry. Ownership must also stretch beyond the entity. Fraud seeps through value chains, so boards should embed shared standards with partners before contracts are signed, not wave audit rights after the fact. As one board-level survey respondent warned:

**'If you don't make collaboration visible and measurable, you're just hoping for integrity.'**

If fraud isn't in KPIs, budgets, and partner standards, accountability remains theory – and fraud remains inevitable.

## A new era of accountability

On 1 September 2025, the UK's failure-to-prevent fraud offence under the Economic Crime and Corporate Transparency Act (ECCTA) changed the rules. Large organisations now face criminal liability and if an associated person commits fraud for their benefit – unless they can prove 'reasonable prevention procedures'. This reform moves fraud prevention from best practice to legal obligation, forcing boards to act. A UK risk executive put it plainly:

**'If you only count the frauds that happened, you miss the savings from the frauds that didn't.'**

Global reactions reveal cultural fault lines.

A US participant said:

**'That would never fly here. We don't hold boards criminally responsible in the same way.'**

Others called ECCTA a wake-up call:

**'It's not about compliance theatre anymore – it's about survival.'**

Boards must embed fraud prevention into governance and publish proof of action. Failure isn't just reputational – it's criminal. Prevention is now the price of credibility.[12]

12 UK Government Guidance (2025) – *Economic Crime and Corporate Transparency Act 2023: Failure to Prevent Fraud Guidance*.

## Board and committees – proactive governance

**Fraud is not a compliance footnote; it is a strategic risk that boards cannot delegate away.**

Yet our research shows audit committees often tick boxes rather than interrogate reality. One audit committee member from the UK reflected candidly:

**'We suffered a major fraud and didn't use internal audit – they were either complicit or under-resourced. We had to hire external investigators.'**

Good governance looks different: fraud appears as a standing agenda item, committees demand residual-risk narratives, and boards rehearse crisis playbooks for Friday-night fraud events. Capability matters too.

As another participant put it:

**'For £20,000 a year to kick up a fuss on 600 pages of audit reports... do you see how it's misaligned?'**

Independence must be real: committees need external forensic support when internal functions are conflicted. Investors and regulators are raising the bar, demanding transparency on fraud prevention alongside ESG metrics. Boards that lead with curiosity and consequence management will earn trust. Those that sign everything and ask nothing will remain fraud's easiest targets.

Voices from the coalition – IIA

# Internal audit – a strategic partner in fraud prevention

## Bridge the siloes

A recurring message in ACCA's coalition survey and roundtables is that fraud prevention cannot be the sole responsibility of any single function, including internal audit. The IIA promotes collaborating with stakeholders across the organisation. Standard 11.1 Building Relationships and Communicating with Stakeholders states, *'The chief audit executive must develop an approach for the internal audit function to build relationships and trust with key stakeholders, including the board, senior management, operational management, regulators, and internal and external assurance providers and other consultants.'*[13]

**'Organisations should set up task forces that involve people from multiple departments offering their perspectives on what is or isn't working, what needs to change and where there are opportunities for improvement.'**

Benito Ybarra, EVP of global standards, guidance and certifications at The IIA

## Adopt proactive mindset

Many organisations are largely reactive, dealing with fraud after it is revealed rather than actively seeking out fraud risks. The internal audit function is well positioned to be a strategic partner in combatting fraud.

When internal auditors are identifying the risks to review in an engagement, they must consider *'specific risks related to fraud'*. (Standard 13.2 Engagement Risk Assessments) Internal auditors can consider fraud risks by conducting a fraud workshop. Once they understand the processes of the area or activity under review, internal auditors can brainstorm to identify where people may try to circumvent controls and commit fraudulent acts. The workshop helps auditors apply a fraud lens to identify strengths and weaknesses in a manner similar to exercises for the consideration of inherent and residual risks.

Additionally, fraud workshops can be expanded to look at the organisation's entire risk landscape. Larger organisations with internal auditors dedicated to IT, finance and operations will find value in bringing internal auditors from these disciplines into a fraud brainstorming meeting, where exchanging expertise is likely to enhance the identification of fraud schemes.

If IT auditors know about a weakness that allows management to override controls in a system and operations auditors know about a lack of management oversight (such as approvals), opportunities for fraud become clearer.

## Integrate technology and data analytics

The IIA's Global Practice Guide, *Internal Auditing Competency Framework*, which is publicly accessible and available in multiple languages, outlines data analytics as a key professional competency for internal auditors. In the fight against fraud, data analytics can be leveraged to support collaboration and proactive efforts. Collaborating to incorporate data available across the organisation can reveal areas with increased fraud risks, enabling internal auditors to focus their efforts on these areas.

## Strengthen fraud awareness and training

Fraud falls under the governance and risk management area of the *Internal Auditing Competency Framework*. Internal audit leaders should offer opportunities for fraud risk training and awareness. In addition, the Certified Internal Auditor exam syllabus covers fraud in various aspects. Obtaining the certification demonstrates awareness of fraud, and the certification's

13 The Institute of Internal Auditors leads and supports the internal audit profession globally and stands at a critical juncture in the fight against fraud. The 2024 Global Internal Audit Standards™ provide valuable insight that can be applied to combating fraud. Institute of Internal Auditors (2024) – *Global Internal Audit Standards™*.

requirement for continuing professional education makes ongoing training essential. Increased fraud awareness helps the internal audit function fulfil its role as a premier fraud-fighting partner. Ybarra explains:

**'It's important that internal auditors are aware of the fraud risks that exist in their organisations. The broad and deep knowledge that internal auditors develop and maintain helps position them as strategic advisors and business leaders of organisations.'**

## Clarify roles in fraud investigation

Chief audit executives should ensure that internal audit charters outline the roles and responsibilities the internal audit function will take on related to fraud, including reporting to the board, performing cross-functional engagements and reporting on fraud risks in individual engagements. During assurance and advisory engagements, internal auditors should consider the probability of fraud. Standard 4.2 Due Professional Care states, *'Internal auditors must exercise due professional care by assessing the nature, circumstances and requirements of the services to be provided including: ...Probability of significant errors, fraud, noncompliance and other risks that might affect objectives, operations or resources.'*

With a high need for competencies focused on data analysis and fraud, internal auditors are committed to continuous professional development within these areas. Ybarra concludes:

**'The ability to leverage strengths and work toward common outcomes is a skill that assurance providers can continually improve. This landmark study is an example of the power of working together to advance and serve the public interest.'**

## What internal audit can learn

The coalition research identifies opportunities for improvement. First, embrace collaboration and avoid isolation – fraud prevention encourages partnerships with risk, compliance, HR, IT, and specialised investigators. Second, advocate for adequate resourcing and clear boundaries to prevent role conflicts. Third, invest in forensic skills and data analytics to complement traditional audit competencies. Fourth, maintain professional scepticism and resist checklist-driven approaches that reduce judgement. Finally, support transparent speak-up cultures whilst recognising that changing organisational culture extends beyond internal audit's mandate.

Internal audit's value is highest when it acts as strategic partner rather than default fraud owner. By building cross-functional relationships, integrating fraud risk into all engagements, leveraging technology and analytics, and continuously developing specialised capabilities, internal audit can fulfil its essential role in the anti-fraud ecosystem – not as a siloed function overburdened by default, but as an independent, collaborative force for organisational resilience.

The ability to leverage strengths and work towards common outcomes distinguishes mature organisations. This coalition study exemplifies the power of working together to advance the public interest.

# 6. Understanding the drivers – why fraud becomes inevitable

**Understanding what fraud looks like and how accountability fails tells half of the story. While rapid technology advancements and economic stress dominate, our research points to one uncomfortable truth – lack of ethical leadership emerges as the most powerful cultural amplifier of fraud, ranking first in certain regions, sectors and demographics.**

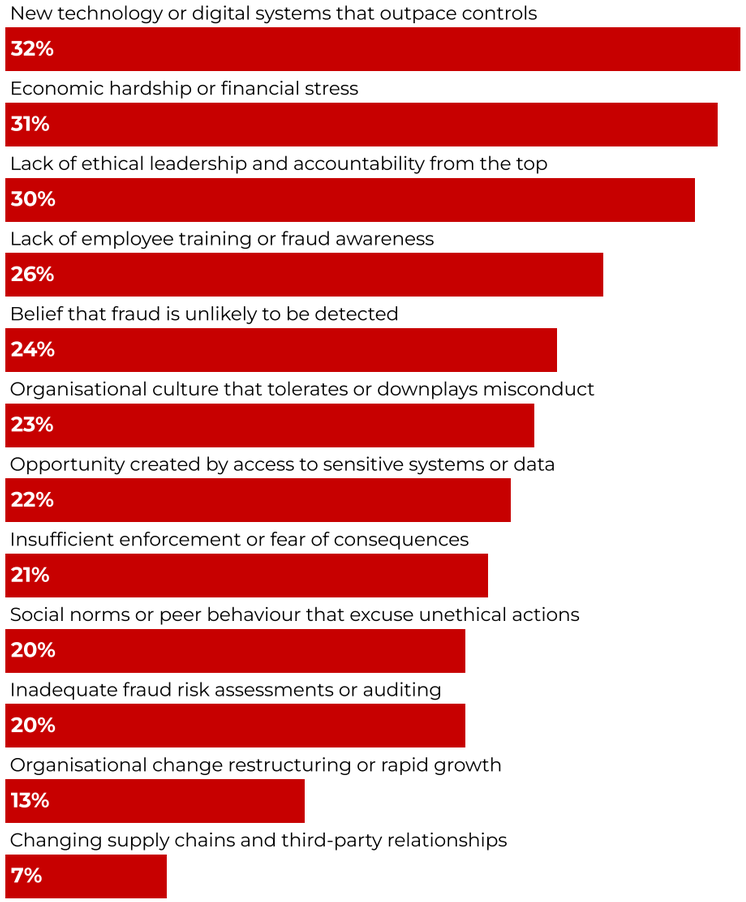
## Demographics reveal hidden patterns

Respondents identify 'new technology outpacing controls', 'economic stress', and 'lack of ethical leadership and accountability' as the main drivers of fraud (Figure 6.1), alongside day-to-day symptoms: weak/unclear controls, limited awareness and unfairly shared accountability, with employees rationalising misconduct where leaders' behaviour suggests it is tolerated.

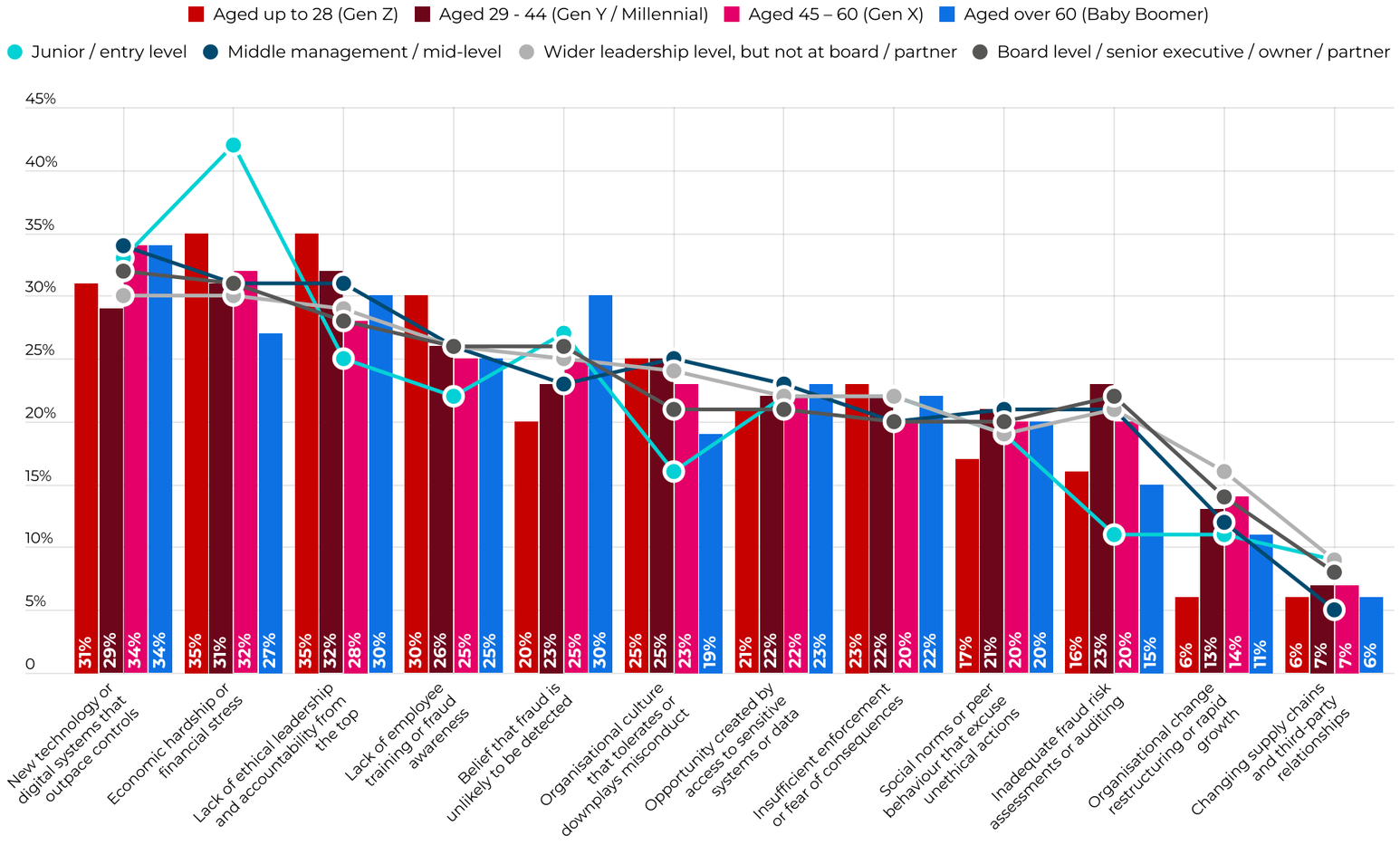
Figure 6.2 illustrates how the main differences in driver rankings seniority-wise lies with the junior and entry level respondents, showing profound differences across generations, and Figure 6.3 across regions. Social norms, peer behaviour and leadership accountability can either drive or deter fraud and these factors vary widely across both regions and generations.

These nuances matter because they explain why prevention strategies often miss the mark. What looks like a comprehensive approach to leadership may address only one demographic's understanding of the problem.

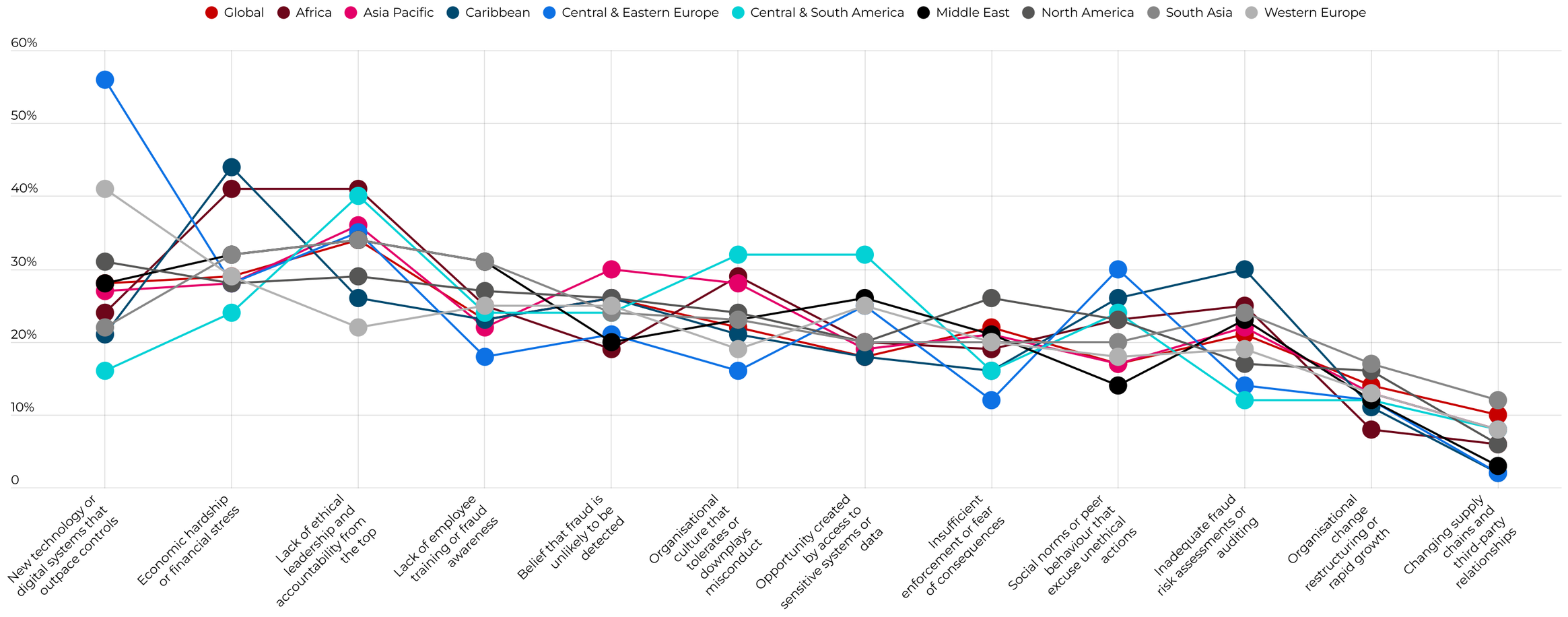
## Figure 6.1 **New tech, economic stress, and weak leadership lead the global fraud drivers**




## Figure 6.2 **Generational and seniority patterns diverge, converging on one finding: leadership tone modulates rationalisation**



## Figure 6.3 **Top fraud drivers – differences across regions**

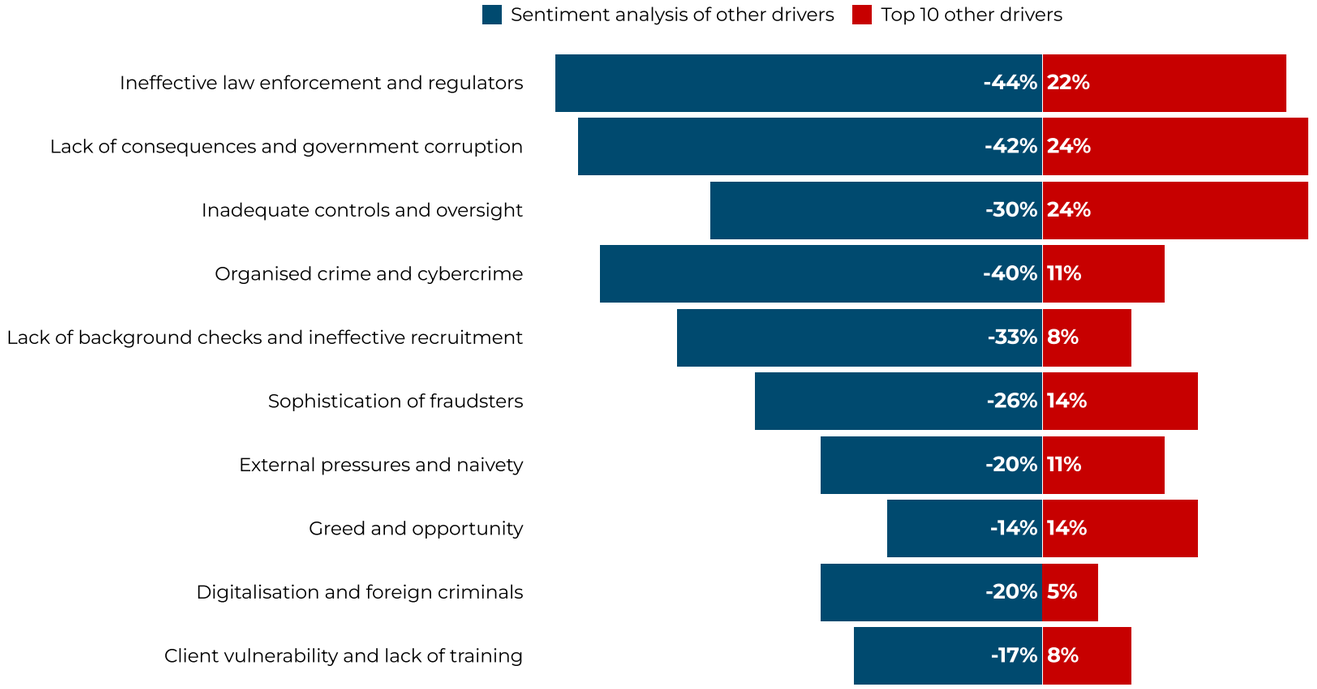


Company size also creates predictable blind spots in fraud driver perception. SMEs (under 250 employees) recognise enforcement gaps and inadequate risk assessments as major drivers, suggesting they're large enough to experience fraud but lack enterprise-level controls. Larger organisations (from 5,000+ employees upwards) paradoxically downplay ethical leadership deficits and employee training gaps as fraud drivers, despite having the scale where these factors become systemic risks. Most tellingly, the largest companies (20,000+ employees) recognise social norms that rationalise misconduct as significant drivers, acknowledging that at enterprise scale, cultural factors outweigh individual pressures.

Finally, in Figure 6.4, we see how the open-ended 'other' responses reflect the spectrum of different types of professionals identifying drivers ranging from 'lack of consequences and government corruption' to 'greed and opportunity' and 'ineffective law enforcement and regulators' to 'inadequate controls and oversight'.

Overall, the survey data and member engagement tell us that leadership is the decisive cultural driver where consequence management is weak, reporting is risky, or civic trust is low. In digitally mature regions and financial services-heavy contexts, technology and economic stress outrank leadership, but leadership still shapes how fast organisations close the hazard–remedy gap. The question of who sets ethical tone and how leadership accountability translates into operational behaviour is explored further in CISI's commentary.

Figure 6.4 **Top 10 other drivers of fraud and sentiment analysis**



## Mind the gaps

When boards and executives fail to model integrity or act decisively on known hazards, they create the conditions for misconduct to thrive. This is not a soft issue – it is a structural vulnerability that cascades through governance, culture, and control frameworks.

As one roundtable participant observed, the culture and ethics present in supervisory and executive boards shape the entire organisation's risk posture.

**'When leadership signals that ethics are negotiable – or avoids difficult conversations about fraud – controls fail silently.'**

Board advisor in Greece

*'Board directors have very broad coverage and yet they're expected to be experts in areas like fraud or cyber. Without clear processes and accountability, oversight becomes inconsistent and reactive,'* a board member respondent in the UK commented.

This leadership gap explains why survey respondents in some demographics ranked 'weak tone at the top' above 'economic stress' and 'technology outpacing controls' as the most significant fraud driver. The deeper question our research raises is why misconduct becomes inevitable in certain organisational environments. See our *Risk Culture* podcast episode *Who's Watching the Board?*, which explores why ethical leadership must go beyond compliance, and how boards can build moral muscle to think long-term and ask better questions about fraud threats and other risks they navigate today.

## What the data tells us

Our regression analysis cuts through conventional wisdom to reveal what truly drives fraud confidence and anxiety:

- **Weak consequence management** strongly correlates with low fraud confidence: if misconduct lacks real consequences, staff expect it to recur
- **Leadership trust** inversely correlates with fraud rationalisation – where trust in leadership is low, justifications for misconduct multiply
- **Integrated data and accountability** correlate with higher confidence –organisations that combine insights across functions perform better

This breakdown explains how the ease of reporting drops most sharply when internal controls are weak, awareness is low, and leaders appear inactive or rationalising misconduct. Assigning fraud to internal audit alone correlates with lower reporting confidence, whereas shared accountability correlates with higher confidence. These findings suggest that weak governance structures themselves become fraud drivers, failing to deter misconduct or send inconsistent leadership signals.

## Where cynicism breeds

As we pointed out before, fraud drivers extend far beyond the classic 'fraud triangle' of pressure, opportunity, and rationalisation.[14] The real engine room of misconduct lies in widespread cultural and governance failures that transform isolated risks into organisational inevitabilities.

**'We're not missing tools. We're missing intentionality and we're missing outcomes.'**

Respondent in the UK

Perhaps the most damaging discovery from our stepwise regression survey data analysis and roundtables was the hazard-remedy gap: organisations excel at identifying fraud threats – procurement risks, cyber threats, weak controls – but fail to provide effective remedies. The result isn't just exposure; it's active cynicism that becomes a fraud driver itself. A CRO in the US captured this perfectly:

**'We produce glossy risk registers, but when the fraud hits, we're still surprised. That gap between hazard and remedy is where the damage happens.'**

A CRO in the US

This gap reflects more than resource constraints; it represents governance inertia that actively undermines trust. When employees see risks being flagged repeatedly but never addressed, they conclude that fraud is noticed but tolerated and never fixed.

14 <https://www.accaglobal.com/gb/en/professional-insights/risk/risk-cultures-healthcare.html>

This conclusion itself becomes a powerful rationalisation for misconduct, for example, *'nothing happens anyway'*.

**'If you treat senior management differently... rationalisation sets in: *"my boss does it and gets away with it; why can't I?"*'**

Participant in Singapore

## Applying personas to drivers

Why the same organisation sees different drivers – our four personas also interpret drivers through distinctly different lenses, creating strategic blind spots:

- **Cynical Insiders** see fraud as systemic and blame leadership tone – they've witnessed the hazard-remedy gap firsthand and accept that 'controls are compromised'
- **Detached Observers** focus on external pressures like economic downturns, absolving internal culture and disengaged from reporting and prevention
- **Optimistic Practitioners** focus on 'a few bad apples' narrative, trust systems and miss enterprise-wide enablers, cultural and root-case factors
- **Overloaded Realists** recognise multiple drivers but feel under-resourced and powerless to address root causes.

When boards adopt optimistic executive perspectives while frontline managers observe widespread failures, prevention strategies inevitably misalign with reality. Prevention strategies must be tailored by persona – one-size-fits-all messaging misfires and breeds cynicism.

## Learning environments – the hidden modifier

Figure 6.5 shows that respondents from weak learning environments were significantly more likely to accept fraud rationalisations like 'everyone does it' or 'it's harmless if no one notices'. In strong learning environments – where mistakes were openly discussed and addressed-these rationalisations virtually disappeared.

Traditional fraud models consider individual moral failures, but our evidence points to systemic cultural breakdowns.

**'Fraud here is not only about personal greed. It is about survival, social obligation, and the absence of deterrence. If your environment rewards corruption, resisting it becomes an act of courage.'**

African roundtable participant

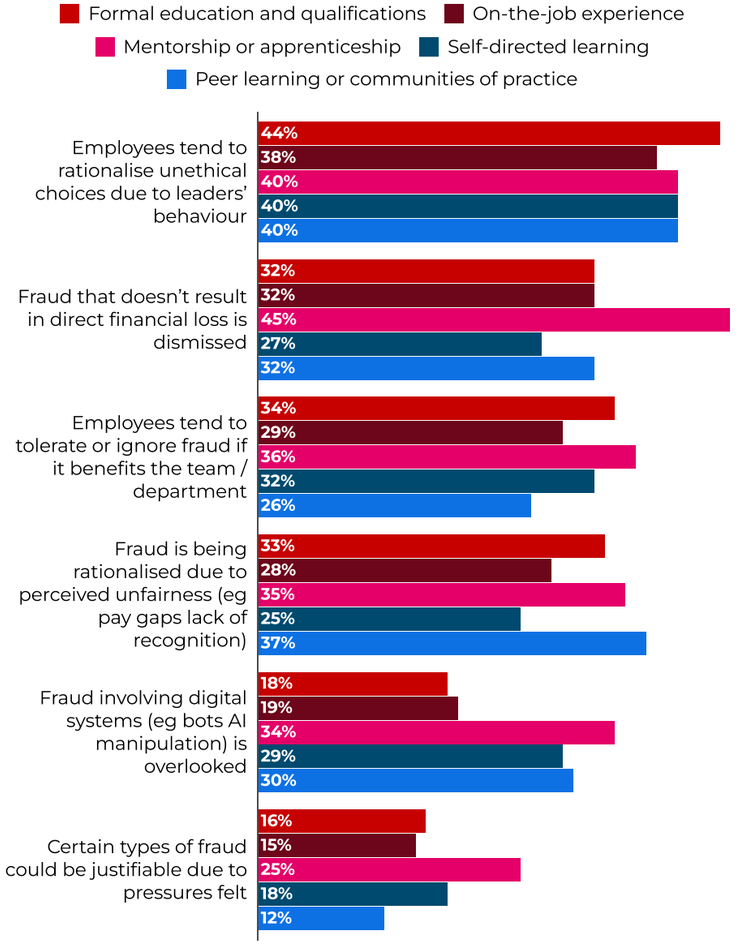
This represents a fundamental insight: rationalisations thrive in silence. Where employees feel unable to discuss mistakes or question behaviour, justifications for misconduct multiply.

**'If mistakes are punished but never discussed, people learn to cover up, not to correct.'**

Asia Pacific participant

Learning environments that encourage openness aren't 'soft culture' – they're hard fraud prevention.

Figure 6.5 **Learning environment vs rationalisation**



## The professionalisation of fraud

As discussed, modern fraud increasingly involves organised networks rather than lone actors.

**‘The fraudster today is not just the middle manager hiding invoices. It is a network using AI, crypto, and global supply chains to cover their tracks. It is industrialised; it is a lucrative business.’**

Risk leader

This professionalisation creates new driver categories: accessibility of advanced criminal tools, regulatory arbitrage across jurisdictions, and the lag in organisational adoption of equivalent defences.

Geopolitical instability emerges as a meta-driver: sanctions, supply chain disruptions, and conflict create conditions that amplify traditional pressures while obscuring oversight. Our analysis raises a fundamental challenge: if fraud becomes inevitable when certain organisational conditions align, prevention must focus on those conditions rather than just individual behaviours. This shifts the emphasis from compliance and controls to culture and governance – from catching bad actors to preventing the environments where misconduct thrives. See further analysis on geopolitical drivers in our *Calls to Action* supplement.

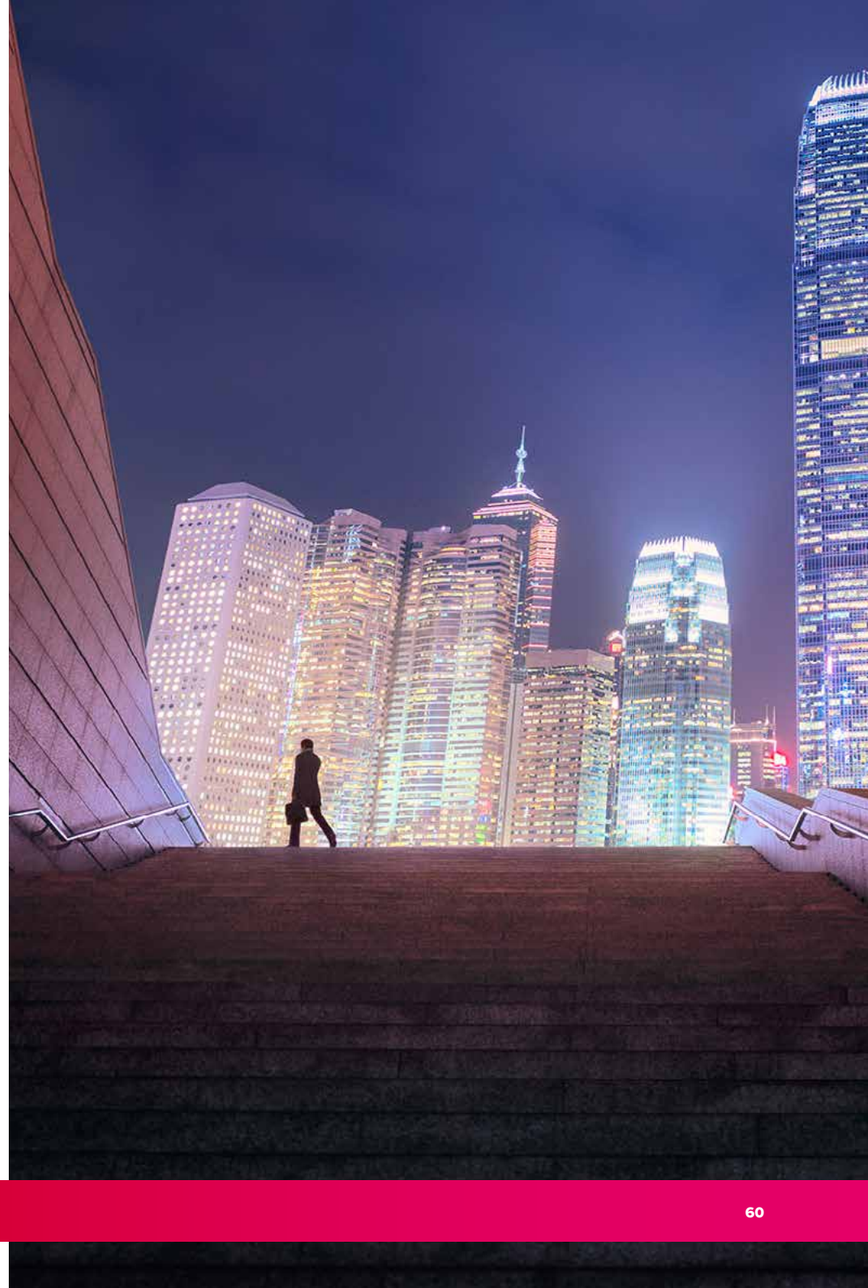
## What actually shifts outcomes?

- **Accountability clarity:** shared ownership – not internal audit alone – correlates with higher reporting confidence
- **Learning environment strength:** open discussion of mistakes dramatically reduces rationalisations (‘everyone does it’)
- **FRA maturity and cadence:** at-least-annual fraud risk assessments correlate with higher fraud-management maturity
- **Technology governance:** AI/cyber controls + behavioural analytics reduce both high-impact cyber shocks and slow-leak procurement losses

### Key takeaways

**Are you addressing fraud drivers or just their symptoms? Does your organisation identify hazards but struggle to implement remedies, creating the cynicism that becomes a driver itself?**

Assess whether prevention strategies account for how different personas perceive drivers differently, evaluate if your learning environment encourages openness or drives mistakes underground, and determine whether leadership signals about consequences are consistent and credible. The fundamental question is whether you’re treating fraud as individual moral failure or recognising the systemic conditions that make misconduct inevitable.



**Voices from the coalition – CISI**

# Ethical leadership as fraud's first defence

On the very day, Monday 1 September 2025, when we were digesting ACCA's coalition survey responses, experts from around the world were gathering in the leafy grounds of Jesus College Cambridge for the 42nd International Symposium on Economic Crime. This annual event draws some 2,000 of the best and brightest brains in this field for a week-long round-up of current developments. Meanwhile, on the same day, across the country in Britain's industrial heartland, Jaguar Land Rover was shuttering its factories after a devastating cyber-attack, which for weeks afterwards wreaked havoc across the firm's huge supply chain.

By the end of a month of widespread, global cyber-attacks, the UK government had bailed out the firm with a £1.5bn loan guarantee to help support its suppliers as the shutdown continued to halt production at the car maker and brought headaches and worse to the 100,000 workers across its supply chain. This risked the livelihood of 30,000 people directly employed at the company's UK plants and about 100,000 more working for firms in the supply chain.[15]

This served as a telling reminder that whilst traditional fraud remains a headache for many in business and finance, and the rest of society globally, cybercrime, both in its direct impact on the organisations targeted and more importantly in its wider systemic effects, is by far the most serious issue we face globally.

Our members emphasise ethical culture as crucial for fraud prevention, advocating a principles-based approach over rigid rules. This approach allows for flexibility in diverse business environments whilst maintaining a strong ethical foundation. A CISI speaker noted the challenge of embedding ethics across different cultures and partners, underscoring a preference for principles that align with organisational purpose rather than a strict rules-based system.

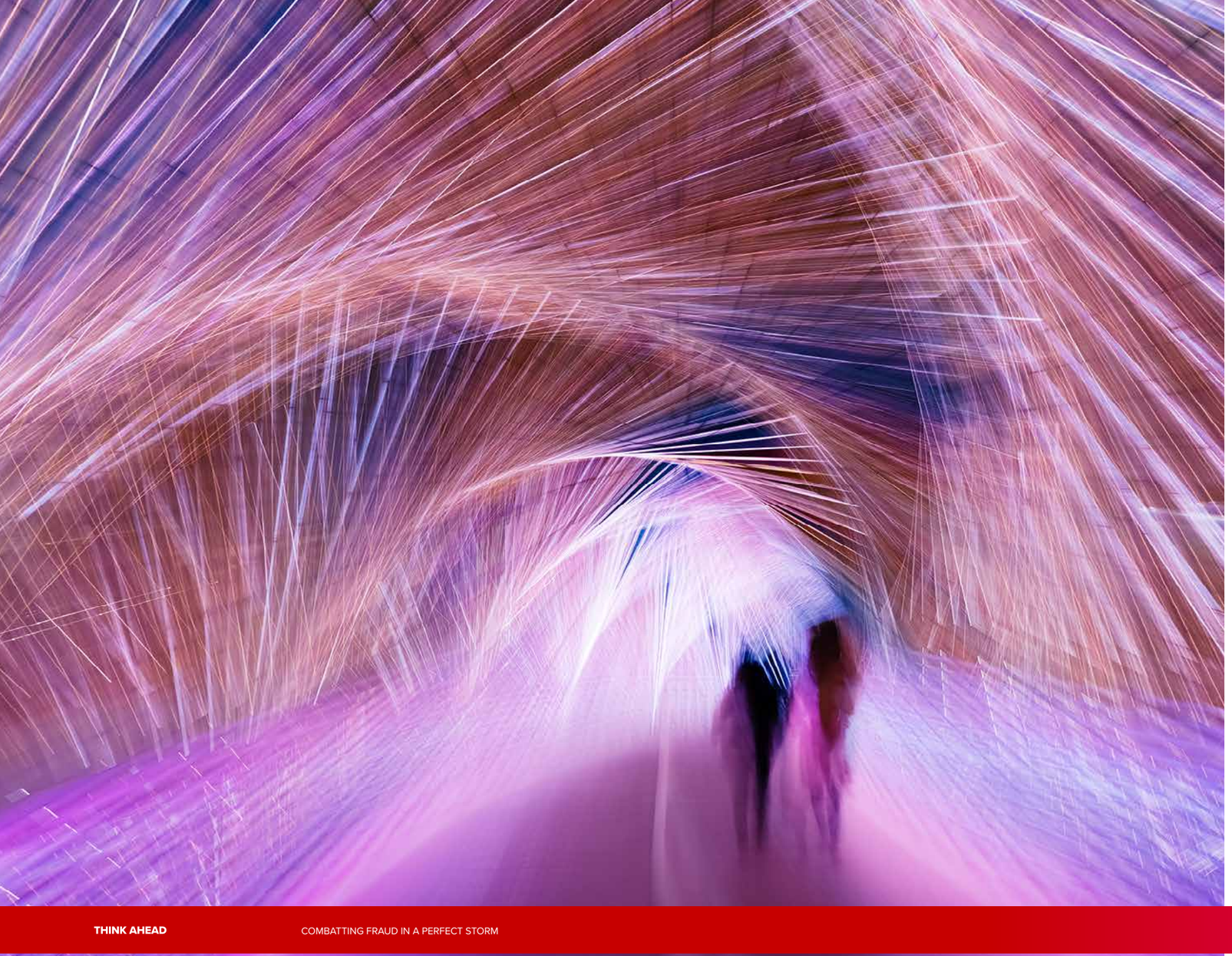
Whilst ACFE and IIA members cite weak internal controls as major fraud drivers (40% and 45% respectively), only 15% of CISI respondents share this view. Instead, CISI members consistently prioritise ethical culture, principles-based governance and leadership accountability as fraud's foundations. This isn't about downplaying controls – it's about recognising their limitations when culture fails.

Chris Stears, Chartered FCSI, of Edmund Group, a stalwart of the Cambridge symposium, is a recognised expert on conduct risk in financial crime, particularly through his co-authored work, Legal and Conduct Risk in the Financial Markets, with Professor Roger McCormick, formerly of London School of Economics. He emphasised that *'conduct risk is inseparable from culture. It stems not only from breaches of law but from everyday behaviours and decisions that, whilst perhaps technically compliant, fall short of ethical or professional standards; effective mitigation therefore depends less on controls alone than on embedding integrity and accountability into governance and board-level assurance'.*

This view aligns with CISI survey patterns, where members prioritised culture and leadership over technical controls as fraud's primary defence. Professor Michael Mainelli FCCA, an Honorary Chartered Fellow of the CISI and Lord Mayor of the City of London in 2024-25, in a seminal study on The Future Of UK Fraud: Challenging High-Volume, Automated Crime published in 2022 was prescient on issues of 'crumbling capacity in this arena: *'The UK and international environment grows increasingly fragile, with increasing cross-border frictions that permit increasing fraud. Social contracts between states and citizens have reached breaking points, and international relations have deteriorated so far that fraudsters operate cross-border with impunity.'*

What emerges most clearly from CISI's coalition participation is that ethical leadership isn't aspirational – it's operational. When boards model integrity consistently, rationalisation becomes harder to sustain. CISI members understand that in securities and investment, stakeholder trust depends on demonstrated integrity, not documented policies. This coalition research confirms that fraud prevention succeeds when governance expertise (CISI), investigative rigour (ACFE), control assurance (IIA), risk quantification (Airmic), and financial systems integrity (ACCA) work in concert. Leadership tone without control discipline creates aspiration without substance. Controls without ethical culture create compliance theatre without resilience.

15 *Financial Times* (2025) – Cyberattack on Jaguar Land Rover and systemic risk implications.



# 7. The triage trap – where fraud signals go to waste

**Triage means prioritising fraud alerts so action follows detection. Without it, organisations drown in signals while real threats slip through. This section explains why triage maturity – not detection volume – defines resilience.**

## When detection outpaces decision

Organisations are detecting more fraud signals than ever, but our survey reveals debilitating paradox – when reporting mechanisms improve, confidence that these signals lead to meaningful action more often erodes. This represents the critical missing link in fraud prevention – the ability to triage, prioritise and act on the avalanche of information that modern detection generates.

Figure 7.1 to 7.3 tell the story in numbers. Ease-of-reporting scores look reassuringly high across professional bodies. Ask whether those reports actually lead to action, and confidence collapses. ACCA and ACFE respondents report moderate-to-high ease; Airmic respondents score significantly lower – evidence that risk professionals see the structural cracks more clearly than their peers.

Figure 7.1 **Ease of reporting varies widely by sector and role (average, on a 1–5 scale)**

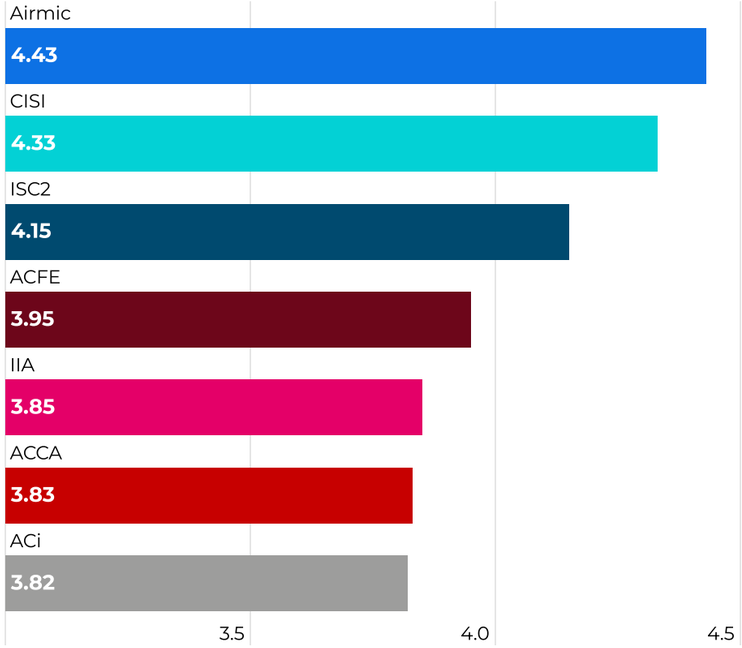
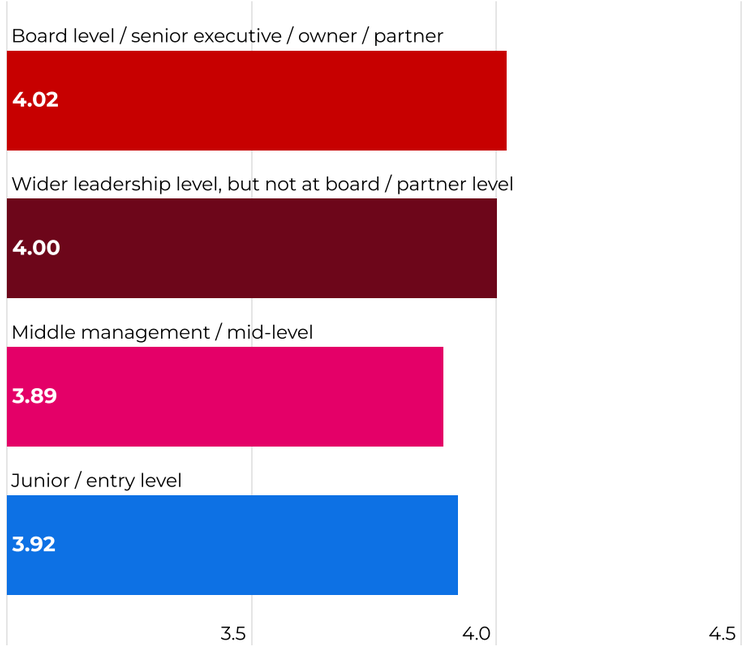



Figure 7.2 **Ease of reporting improves with seniority (average, on a 1–5 scale)**




This is what we mean by the triage trap: a system that drowns in alerts while missing the threats that matter. Detection capacity rises while triage capacity lags, creating bottlenecks where critical signals disappear into organisational noise.

When employees see risks flagged repeatedly but never addressed, they don't just lose confidence. They conclude that fraud is noticed but tolerated. That conclusion becomes its own rationalisation for misconduct.

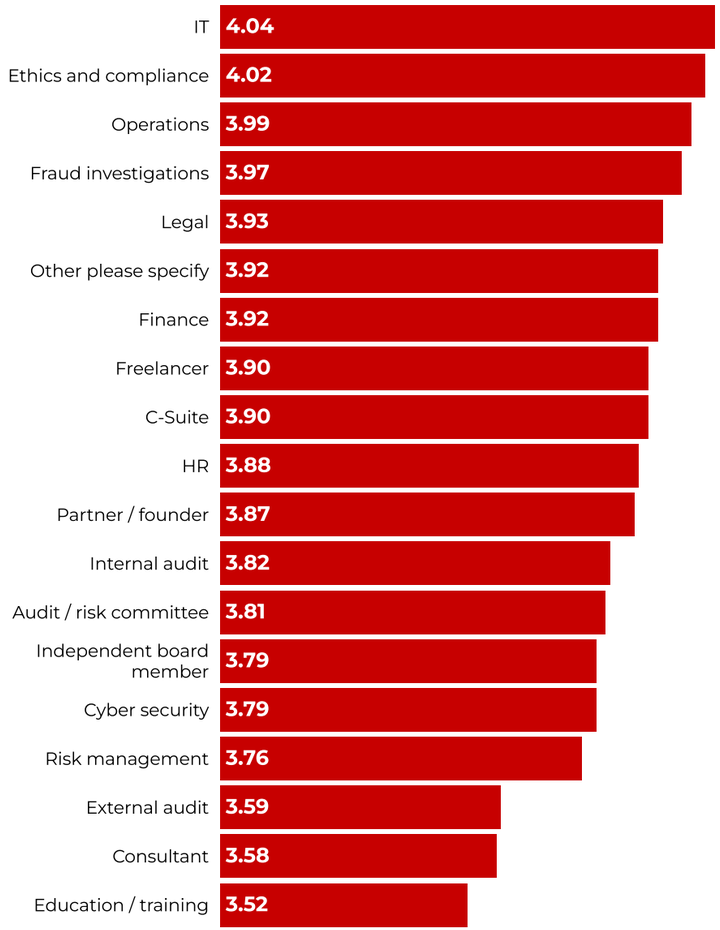
## The frontline blindspot

Figure 7.2 exposes a concerning asymmetry: reporting ease rises dramatically with seniority, while junior staff – closest to fraud signals – report lowest confidence. Financial services and shared services feel most enabled; mid-tier accounting firms, consultants, and external auditors skew neutral or unsure. Figure 7.3 reveals functional gaps: cybersecurity and risk teams report higher ease than finance and procurement teams, where fraud happens.

**'We need to help people understand what happens when they make a report. We need to humanise the whole process.'**

US roundtable participant

## Figure 7.3 **Ease of reporting fraud: by function (average, on a 1–5 scale)**




Crucially, prevalence doesn't predict ease of reporting. Internal frauds – expense claims, payroll manipulation, abuse of authority – are widely experienced but the hardest to report. Cultural and structural barriers don't just distort reporting; they strangle the entire triage process.

Compounding this problem, over one-third of respondents argued that fraud accountability sat in the 'wrong' organisational location, with compliance departments handling issues that belonged with business units. This ownership confusion muddles the entire triage process – when it's unclear who is responsible for acting on signals, those signals inevitably languish.

## Why triage feels broken: four perspectives

Behavioural monitoring represents an emerging frontier in fraud triage. By tracking patterns such as control overrides, reluctance to take leave, or unusual expense justifications, organisations can prioritise behavioural risks before they escalate into material incidents.

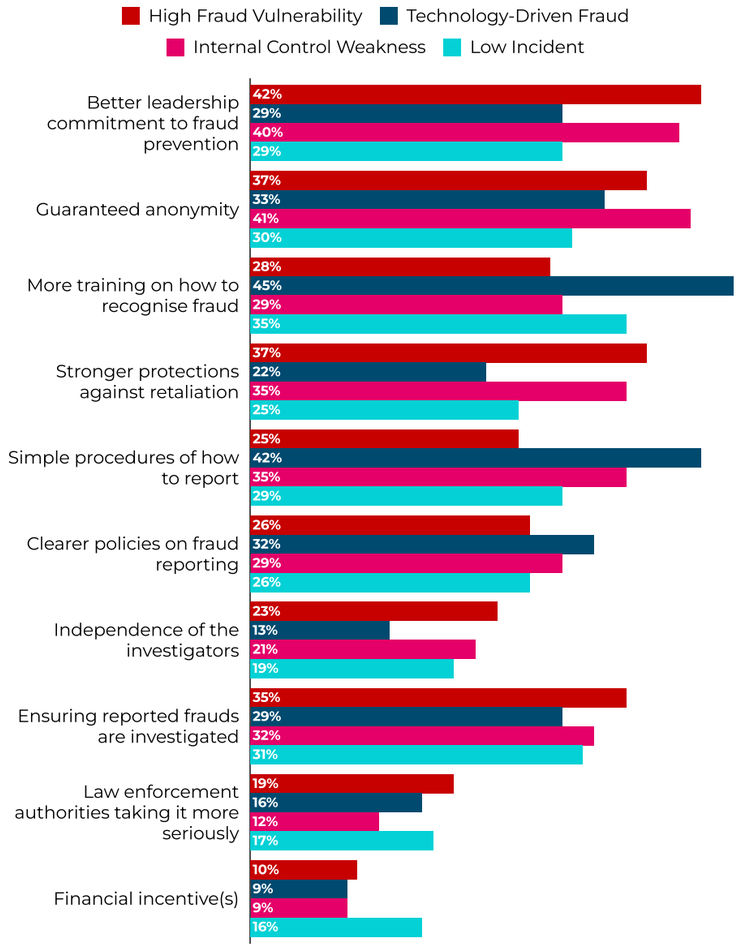
Figures 7.4 and 7.5 overlay our persona analysis, revealing how the same triage system produces four completely different realities:

- **Optimistic Practitioners** assume triage works and trust the process
- **Cynical Insiders** know it's broken and assume reports vanish or backfire
- **Overloaded Realists** see the signals but feel powerless to shift priorities
- **Detached Observers** don't engage because they think it's someone else's problem.

These aren't minor perception gaps. They're fractures that undermine the entire framework's credibility. Weak triage breeds disillusionment, which kills future reporting, which leaves fraud unaddressed, which proves the cynics right. When boards live in the optimistic view while frontline managers see the systemic failures, prevention strategies don't just misalign with reality – they become actively counterproductive.

## Figure 7.4 **Persona responses to triage (average, on a 1–5 scale)**

Figure 7.5 **Clusters differ in expectations and confidence**




## The data fragmentation problem

Even sophisticated organisations can't triage what they can't see whole. Fraud-relevant data sits fragmented across disconnected systems: procurement records in one platform, expense claims in another, HR flags in a third, whistleblowing reports managed separately by compliance or legal.

Triage decisions get made on incomplete pictures. As one European participant explained, the challenge isn't generating alerts – *'it's having the data architecture to know which alerts actually matter'.*

A Singapore-based bank learnt this the hard way. Their AI tool generated over 400 fraud alerts daily. Without triage rules, teams chased low-value anomalies while a US$2.5m procurement collusion scheme sailed through unnoticed. Technology accelerated detection without the governance to match. The result was chaos masquerading as resilience. See *Calls to Action* on data mapping.

## Regional variations in triage failure

Our roundtables also revealed how triage failures manifest differently across regions, but with universally damaging effects. In the Middle East, one participant described how *'procurement fraud is everywhere, but it looks so much like inefficiency that it never gets flagged. By the time someone realises, the money is lost.'* Africa echoed this with consequence-free environments: *'We can raise concerns, but there is no consequence management. Nothing happens. People stop speaking up.'*

The Asia-Pacific region highlighted technology overload: *'Our AI tool generates hundreds of alerts daily. The problem is deciding which are credible. Without triage, we either chase shadows or ignore real threats.'* Meanwhile, Europe focused on the speed mismatch: *'Cyber-enabled fraud is the only risk where I feel genuinely outpaced. Every time we adapt, the criminals adapt faster.'*

These voices highlight a shared reality: sophisticated detection systems are generating more signals than organisations can meaningfully process.

## Procurement: triage failure in slow motion

Several factors make procurement fraud exceptionally difficult to triage.

**Camouflage effect:** unlike cyberfraud, which generates sharp incident alerts, procurement fraud blends seamlessly into routine transactions, making it nearly invisible to standard triage systems.

**Cultural normalisation:** in some regions, minor kickbacks or inflated invoices have become normalised business practices, blurring the line between fraud and accepted inefficiency.

**Complexity chains:** fraud often hides in sub-contracting or third-party relationships where oversight is weakest and triage systems have limited visibility.

**Ownership confusion:** finance blames procurement, procurement blames compliance, and boards often dismiss it as operational noise rather than systematic risk.

When nobody clearly owns the decision about which procurement anomalies actually warrant escalation, signals just pile up. No action, no accountability, no resolution.

## Technology: accelerator or amplifier?

AI and analytics cut both ways. Some organisations use them effectively – clustering anomalies, helping human reviewers focus on what matters. Others discover that automation without judgment creates new problems.

**'The AI flags what's statistically unusual. It has no idea about business context. You still need people who understand how things actually work to make the call.'**

Technology can process signals at scale that humans never could, but triage still requires human judgment about context, materiality and organisational priorities. Without governance frameworks that translate algorithmic outputs into actual decisions, detection capacity becomes a liability, not an asset.

Behavioural monitoring – tracking override clusters, leave patterns, expense justifications – offers a way forward. Our cluster analysis shows different personas interpret these signals through completely different lenses, reinforcing why governance must integrate behavioural insight, not just technical alerts.

## What boards don't see

Most boards ask, *'how many fraud cases did we have?'* The smarter question would be *'how many red flags got ignored or mis-triaged?'*

Boards that actually understand triage demand dashboards showing what was reported, how it was prioritised, what actions followed. Not sanitised statistics about closed cases. Real visibility into where signals went to die. As Foss emphasised:

**'Fraud doesn't break at midday Monday. It hits Friday night when everyone's gone home. Do you have a playbook for that?'**

Bryan Foss, board director and co-founder of the Risk Coalition

That's the governance gap in one question. Boards get reassuring numbers about incidents that happened. They stay blind to the signals that were missed, buried, or ignored – the operational failure point where prevention collapses into theatre.

## Breaking the cycle

Mature organisations don't just process alerts. They close credibility loops – the 'nothing happens anyway' cynicism which undermines willingness to report. Staff need to know their concerns were considered, even if not escalated. That transparency about triage decisions – not the outcomes, but the process – is what sustains reporting confidence. The best organisations embed five disciplines:

- **Service-level agreements** that define time-to-triage and time-to-decision
- **Dashboards that show the workflow** – what was reported, prioritised, acted on
- **Feedback loops** that inform reporters of outcomes
- **Behavioural integration** combining anomaly detection with override patterns and leave anomalies
- **Residual-risk notes** published monthly, naming exposures, owners, deadlines

These aren't aspirational practices. They're the operating system that converts detection into decision. Section 8 shows how these elements integrate into fraud risk assessments that actually work – living tools, not compliance filing cabinets.

### Key takeaways

**Does your organisation generate more fraud alerts than it can process?**

Assess whether triage systems distinguish high-frequency/low-impact noise from low-frequency/high-impact threats, check if reporting ease drops at the frontline where signals emerge earliest, and confirm that accountability for acting on alerts is clear. Challenge your board: do they see dashboards of what was reported, prioritised, and acted on – or just sanitised case counts? The real question is whether detection capabilities are backed by triage maturity, or whether you're drowning in alerts while threats slip through.

# SME triage that works in practice

**SMEs face a hard reality: they experience fraud at rates comparable to larger entities but lack dedicated anti-fraud teams, sophisticated analytics, or deep specialist benches. Our survey shows confidence in fraud management declines as organisation size decreases, with mid-tier and small firms feeling least enabled to address fraud risks.**

Figure 7.6 illustrates how triage challenges intensify for smaller organisations: fewer staff to process alerts, limited technology, and roles that blur between operations and oversight.

But resource constraints don't mean accepting triage failure. SMEs have natural advantages that large corporates don't: proximity to operations, faster decision-making, and closer relationships. The key is building triage systems that exploit these strengths rather than mimicking enterprise approaches that don't scale down.

## Low-cost, high-impact triage

**Simple scoring systems:** You don't need AI to prioritise alerts. Create a basic scoring matrix: amount involved, control override (yes/no), internal vs external party, repeat pattern. Anything scoring above your threshold gets escalated within 48 hours.

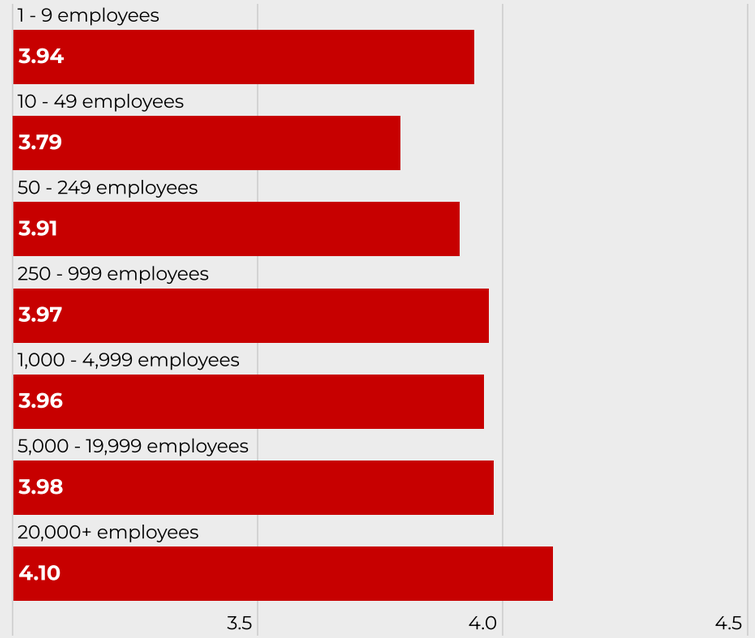
**Designated triage owner:** One person (often finance manager or senior accountant) owns the weekly review of all fraud-related signals: anomalies flagged by accounting software, procurement questions, HR concerns, speak-up reports. They don't investigate – they decide what needs investigation.

**Monthly huddles:** 30-minute cross-functional sessions (Finance, Operations, HR) to review the alert log. What got escalated? What got closed? What patterns are emerging? This creates the feedback loop that builds credibility without requiring formal systems.

**Peer arrangements:** SMEs in similar sectors can establish informal networks where another professional periodically reviews high-risk transactions. Professional bodies can facilitate these arrangements. Fresh eyes spot what familiarity misses.

**Use free tools strategically:** Cloud accounting systems often include basic anomaly flagging (duplicates, round amounts, vendor address matches). Even spreadsheet pivot tables can identify concentration risks and outliers. Focus technology on your highest-risk areas – typically procurement and payments.

Figure 7.6 **Larger firms report higher ease of reporting than SMEs (average, on a 1–5 scale)**



## When to escalate externally

Resource constraints mean knowing when to bring in specialists. Engage external help for:

- Suspected material fraud (jurisdiction-dependent thresholds)
- Cases involving owners or senior management
- Patterns suggesting collusion or organised activity
- Initial fraud risk assessment (often one-day engagement)
- Training boards on fraud governance fundamentals

The cost is typically trivial compared to losses:

**'Basic anomaly detection caught a €45k fraud. The forensic review cost €3k. Even if we only prevent one incident a year, the math works.'**

European participant

## Red flags that demand immediate triage

- Vendors demanding urgent payment or threatening service disruption
- Employees defensive about routine questions or reluctant to take leave
- Round-number invoices or amounts just below approval thresholds
- New suppliers with unclear ownership or multiple vendors at same address
- Override requests without documented business justification.

## SME advantage

Leaders in smaller organisations know their people – behavioural red flags are easier to spot when you see someone daily. Decision-making is faster – no bureaucratic layers where signals disappear. Communication is direct – you can walk across the office instead of filing reports up chains of command.

Build triage around these strengths. Weekly alert reviews take 30 minutes when everyone's in the same building. Peer challenge works when relationships are real, not organisational chart abstractions. Consequence management is immediate and visible when teams are small.

The organisations that fail aren't those with limited budgets. They're those that treat fraud as someone else's problem or assume controls they can't afford mean accepting fraud as inevitable. The organisations that succeed treat triage as a discipline, not a department – and prove that proximity beats technology when you use it deliberately.

# Making risk appetite matter for fraud risk – from statements to reality

**One of the most persistent challenges in fraud risk management shown through this coalition survey is the disconnect between an organisation's risk appetite policy and operational practice.**

Risk appetite – sometimes also referred to as *risk attitude* – and risk tolerance – the amount of risk or degree of uncertainty that an organisation is willing to take – need to be calibrated at different levels of the business, as well as across different corporate functions and the different jurisdictions in which the organisation may operate.[16] Fraud, or health and safety risks call for a zero tolerance approach, but more risk-taking may be needed in other areas in order to bring about business opportunities.

As an example of UK legislation in this space, the Economic Crime and Corporate Transparency Act (ECCTA), enacted in 2023, introduces the new strict liability corporate offence of failure to prevent fraud, which sends a very clear message.

Most organisations declare 'zero tolerance' for fraud in their risk appetite statements. But getting from statements to reality often remains aspirational.

This largely stems from the confusion about what organisations actually expect from risk management, and how resources should be allocated. 'Zero tolerance' for fraud does not mean that organisations must devote all their resources in preventing people from stealing office supplies-. Rather, they need to focus on the gap between board-level declarations and front-line reality, and how this undermines effective fraud prevention and allows critical warning signs to be missed, fall through the cracks, or even dismissed.

## Who owns fraud risk?

The question of ownership for fraud risk is critical. While the responsibility for risk appetite policy rests at a board level, reflecting strategic direction and tolerance for risk – in close collaboration with the organisation's senior decision-makers – the practical reality is often blurred by unclear accountability.

The relationship between the CRO and CFO is particularly crucial for fraud prevention. Finance typically does not report to the CRO, which is how vital early warning signs can be missed. Yet concentrating fraud risk ownership solely with either role creates its own problems.

The CFO's financial oversight makes them a natural stakeholder, but potential conflicts of interest mean they cannot be the sole owner. Meanwhile, CROs sometimes find themselves blamed when fraud occurs, yet they may lack the mandate and authority to drive necessary changes. This is especially so when fraud can impact a wide range of areas from technological to people risks. Where risk is truly integrated into the management of the organisation, there might be a senior leader with overarching responsibility for a subject, but there would also be other owners who must work together to ensure there are no gaps.

16 Airmic (2024) – *Risk Appetite EXPLAINED Guide*, p. 23.

The solution lies in recognising fraud risk as requiring leadership and joint ownership: the board sets the strategic boundaries, while the CRO and CFO collaborate closely on preventing fraud, with both reporting to the CEO as the ultimate owner of fraud risk. This collaboration must be genuine – involving regular communication, shared intelligence and aligned incentives – rather than merely structural as on an organisational chart.

## From strategy to statements to reality

Risk appetite must evolve from a static document into a living framework that guides culture and, in turn, operational choices. This means integrating it into resource allocation, due diligence processes, and strategic initiatives. When organisations identify top fraud risks through assessment, risk appetite should determine which receive immediate attention and investment versus monitoring with existing controls.

This operational approach is particularly critical for emerging risks like AI-enabled fraud. Boards must establish risk appetite before embarking on digital transformation, as risk tolerance can shift unpredictably under pressure. Early clarity ensures consistent decision-making as organisations mature in adopting new technologies.

## Communication, incentives, trust: the antidote to fraud risk

Risk appetite cannot be confined to reports circulating between the risk department and board. It must become part of everyday conversations across all functions, with employees at every level understanding how it applies to their specific roles and decisions.

This requires breaking down silos through collaboration across different teams. Regular knowledge-sharing sessions between risk management and executive leadership can ensure fraud risk remains a standing agenda item and that risk appetite is recalibrated in response to changing threats.

Incentive structures must align with stated risk appetite. If performance evaluations prioritise short-term financial gains without considering ethical conduct and risk management, risk appetite becomes meaningless. Leadership must model expected behaviours, and reward systems must support employees who identify control weaknesses, report concerns, and act within organisational risk boundaries.

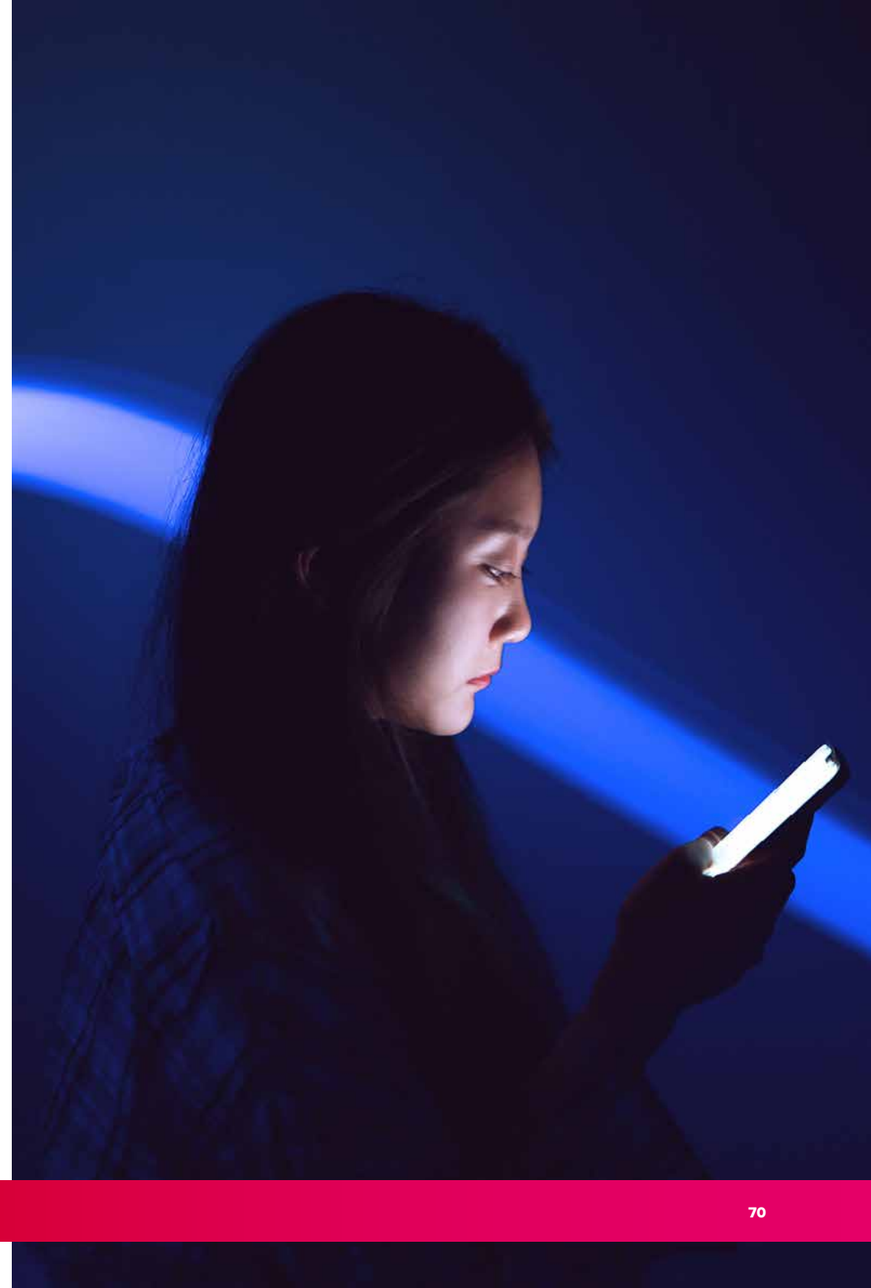
When people understand that speaking up about potential fraud aligns with organisational values and will be supported rather than punished, they can do so without fear of recrimination. The stated risk appetite then begins to shape actual behaviour and help build a positive culture for the organisation.

## The ECCTA opportunity

In the UK, the introduction of the ECCTA provides an opportunity to revisit these fundamentals. Organisations must critically examine whether their risk appetite on fraud is integrated into fraud risk assessment processes, guiding prioritisation and resource allocation.

Most importantly, they must move beyond compliance to genuine cultural transformation, where stated risk appetite shapes how fraud risk is owned, assessed, and managed across the entire enterprise – with clear accountability from board to front line.

**Julia Graham** and **Hoe-Yeong Loke**, Airmic



# 8. The maturity divide – when risk assessments become living tools

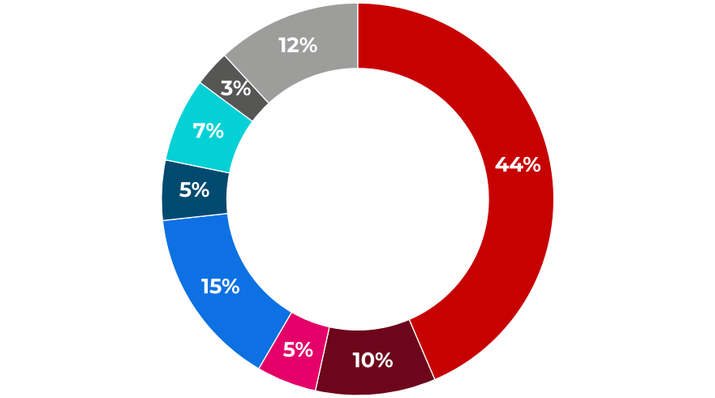
**Fraud risk assessments are often presented as the backbone of prevention. Our research reveals that the difference between a policy on paper and an assessment embedded in decision-making is the difference between fragile defences and resilient governance. This section explains why cadence matters, what maturity looks like, and how behavioural and governance gaps undermine effectiveness.**

## From paper to practice

Across our dataset, a maturity divide emerges. As Figure 8.1 shows, 40% of organisations conduct fraud risk assessments at least annually, while 13% only assess after an incident has occurred. Perhaps more perplexing, 6% don't conduct FRAs and aren't planning to, with another 11% responding 'don't know' – signalling awareness and governance gaps.

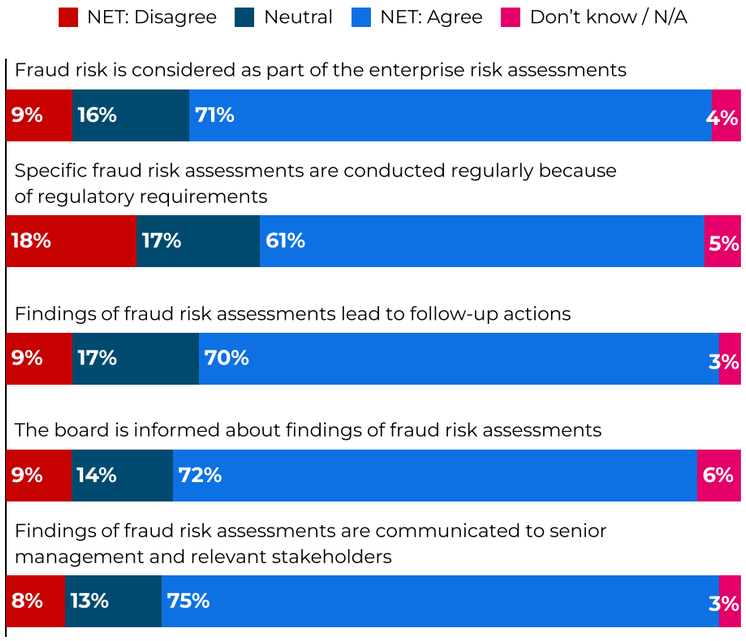
Overall, our research proves that most organisations confuse existence of FRAs with effectiveness. When we examined quality indicators, practice scores averaged just 3.28–3.52 out of 5, hovering between neutral and moderate agreement. This lukewarm performance suggests many organisations have FRA processes in place, but the operating discipline remains uneven. Figure 8.2 illustrates this cadence divide, while Figure 8.3 shows how practice quality clusters in the mediocre middle – organisations going through the motions without genuine maturity.

## Figure 8.1 **Most organisations conduct fraud risk assessments annually — but a worrying share only acts after incidents or not at all**

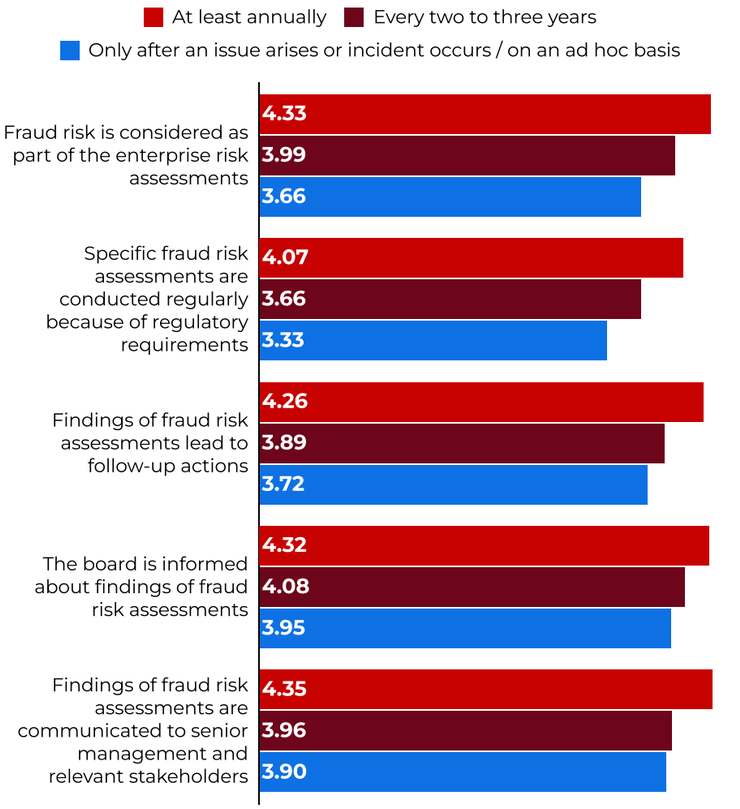



At least annually
Every two to three years
Less often than every three years
Only after an issue arises or incident occurs / on an ad hoc basis
Not conducted previously, but plan to within the next two years
Not conducted previously, and not planning to
Other, please specify
Don't know / not applicable

## Figure 8.2 **Even where FRAs exist, practice quality clusters in the middle — signalling uneven discipline and limited follow-through**




## Figure 8.3 **Confidence in fraud management rises with FRA maturity — especially when assessments are regular, cross-functional and acted upon**



The regression analysis tells a more nuanced story: respondents in organisations with integrated and regularly refreshed FRAs reported significantly higher confidence in managing fraud. Conversely, irregular or siloed assessments performed no better than having no assessment at all. This evidences a simple truth: maturity is built on cadence, cross-functional inputs and consequence management, not on length or elegance of wording.

Accountability gaps are structural: boards say they should own fraud oversight, yet practical ownership drifts and the first line lacks both mandate and resources. A living FRA closes that gap by naming the residual exposure after controls, the owner with budget and the date by which the risk must measurably move. The triage trap described in Section 7 is the other hinge: more signals do not mean more action. A mature FRA hard-wires 'what happens next' by linking each alert category to a time-bound decision path and a feedback loop back to reporters, so confidence and vigilance rise together.

But before organisations can bridge the maturity divide, they must first understand what they're actually assessing. Too many treat FRAs as control audits rather than forward-looking risk analyses.

## Understanding *what* to assess

Our research reveals that a fundamental misunderstanding undermines most fraud risk assessments. As one of ACCA's special interest group experts explains:

**'Most companies treat it like a controls audit – checking what's already in place – rather than a forward-looking analysis of emerging threats. That means they miss the human element entirely. If you're not assessing intention and capability, you're blind to half the risk.'**

Rupert Evill, founder of Ethics Insight and a special interest group member

Our data shows that traditional compliance-driven assessments ignore the behavioural drivers that precipitate fraud. Organisations focus obsessively on technical controls while overlooking rationalisation and pressure, the psychological foundations of misconduct. Roundtable discussions consistently highlighted these behavioural drivers –rationalisation, perceived fairness, leadership credibility, normalisation of overrides – that rarely feature in formal FRAs but regularly enable fraud schemes.

Risk appetite statements also often miss the mark.

**'I think you'll see that most companies, if they create a risk appetite statement, they say that they have zero tolerance to fraud and that fraud risk capital is zero. That's the ask I get and I'm like *"guys, let's be real. This is fraud and it's more complex than that".*'**

Risk management executive in Europe

The ownership vacuum is tangible. As one roundtable participant in the Asia-Pacific explained:

**'I push for fraud to be as a line item in the risk register, so it gets that attention. But the fact that I have to push for it shows that it wasn't originally there. It has never occupied enough space. They see it as other people's problems rather than doesn't really happen in my area. Isn't this a finance team's area? Isn't this a legal's area?'**

Roundtable participant in the Asia-Pacific

Nevertheless, others shared how bow-tie analysis in FRAs not only helped them learn from certain case scenarios but also forced a common language across tech and non-tech leaders that links causes, controls and consequences visibly for boards. A risk manager from a mining company added: *'Bowties forced a common language – "Why is patching only 60%? Who's stopping it?"'*

Leaders that insist on a residual-risk narrative – what remains after existing controls – gain a realistic view of exposure and are faster to act when risk signals change.

## Why FRAs still fail

Recognising what to assess is only the first step. Despite widespread adoption of FRAs, our research also exposed three systemic gaps that repeatedly undermine even well-intentioned assessments.

**The behavioural gap:** Many assessments catalogue controls but ignore the cultural engines driving misconduct – rationalisation, perceived fairness, leadership credibility, normalisation of overrides. When these variables are unmeasured, organisations mistake quiet for safe. Evill offers a practical diagnostic: *'If you pair performance data with engagement data, you can predict where fraud risk spikes. Low performance plus low engagement? Expect petty fraud and absenteeism. High performance but low engagement? That's where you'll find embezzlement – people smashing targets but with zero loyalty.'*

**The triage gap:** Organisations excel at identifying threats yet falter at turning signals into action. Red flags accumulate in hotlines and analytics queues without prioritisation rules, service levels or feedback loops.

**'To proactively look for fraud, you need to get into the mindset of a fraudster, asking what could they exploit? Remembering that fraudsters may find value in something that your business model uses but does not specifically monetise, an example of this could be personal data.'**

Risk manager in the UK

**The governance gap:** Survey data shows 70% agreed FRA findings reach boards, yet roundtables reveal boards treat FRAs as compliance paperwork rather than decision tools. They receive long, reassuring narratives instead of short, decision-ready views of residual risk, ownership and timing.

An IIA member in the US described their organisation's trajectory: *'We have not been performing ongoing fraud risk assessments. The last one that they did was about three years ago and they outsourced it but in the last six months, we've made more progress than what I think we've made in the prior three years.'*

**'It's not sufficient. Our fraud assessment focuses on financial crime, but we need a more holistic view of fraud risk across the organisation. Many other weaknesses, systems, and behaviours can fuel it.'**

European participant

These gaps – behavioural blindness, triage failure, and governance theatre – aren't inevitable. Mature organisations close them through disciplined routines, not grand programmes. So, what does maturity look like in practice?

### Small doesn't mean safe

**A cluster of numerous low-value frauds (eg, expenses, petty procurement, policy overrides) is a culture risk indicator – a sign that norms tolerate bending rules.**

In our roundtables and regression work, organisations that treated these 'small leaks' as noise scored lower on fraud risk management maturity and were more likely to miss higher-impact exposures later.

## What makes FRAs mature

A mature FRA integrates behavioural science, operational data and governance oversight. It explains what remains after controls and who owns that residual exposure, connecting detection with triage so alerts are ranked by consequence and acted upon within defined service levels.

Maheswari Kanniah, former group chief regulatory and compliance officer at Kenanga Group, demonstrates what active board engagement looks like: *'I don't sugarcoat compliance risks. I present real cases, dissect consequences, and say plainly: "This will trigger a fine of X amount. These are the sanctions. Here's the licensing fallout." I educate the board and audit committee with urgency and clarity. I bring in police officers and anti-corruption experts to brief them on emerging scams and fraud trends. The result? My board became vigilant. They ask tough, targeted questions. My internal audit team prepares rigorously, knowing the chairman will demand: "Did you detect any fraud? Did you verify this? Did you challenge that?" That's the culture we need, one where oversight is active, informed, and unafraid.'*

This hands-on approach creates transformed governance: boards move from passive recipients of comfort narratives to active challengers of risk assumptions. Quarterly case reviews combined with police and anti-corruption briefings give leaders typologies and staff visible consequence management. Board walk-abouts make 'tone at the top' concrete and gamified campaigns make awareness stick across borders. Publishing anonymised outcomes internally is the hinge between policy and trust.

## Handle the label carefully

Foss raises a crucial operational point that mature organisations build into their FRAs: *'Firms will identify very many potential frauds on incidents perhaps. As soon as these are labelled frauds in internal process documentation or emails, the regulatory reporting clock starts counting. So, like with suspected but not confirmed data breaches, don't apply the "fraud" name until you are prepared to start that clock. That must be a rule across all role types, otherwise someone can step out of line while investigation is still underway.'*

This isn't about suppressing concerns – it's about rigorous incident classification. Many potential fraud signals come to nothing upon investigation. Premature labelling triggers regulatory obligations, creates legal exposure, and generates false positives that undermine credibility.

**'Mature FRAs include clear terminology protocols: 'anomaly under review', 'incident requiring investigation' and 'confirmed fraud' represent distinct stages with different escalation rules and reporting obligations. This discipline protects both investigative integrity and regulatory compliance.'**

From a practical lens, think of vulnerability in the context of the threat to understand exposures – threat plus vulnerability equals exposure. *'That forces you to think about intention, capability, predictability and resilience, not just controls,'* Evill explains.

### The right questions can change behaviour:

*'Who holds company laptops or mobile devices with privileged access, and how does least privilege work in practice? Which roles can override approvals – how often, and where are the clusters? Where are low engagement/high-performance hotspots? Which suppliers changed beneficial ownership or bank details this quarter, and what proportion were independently verified? What percentage of red flags breached escalation SLAs [service level agreements] – where, why, and what changed? How many high-risk payment authorisations followed a verified callback? What did the last deepfake/business email compromise drill reveal, and how were flows strengthened afterwards? Which training modules produced measurable behaviour change?'*[17]

Practical frameworks can accelerate maturity development. Transparency International Sweden's *Business Integrity Tool*, developed with support from Swedfund and Ethics Insight, provides investors with systematic guidance for conducting integrity due diligence and developing action plans. The tool's strength lies in its sector-specific risk questions and its progression from gross risk identification through control assessment to residual risk management, mirroring the FRA maturity journey organisations must undertake. See Appendix for more details.

17 Service Level Agreements (SLAs) in fraud risk assessments are formal contracts that define performance standards and quality for fraud detection and prevention services, particularly when outsourcing to a third party. They outline specific responsibilities, performance metrics like response and resolution times for incidents, and penalties for non-compliance to ensure both parties meet agreed-upon standards and manage fraud risk effectively. Transparency International Sweden (2024) – *Business Integrity Tool*.

## Proving prevention pays

Mature organisations don't just prevent fraud – they prove it pays. This requires shifting from compliance-cost narratives to investment-return evidence. The calculation is straightforward but rarely performed: prevented loss (blocked payments, supplier off-boardings, recovered assets, avoided regulatory fines) versus cost-of-controls (technology, training, dedicated resources, investigation capacity).

**'Audit committees should be asking: what is the cost of controls versus the cost of failure? It's not just a compliance spend – it's an investment that pays for itself if measured properly.'**

UK board director

But it's not just about reducing loss and all the indirect costs of responding to and treating fraud. Investors increasingly apply discounts on weaker governance, or higher rates on loans, and there is an 'ethical alpha' – the premium we pay for companies and their products when they demonstrate integrity, sustainability, and the rest.

When leadership sees prevention generating measurable returns, momentum holds. Boards that receive quarterly ROI dashboards showing fraud losses avoided alongside control costs can justify incremental investment in analytics, training, or specialist capacity. This transparency also resolves a common tension: finance teams questioning whether anti-fraud resources represent value, and risk teams struggling to quantify impact.

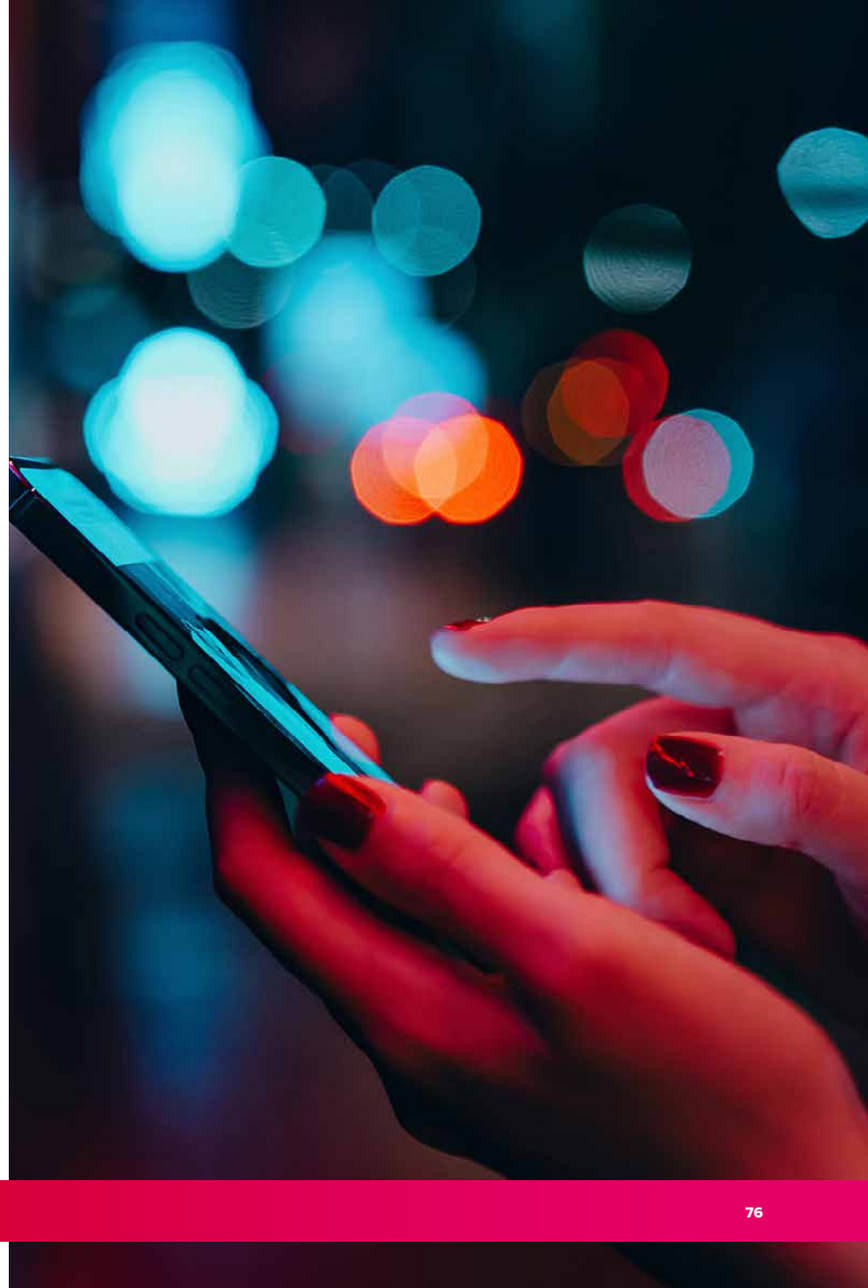
The organisations demonstrating strongest FRA maturity in our research shared three measurement disciplines:

**Track near-misses and interventions, not just confirmed fraud.** A blocked suspicious payment or a vendor removed during due diligence represents prevented loss, even if never formally classified as fraud. These 'saves' rarely appear in traditional fraud reporting but demonstrate control effectiveness.

**Calculate full-cycle costs of fraud incidents.** Direct loss is only the start. Add investigation time, legal fees, remediation work, regulatory engagement, reputational damage, insurance premium increases, and opportunity cost of management attention. One European participant calculated that a €45k fraud cost the organisation over €200k when all factors were included.

**Publish prevention metrics internally.** Quarterly summaries showing blocked transactions, interventions, and estimated savings build credibility for the fraud prevention function and reinforce the culture that speaking up leads to tangible protection. Transparency about ROI makes prevention visible rather than assumed.

Several roundtable participants noted that once boards saw prevention ROI quantified, questions shifted from 'can we afford this?' to 'where should we invest next?' That reframing – from cost centre to value generator – fundamentally changes how organisations resource and prioritise fraud risk management.



## Why forensic skills matter

Maturity requires more than governance discipline and behavioural instrumentation. It also demands a capability that many organisations relegate to post-incident response: forensic expertise. However, forensic accounting was frequently misunderstood as a niche or purely post-incident discipline in our research. In reality, it is one of the most strategic capabilities an organisation can possess in an AI-enabled world.

Boards often assume that audit equals fraud detection; it does not. Forensic work brings legal-process awareness (chain of custody, admissibility), pattern recognition beyond sampling, and investigative scepticism that challenges convenient narratives. Those strengths transform an FRA from a catalogue of risks into an engine for discovery and consequence.

Our interviews repeatedly surfaced the same lesson: when forensic perspectives are present at design time, controls are simpler, triage is cleaner, and investigations move faster. As one forensic accountant participant put it: *'If you can't explain override clusters or vendor anomalies to a board in plain language, your FRA is a paper tiger.'* Elevating forensic skills through dedicated roles, on-call panels or structured secondments builds the organisational muscle to interpret weak signals, separate error from intent and convert detection into sustainable remediation.

## Optimising FRAs with AI

Forensic expertise provides the investigative lens; technology provides the scale. When used responsibly, AI can transform FRAs from periodic exercises into continuous sensing systems, but only if organisations understand both the promise and the peril.

We found how it can accelerate drafting, highlight anomalies at scale and help teams move from periodic reviews to continuous assessment. This is not about replacing jobs but allowing people to do them better. The UK Public Sector Fraud Authority (PSFA) has shown how AI can eliminate the 'blank page' problem by producing first-cut assessments that humans then interrogate and validate. In high-velocity environments, that shift can free scarce expertise to focus on judgement, not clerical production.

But credible ROI also depends on structured, consolidated data which even the most mature organisations struggle to achieve and most of the 'off-the-shelf' AI tools miss early warning indicators from 'non-fraud' data. *'Most organisations are full of poorly structured data and duplicative or clashing systems, so the first step is to deal with the most likely threats given what we do, and where we do it, and then map that against existing processes. Those processes and data might show all sorts of "non-fraud" data sources that are highly useful early warning indicators for fraud, for example, engagement survey data, exit interviews, turnover, speak-up data, overtime, attendance and absenteeism, and job stagnation/rotation. AI tools don't know what to do with that data because the AI is looking for purely fraud-detection tools, which are all quite reactive,'* Evill adds. Mapping these signals alongside payment anomalies and vendor changes turns AI from a reactive detector into an early warning system.

AI's benefits arrive with several non-trivial risks. Open models can leak sensitive data; generative systems can hallucinate with unwarranted confidence; and poorly governed automation can create a false sense of certainty that outpaces due process. Responsible adoption therefore requires explicit governance: verifying data provenance, validating and stress-testing models, red-teaming deepfake and social-engineering scenarios, and maintaining human oversight for consequential decisions.

**'AI should never replace professional scepticism; it should enhance it.'**

### Key takeaways

#### Are your fraud risk assessments living tools or compliance theatre?

Evaluate whether assessments integrate behavioural science with financial analysis, determine if boards receive decision-ready intelligence rather than long narratives, and assess whether triage systems convert reports into action. Challenge whether your FRA examines behavioural drivers like rationalisation patterns and override clusters or merely catalogues controls. Most critically, ask if your board expects regular residual-risk notes naming specific exposures, owners, and deadlines – or whether they receive comfort narratives that underestimate risk.

## Governance-grade fraud insight, without the theatre

**Boards don't need another doomsaying report about the ubiquity of fraud or a static risk register; they need a way to turn all the things you could worry about into a short, ranked list of what to do next.**

Ethics Insight is developing an AI-assisted triage tool built on a deep knowledge base: hundreds of deals and post-investment reviews, thousands of investigations, regulatory filings and typologies. It is designed to complement, not replace, human judgement and existing frameworks.

We start outside-in. Country, sector, transaction, and partner exposures are scored using a structured rubric – rule of law, procurement transparency, sector fraud typologies, channel risk – so the questions you face are specific to your operating context rather than generic heat maps. That creates a defensible list of plausible fraud threats to move beyond generalised indices to genuine clarity.

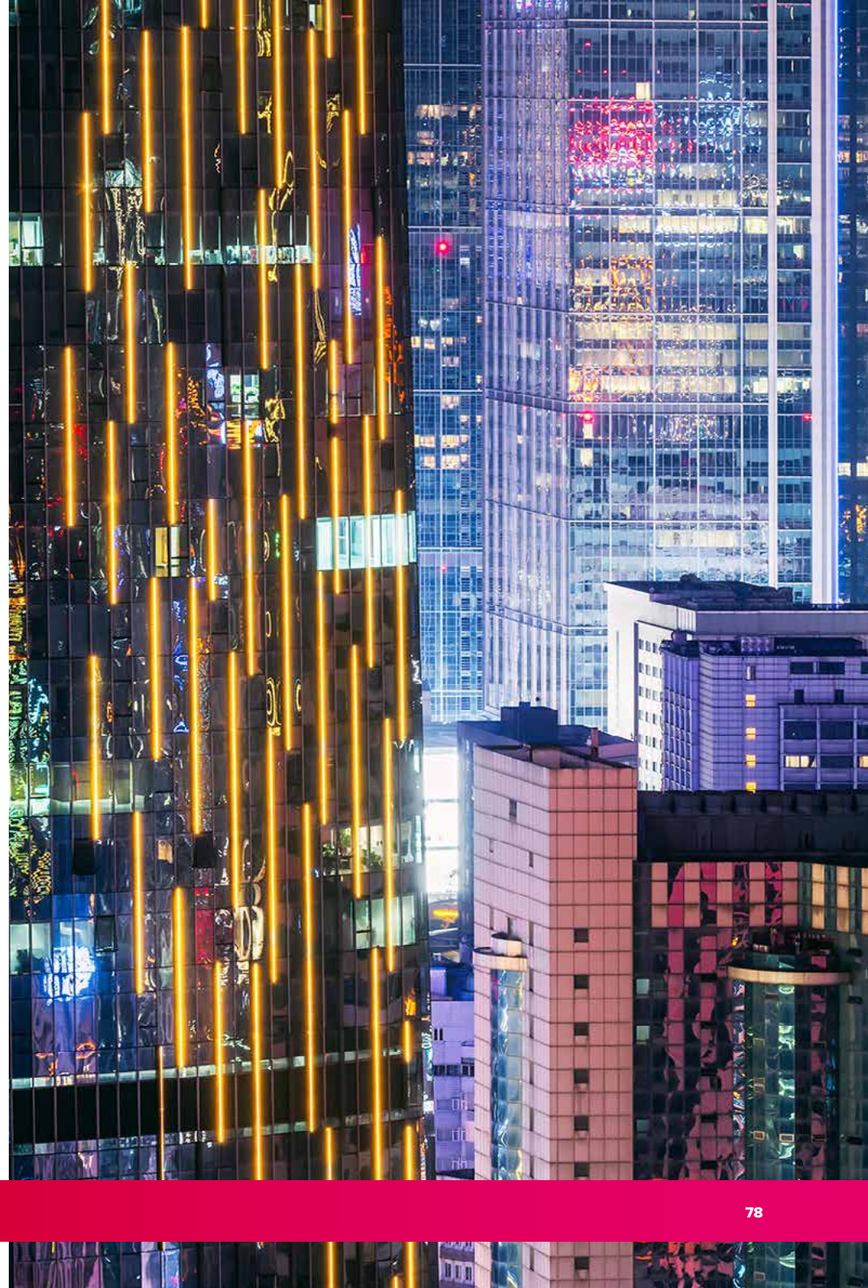
Next, we test what exists. Policies, processes, and controls are interrogated and mapped to the realistic and rightsized threat scenarios – segregations, approvals, analytics, speak-up.

We then probe the knowing-doing gap with implementation questions – now shrunk to a few hours' work, not weeks of invasive audits. We ask things like who overrides, how often is this or that checked, what evidence, what data isn't there, and so on. This focus on doing, not just having, closes the accountability (ownership versus assurance confusion) and maps fraud to operations.

Finally, we prioritise and rightsize. Findings are converted into a concise action plan based on your governance framework, with risk-based and targeted fixes. For example, in a recent case, a renewable energy firm was contemplating outsourcing (six-figure contract) analytics to 'identify as yet uncategorised fraud'. The prioritising indicated that it might be cheaper, quicker and more effective to first tidy up vendor data before integrating a few simple (and affordable) add-ons to their existing accounting platform.

Where helpful, we map controls across the value chain or project lifecycle – from licensing to procurement and operations – so teams see red flags, tests and owners at each stage.

The result is not another weighty report. It's a living (and interrogable) feedback loop that helps boards connect decisions with outcomes, surfaces behavioural weak points, and equips management to iterate faster than adversaries.



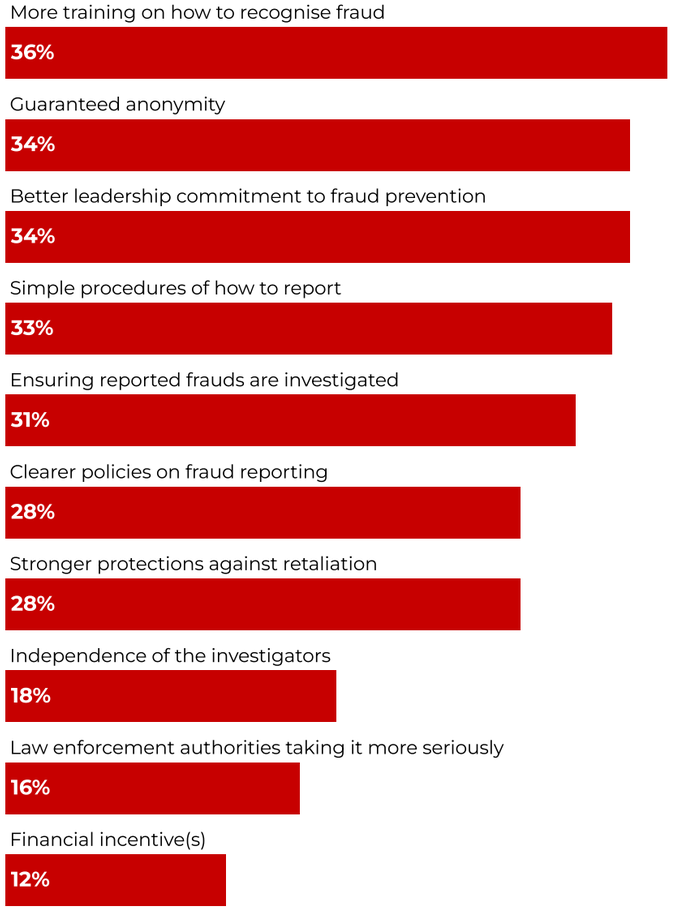
# 9. Fostering cultures of integrity – from whistleblowing to raising concerns

**Our research reveals that while many organisations have whistleblowing policies, these channels are mistrusted, misused or under-used.**

The result is a credibility gap where fraud and misconduct remain invisible until crises occur.

Fraud thrives not only where controls are weak but where cultures silence concerns. Our research reveals that while many organisations have whistleblowing policies, these channels are mistrusted, misused or under-used. The result is a credibility gap where fraud and misconduct remain invisible until crises occur.

## Figure 9.1 **What encourages reporting (global)**




Our survey data shows that although two-thirds of respondents say it's easy to report fraud, ease rises dramatically with seniority and company size. Financial services and shared services feel most enabled to report, while mid-tier and small accounting firms, consultants, external auditors, and the self-employed skew neutral or unsure. This represents a dangerous gap: many of those closest to the fraud – junior staff, contractors, external auditors – often find it hardest to raise concerns. Figure 9.1 identifies the most effective levers for encouraging fraud globally. As Figure 9.2 shows, generationally, Gen Y elevates anonymity and independence, while Gen X emphasises training.

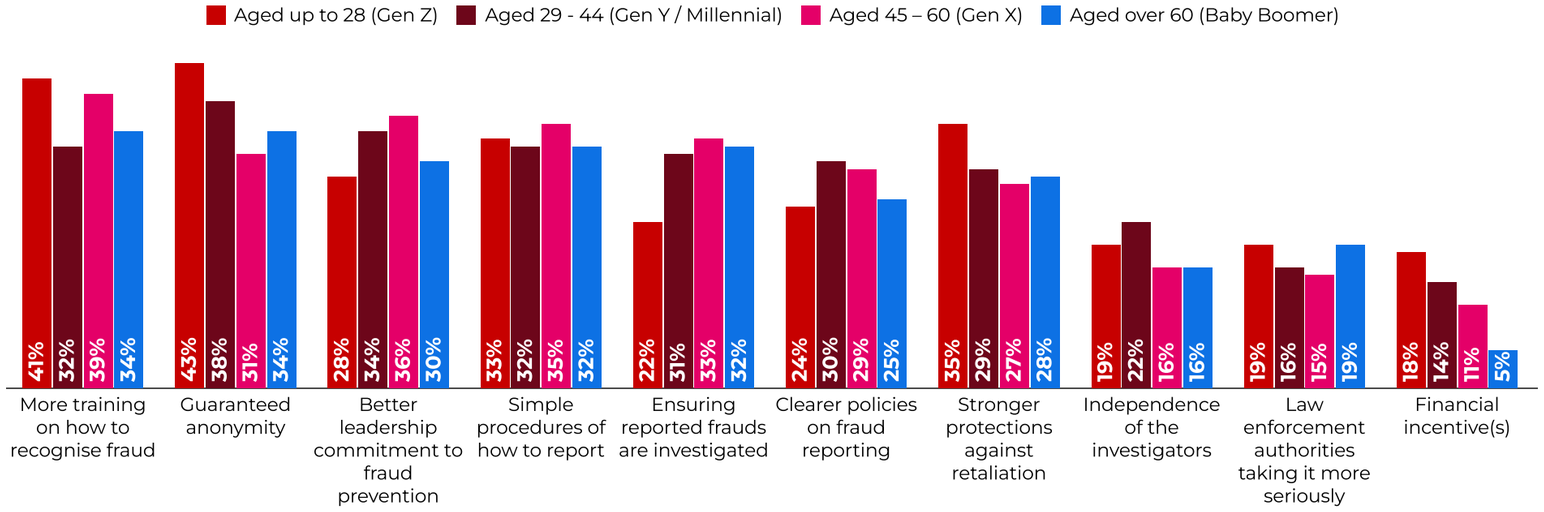
## The terminology problem

The very term 'whistleblowing' emerged as part of the problem. In roundtables across regions, members consistently said that the word carries negative connotations of betrayal and punishment. Figure 9.3 shows regional differences in reporting channel preferences. In some national cultures, to 'blow the whistle' is seen as disloyalty, even treachery.

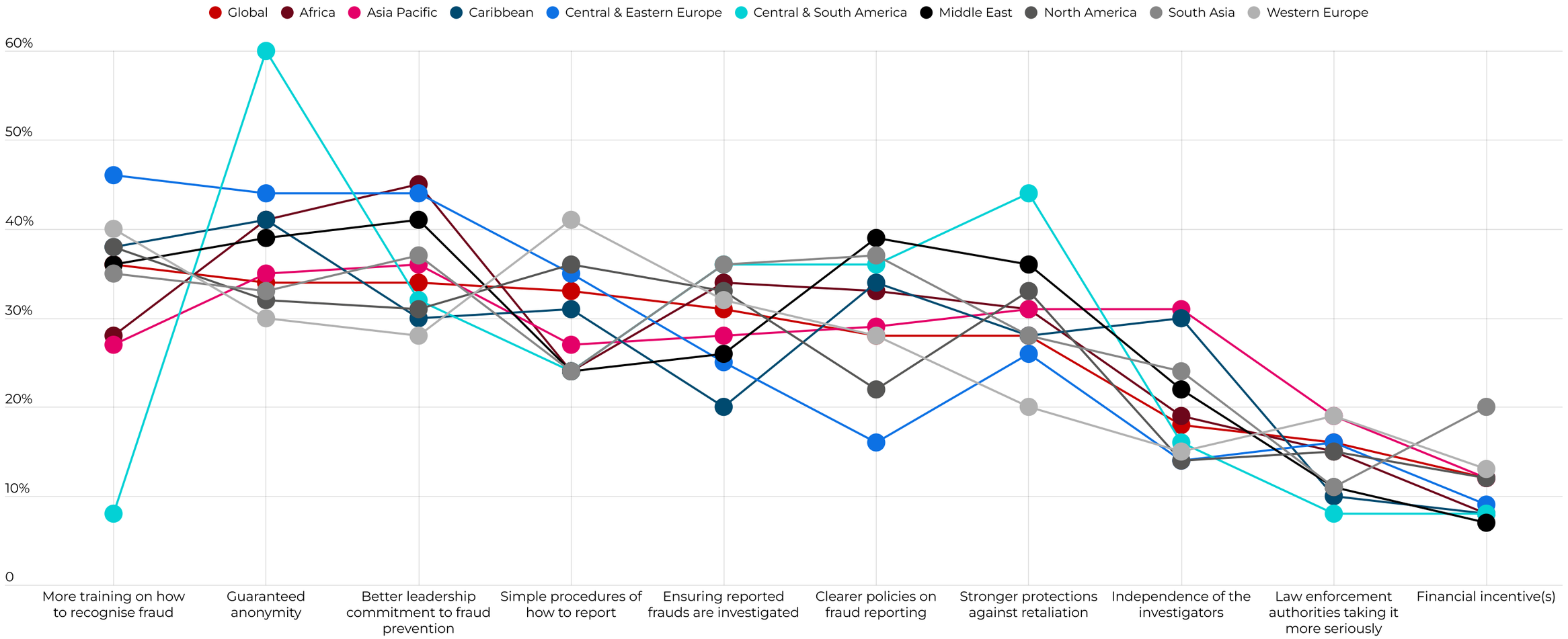
**'In our culture, speaking up against your manager is unthinkable. You'll be ostracised even if the policy says you're protected.'**

Senior internal auditor in the Asia-Pacific manufacturing sector

## Figure 9.2 **Generational differences shape motivators**



## Figure 9.3 **Encouragement by region**



Pav Gill, Wirecard whistleblower and co-founder of Confide Platform, puts it bluntly:

**‘Just because you don’t like the person that struck the match, that doesn’t mean you ignore the fire. Motive shouldn’t matter at stage one – if the facts are real and could have a material adverse impact on your company, that’s what should matter.’**

Pav Gill, Wirecard whistleblower and co-founder of Confide Platform

Still, organisations often become distracted by questions of motive and credibility rather than focusing on the substance of concerns raised.

Our cluster analysis underscores why a generalised whistleblowing approach does not work. Overloaded Realists want to speak up but feel nothing will change. Cynical Insiders distrust the system entirely, assuming reports will be buried. Optimistic Practitioners believe policies exist and assume they work. Detached Observers do not engage with reporting at all. This explains why survey results showed a disconnect: while many organisations rated themselves as having ‘robust reporting systems’, respondents across levels and regions rated ease of reporting significantly lower.

## When policies don’t protect

The credibility gap between policy and practice was clear across our regional roundtables. One US participant captured this: *‘There still is never a happy whistleblower. It’s a policy on paper. How is it actually being put into practice?’* This sentiment was echoed globally:

**‘People are still blowing the whistle, but there are no clear guidelines. The policy is there, but there are no regulations on impact. If someone is complaining about their supervisor, there is no protections in the law.’**

Canadian participant

The Malaysian context reveals how legal frameworks can conflict with good practice. Malaysia’s Whistleblower Protection Act requires that the very first point of contact for an employee must be an enforcement agency like the anti-corruption commission or securities regulator – meaning that if you told your boss in the company first, you disqualify yourself from protection. This creates an impossible choice: follow company policy and lose legal protection or bypass your employer entirely and escalate externally from day one.

Fear of retaliation remains pervasive. A participant in India described how employees are *‘very much scared to use that speak-up because of retaliation… even if I can pinpoint it, it can come to a performance price.’* This fear persists despite formal policies guaranteeing confidentiality, highlighting a disconnect between stated values and lived experience.

## The firewall solution

One of the most practical innovations to emerge from our research is the firewall investigation model. Separating reporter liaison from the investigation team strengthens both trust and integrity. Team A manages intake, welfare, updates and anti-retaliation monitoring. Team B conducts evidence gathering, interviews and findings. Both share case IDs and audit trails but do not directly interact with the reporter.

In a regional bank where this model was adopted through the Confide Platform, average acknowledgement 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. Participants in Gill’s training sessions, including the world’s first whistleblowing case-management masterclass delivered to Malaysia’s Securities Commission, consistently rated this as one of the most practical takeaways.

The firewall approach addresses a fundamental problem: reporters need consistency and trust in their point of contact, while investigators need independence and objectivity. Combining these roles in one person creates conflicts that undermine both functions.

## Consequence management: tigers that bite

Respondents, especially in Africa and the Middle East, stressed that consequence management is as important as policy design. Fraud reporting systems fail when staff see that nothing happens to perpetrators, or worse, that whistleblowers are punished.

**'Policies without enforcement are like tigers that don't bite. People need to see both consequences for misconduct and rewards for raising concerns.'**

Chief risk and compliance officer at an African bank

The lack of visible consequences creates rational cynicism. Why take the career risk of reporting when leadership demonstrably ignores or buries concerns? Another Africa participant working in financial services described the result:

**'We can raise concerns, but there is no consequence management. Nothing happens. People stop speaking up.'**

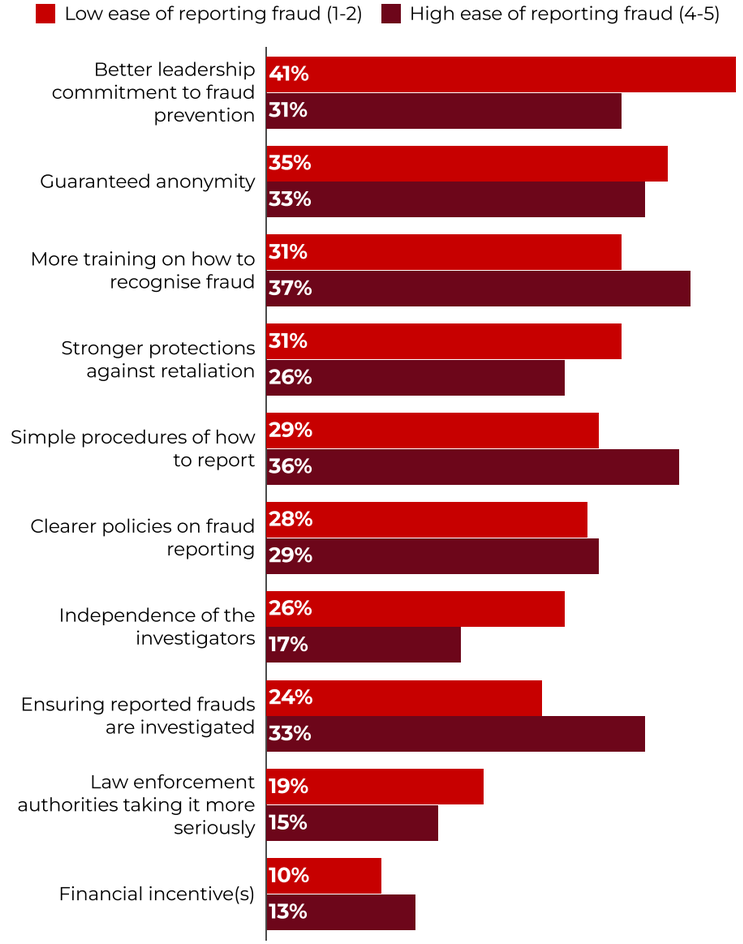
Africa participant working in financial services

Some organisations are experimenting with recognition systems that reward employees for flagging risks. Gill describes how bounty cultures can work for mid-sized companies when structured properly: reward only substantiated cases with material recovery or risk reduction, use sliding scales with caps payable once outcomes are final, make decisions through committees independent of the case chain, and publish eligibility criteria while keeping awards confidential unless the reporter opts in. The key risk is preventing a culture where everyone actively starts digging for dirt purely for monetary gain, so this must be structured as a governance mechanism, not a PR exercise. Some organisations are experimenting with bounty systems. See *Calls to Action* supplement for implementation guidance.

The most powerful way to build trust is demonstrating that no one is above accountability, including senior executives and high performers. Several participants suggested organisations publish anonymised quarterly 'speak up outcomes' notes showing case categories, resolution times, corrective actions taken and lessons learned. When employees see action results from reporting, confidence builds. When they see silence or cover-ups, cynicism entrenches.

As Figure 9.4 illustrates, where reporting is hard, the asks are leadership commitment, anti-retaliation and independent investigations; where it's easy, the asks shift to training, simple procedures and follow through.

Figure 9.4 **Hard vs easy reporting asks**



## Normalising integrity conversations

The lesson is clear: whistleblowing policies alone will not build resilience. Organisations must reframe the issue as a broader culture of raising concerns – not just about fraud, but about any behaviour that could compromise integrity.

**'Fraud is a legal category. Integrity is bigger. If we only wait for clear fraud to be reported, we've already lost the culture battle.'**

Finance professional from large corporate

This reframing makes speaking up routine and normalised, not extraordinary or adversarial. It shifts the focus from legal thresholds – what counts as reportable fraud – to ethical standards encompassing conflicts of interest, misuse of data and grey zone behaviours. It creates a continuum of integrity where concerns are logged, triaged and addressed early, before they escalate into fraud.

Gill emphasises that rather than focusing solely on whistleblowing, companies should enable people to raise any concerns without fear. This includes rewarding employees who identify operational flaws, process gaps or conflicts of interest, demonstrating that speaking up is valued, not punished. Not every concern is fraud. A junior engineer flagging that customer data is being misused in an AI solution is raising a legitimate product concern, not 'blowing the whistle'. Organisations need to create space for these conversations.

Publicising outcomes internally through anonymised disclosures came up repeatedly in roundtables. As participants across regions emphasised, 'it is key to walking the talk'. Transparency about what happens to reports – even in aggregate form – builds the credibility that formal policies cannot.

## Training that works

For fraud recognition, training must be role-specific and aimed at hardest-to-report schemes – procurement, internal financial fraud, expense fraud and abuse-of-authority cases where prevalence is high, but reporting remains difficult. Organisations should build short, scenario-based modules for procurement, accounts payable, HR and payroll, sales operations, and frontline supervisors. These modules must include jurisdiction-specific speak-up options (including anonymous, app-based channels) and anti-retaliation assurances baked in. To convert awareness into trust, publish investigation outcomes and timelines. Measure near-miss signals, time-to-decision and hold rates on suspect payments – not training hours.

Treat speak up data like a protected asset: clear ownership, strict access roles, and documented retention. Reporters gain confidence when they see outcomes and know their data is safe. For investigators, consistent metadata (case ID, timestamps, classification) turns 'stories' into signals you can triage with the rest of the fraud data.

For case handlers, organisations often assign whistleblowing responsibilities without proper training or certification. Interactive training covering real-world scenarios like Wirecard, Wells Fargo, Boeing and Theranos – addressing conflict navigation, escalation protocols, independence definitions and why the first 48 hours are critical – is essential for HR, legal, compliance, risk and board members who handle cases. Malaysia's Securities Commission pioneered this training approach using AI-powered tools to uncover new scam tactics, recognising that case management requires professional development, not just policy compliance.

## Tailoring policies to context

Cultural barriers vary widely across geographies, reinforcing the point that policies must be tailored to national and organisational contexts, not imported wholesale. Every jurisdiction has its own legal and cultural nuances and contradictions.

Figure 9.3 showed how regional patterns differ: Africa and Central & South America prize anonymity (and Africa also leadership); North America asks for anti retaliation; Asia Pacific and the Caribbean emphasise independence of investigators; Western Europe prefers training and simple procedures.

In Asia-Pacific contexts, hierarchical norms make speaking up against superiors particularly fraught. The fear isn't just professional consequences but social ostracism. Several European roundtables linked cultures of integrity to transparency in public spending and investment, with participants arguing that anti-corruption measures must be visible to maintain public trust. North American frameworks are heavily driven by litigation risk, creating highly formal whistleblowing structures that can be intimidating or inaccessible to those unfamiliar with legal processes. One European participant captured the challenge of importing policies across borders:

**'In the Eastern bloc you would be seen as a bad person. You're calling on your colleagues and informing on them, so you have to look at all these cultural and historical aspects to understand how speaking up or whistleblowing is treated.'**

Compliance officer

## Capital's role in fraud prevention

Another under-discussed dimension is the stewardship role of investors and lenders. Fraud harms both companies and their capital providers. *'The till of a company is really the investor or the bank. If fraud drains that till, it is the investment community that takes the hit,'* as one UK board member commented.

Roundtable participants argued that both investors and lenders should use their influence to demand stronger fraud risk management and more transparent reporting of fraud incidents. Yet survey responses suggest few firms currently demand this level of disclosure. One European participant asked pointedly:

**'Investors sign up to the UN's PRI [Principles for Responsible Investment], but rarely ask: is this company paying bribes? Are they taking a blind eye? Are they conducting proper fraud risk assessments as part of their investment process? ESG without anti-fraud is window dressing.'**

Financial services participant

Doing so would send a powerful signal: companies that fail to manage fraud risk may lose access to capital. When boards see that capital allocation hinges on prevention maturity, momentum follows.

## What *actually* changes behaviour

What does it take to move from whistleblowing policies to cultures of integrity? Our research points to several necessary shifts in practice.

First, multiple channels must coexist. Not everyone is comfortable with hotlines. Digital platforms, anonymous options, peer-reporting systems and direct escalation routes must all be available and transparent. Younger staff, particularly those in early-career roles, tend to prefer mobile app or chat-based intake channels and are more likely to select anonymity. Older staff more often choose named reports routed through email, phone or direct escalation to managers or HR. Across all age groups, the decisive factor is not channel but trust. Reporters gain confidence when they see follow-up, timelines met, and senior-subject cases handled visibly and independently.

Second, triage processes must function. Reports must be logged, categorised and acted on quickly, or credibility collapses. As we have discussed, weak triage is where most reporting systems fail – not in policy design, but in operational follow-through.

Third, transparency about aggregate data on cases raised and actions taken should be shared internally and, where feasible, externally. Employees need to see that reporting leads to outcomes, not silence.

Fourth, role clarity matters. Employees need to know who will hear their concerns, how independence is maintained, and what outcomes they can expect. This is where boards and audit committees come in. If they receive only sanitised statistics, they will never grasp the lived experience of fraud reporting. If they insist on root cause analysis and culture metrics, they can set new standards of governance.

By reframing whistleblowing as raising concerns, tailoring approaches to cultural contexts, enforcing consequences, building firewall processes, investing in proper training and involving investors, organisations can shift from policies on paper to cultures in practice. In doing so, they not only prevent fraud but also strengthen their overall risk culture and governance.

### Key takeaways

**Does your organisation still use 'whistleblowing' terminology, or have you reframed this as normalising integrity conversations?**

Assess whether reporting channels accommodate different cultural contexts and communication preferences, evaluate if consequence management includes both penalties and recognition, and determine whether reports receive transparent triage that builds credibility. Most critically, examine whether your approach addresses different personas in your organisation – Overloaded Realists need support, Cynical Insiders need trust-building, Optimistic Practitioners need reality checks, and Detached Observers need engagement.

### Practical solutions from the field

**Pav Gill, co-founder of Confide Platform and member of our special interest group, provides additional practical guidance based on his pioneering whistleblowing case-management training:**

**On handling whistleblowing vs blackmail:** Investigate the allegation on its merits and the demand as a separate conduct issue. Two lanes from day one. Document the sequence tightly and involve law enforcement early if threats cross into extortion.

**On policy conflicts in jurisdictions like Malaysia:** For companies balancing conflicting laws, offer dual-track policy options allowing both internal and direct-to-agency reporting without loss of protection. Ensure first receivers are outside management lines, and senior-subject cases receive board-level or external oversight. Maintain documentation discipline – separate fact-finding from employment actions so evidence is preserved and not subsumed under HR or legal defensiveness.

**On training impact:** Themes that shifted thinking most in training sessions include boards starting to ask for unresolved case lists rather than just volume dashboards, clearer triage criteria for distinguishing protected disclosures from grievances, and recognition that retaliation risks peak after case closure, leading organisations to implement follow-up welfare checks at 3, 6, and 12 months.

# 10. The questions that could change everything

**Fraud resilience isn't built on more rules – it starts with sharper thinking and the courage to challenge assumptions. The organisations that thrive will be those that ask harder questions before fraudsters exploit the gaps.**

The questions below are not generic checklists. They are drawn from what our survey data and 31 roundtables revealed about where fraud thrives: accountability vacuums, cultural blind spots, emerging threats, and governance inertia. They are grouped by role and tuned to real-world vulnerabilities.

Use them as a provocation, a boardroom agenda, and a cultural litmus test. The organisations that survive will be those willing to ask uncomfortable questions early – and act on the answers.

## Boards and audit committees

- Is fraud a standing agenda item with case-learning at every meeting?
- Do we have a sitting director with ethics, risk, compliance, or audit background on the board?
- Do we receive a residual-risk narrative (what remains after controls, who owns it, and by when)?
- Have we stress-tested a deepfake or AI-enabled fraud scenario? What failed?
- Are failure-to-prevent obligations (eg, ECCTA) embedded in our governance and evidenced?
- Do we see triage dashboards showing what was reported, prioritised, and acted on – not just final cases?
- Do we receive a one-page 'data readiness' view alongside FRA results covering owners, lineage, quality breaches, and change tracking for valuation-critical data?
- Are investigation routes independent of management influence, and do we publish anonymised outcomes internally to sustain speak-up confidence?
- Is fraud prevention ROI quantified (cost avoided vs cost of controls)?
- Do we have cross-border playbooks for evidence preservation and regulatory engagement?
- Are ESG and crypto risks integrated into board-level risk discussions?

## Executive leadership

- Is fraud prevention in the COO's KPIs and budget?
- Do we have a Friday-night crisis playbook for fraud events?
- How do we signal integrity beats optics in ESG, growth, and investor narratives?
- Are cross-functional fraud response teams (finance, cyber, HR, legal) active and drilled?
- Do we track time-to-triage and time-to-decision SLAs for fraud alerts?
- Are AI and cyber risks integrated into enterprise scenarios, not siloed in IT?
- Do we monitor fraud risk intelligence from high-risk markets?
- Are failure-to-prevent obligations mapped to operational controls?
- Do we test fraud scenarios involving corporate/director liability under ECCTA?
- Is due diligence on agents and suppliers risk-based and documented?
- Which datasets and join keys are our single points of failure for fraud prevention, and who owns their resilience?
- What are the SLAs for crossfunctional fraud data sharing (triage timelines, formats, escalation)?

## Risk management

- Are AI-enabled fraud, ESG misreporting, and sanctions breaches in our risk scenarios?
- Do KRIs include behavioural indicators (override rates, leave anomalies) as well as loss events?
- Are fraud risk assessments at least annual, cross-functional, and linked to resource allocation?
- Do we run red-teaming or mystery shopping for procurement and payment controls?
- Are geopolitical and third-party risks embedded in enterprise risk maps?
- Do we monitor regulatory change (e.g., ECCTA, crypto) and update fraud scenarios accordingly?
- Are fraud findings and learnings shared across functions, anonymised in a way that does not breach data privacy laws?
- Do we have escalation protocols for fraud indicators?
- Are risk appetite statements tested against fraud exposure?
- Is fraud risk embedded in M&A and investment due diligence?

## Finance & accounting

- Do payment controls apply ‘verify then trust’ for high-risk changes (bank details, urgent requests)?
- Are vendor concentration, split transactions, and duplicate logic reviewed monthly?
- Is forensic skill embedded in Finance or on-call for anomaly interpretation?
- Do we reconcile fraud cost base vs cost-out savings for board visibility?
- Are crypto and ESG exposures tested for fraud risk, not just compliance?
- Are fraud indicators integrated into financial dashboards?
- Do we test for override risks in financial reporting?
- Are whistleblowing logs reviewed for financial anomalies?
- Do we validate supplier authenticity and beneficial ownership?
- Is fraud risk considered in financial forecasting and stress testing?

## Internal audit

- Do audits include fraud prevention effectiveness, not just policy presence?
- Can junior auditors escalate around hierarchy if they suspect fraud?
- Do we audit culture metrics (speak-up integrity, retaliation checks) alongside controls?
- Are geopolitical and third-party risks part of audit scope?
- Do we test fraud scenarios involving override and collusion?
- Is professional skepticism documented in audit judgments?
- Are fraud risk assessments reviewed for completeness and follow-up?
- Do we use forensic specialists or data analytics where fraud risk is high?
- Are audit findings linked to fraud deterrence outcomes?
- Do we assess fraud readiness in ESG and crypto domains?

## Compliance & investigations

- Are speak-up channels jurisdiction-fit (anonymous, app-based where needed)?
- Do we publish aggregate outcomes to build trust?
- Are KPIs outcome-based (risk reduction, early interventions) rather than output-based (training hours)?
- How do we lawfully share fraud typologies across Finance, IA, and Cyber without breaching data laws?
- Do we test retaliation risks and feedback loops in investigations?
- Are fraud typologies updated with emerging threats (AI, crypto)?
- Is compliance involved in cross-border evidence preservation?
- Do we monitor fraud reporting trends and act on anomalies?
- Are training programmes tailored to fraud risk exposure?
- Do we have escalation protocols for internal fraud indicators?

## Investors & asset owners

- Do we require investees to publish fraud risk assessment cadence and maturity scores?
- Are anti-fraud and anti-bribery standards embedded in ESG due diligence?
- Do we interrogate whistleblowing credibility (investigation completion, feedback loops) as part of stewardship?
- Are portfolio companies AI- and crypto-risk ready, with evidence of governance?
- Do we assess fraud resilience as part of investment risk?
- Are fraud disclosures part of stewardship reporting?
- Do we engage with boards on fraud oversight maturity?
- Are ESG metrics tested for fraud vulnerability?
- Do we monitor fraud litigation and regulatory exposure in portfolio companies?
- Is fraud risk embedded in exit strategy planning?

## External auditors

- Have we challenged management's assertion of 'no fraud' with evidence (e.g., fraud risk assessment, whistleblowing logs)?
- Have we discussed fraud risk factors as a team, setting aside assumptions about management integrity (ISA 240 para 16)?
- Do our audit procedures address incentives, override risks, and third-party exposures – not just controls on paper?
- Have we considered outward-facing fraud risks (eg, ECCTA failure-to-prevent obligations) in our risk assessment?
- Do we have escalation protocols if fraud indicators emerge during the audit?
- Are we using forensic specialists or data analytics where fraud risk is high?
- Have we documented how professional skepticism was applied in key judgments?
- Do we test management override and collusion scenarios?
- Are fraud risk assessments reviewed and integrated into audit planning?
- Do we assess client readiness for ECCTA and POCA exposure?

# 11. Closing remark

**On 2 December 2024, the twenty-third anniversary of Enron's bankruptcy filing, rumours began to spread that the disgraced energy giant had returned. A sleek new website, enron.com, appeared to show that the company reincorporated under its original brand. While people on the internet debated whether it was a prank or a proper comeback, the story carried symbolism.**

The Enron collapse, synonymous with corporate fraud on a planetary scale, was a seismic event that reshaped US corporate governance and audit regulation, with global ripple effects. Stronger audit oversight, board independence requirements, and disclosure rules – many regulations across the globe were influenced by the Sarbanes-Oxley Act (SOX) and its sweeping provisions for corporate accountability. Given the decisive regulatory response, it seemed reasonable to assume that the problem of fraud had vanished into the annals of history.

Not at all. Two decades after Enron's bankruptcy, we are sleepwalking into a fraud epidemic. Fraud is on the rise in many areas, particularly in digital, financial and consumer domains. It is increasingly sophisticated, powered by automation, AI, deepfakes, synthetic identities, and organised criminal networks. Each wave of innovation creates new, wider attack surfaces, and fraudsters pivot faster than regulators or enforcers can respond. This is why the focus of the newly enacted ECCTA on 'failure to prevent fraud', making large companies (and, indirectly, their boards and senior management) liable if they don't have adequate procedures to stop fraud, is so timely. It's also very much in the spirit of SOX's 'internal controls'.

But the worst of all is how fraud has become normalised, starting from the very top of corporate hierarchies. No wonder respondents in ACCA's coalition survey name 'lack of ethical leadership and accountability' as on the main drivers of fraud (Figure 6.1). It's time we ask: how can boards do more to allocate priority and resources to combat fraud?

The idea that lies on the surface is that the world of 2025 looks very different from 2002, when the SOX was introduced. Green fraud. Cyberfraud. Deepfakes. Did we even know these words back then? Innovations emerged, and new developments occurred, and, as is often the case, the types of fraud have multiplied as well. Loading all that onto audit committees – the 'kitchen sinks' of the board – has proved ineffective. Several high-profile scandals, including those involving the Post Office, Carillion, and Halifax Bank of Scotland, have clearly demonstrated that risk management and internal controls cannot be outsourced to independent directors alone.

Fraud prevention is every director's business: protecting the company, its stakeholders, and their own liability. The full board must demand role clarity and relevant data from management, connect the dots on fraud risk across the enterprise, and cascade the sense of urgency down the organization. They must also ask harder, better questions. One of these is 'Who's accountable for fraud risk in our Three Lines?'

Tellingly, this study leaves that question unanswered. But the new impetus created by ECCTA is a chance to get the fundamentals right. How boards choose to lean in, rather than look away, will make all the difference. The practical steps in our *Calls to Action* supplement show what that looks like in governance terms.

Public records show that in 2020, the Enron trademark was bought for $275. Did we actually learn the lesson, or is the next Enron only a matter of time?

**Vera Cherepanova**, chair of ACCA's Global Forum for Governance, Risk and Performance

# Appendices.

## Appendix A: How our ‘prevalence vs materiality’ matrix compares to established typologies, such as the ACFE Fraud Tree

**Boards and practitioners know the ACFE Fraud Tree, a global taxonomy that groups schemes into asset misappropriation, corruption, and financial statement fraud. It’s excellent for classification and case learning but our study adds two lenses to this:**

Table A1: Comparing typologies of fraud

| FRAMEWORK | WHAT IT PROVIDES | WHERE IT HELPS | WHERE ACCA SURVEY ADDS VALUE |
|---|---|---|---|
| **ACFE Fraud Tree** (Asset Misappropriation, Corruption, Financial Statement Fraud) | A taxonomy of schemes. Widely taught and adopted; useful for case coding, training, and detection. | Explains ‘what type of fraud it is.’ Good for auditors, investigators, and benchmarking. | Our respondents show that schemes aren’t enough – boards also want to know how often and how hard different frauds hit. |
| **Prevalence–Materiality Matrix** (ACCA survey) | Two-axis lens: fraud frequency vs severity of impact. | Prioritisation: helps boards decide where to spend time, money, and controls. Eg procurement is common but mid-level materiality; cyber is rarer but catastrophic. | Adds nuance: prevalence ≠ materiality. Shifts focus from ‘fraud exists’ to ‘fraud priorities’. |
| **Convergence & Value-Chain Lens** (our roundtables & analysis) | Shows how cyber access, procurement manipulation, corruption, laundering and identity frauds interact in organised playbooks. | Assurance design: organisations see fraud not as siloed but as ecosystem risk spanning suppliers, partners, platforms, and regulators. | Goes beyond classification to systemic view. Integrates organised crime, geopolitics, and technological enablers (AI, crypto). |

**Key takeaways**

**Typologies are not competing but complementary.**

Use the Fraud Tree to diagnose and teach schemes, the Prevalence–Materiality Matrix to prioritise investment, and the Convergence/ Value-Chain lens to design defences that match how fraud actually operates today.

# Appendix B: Fraud risk assessment frameworks – a comparative view

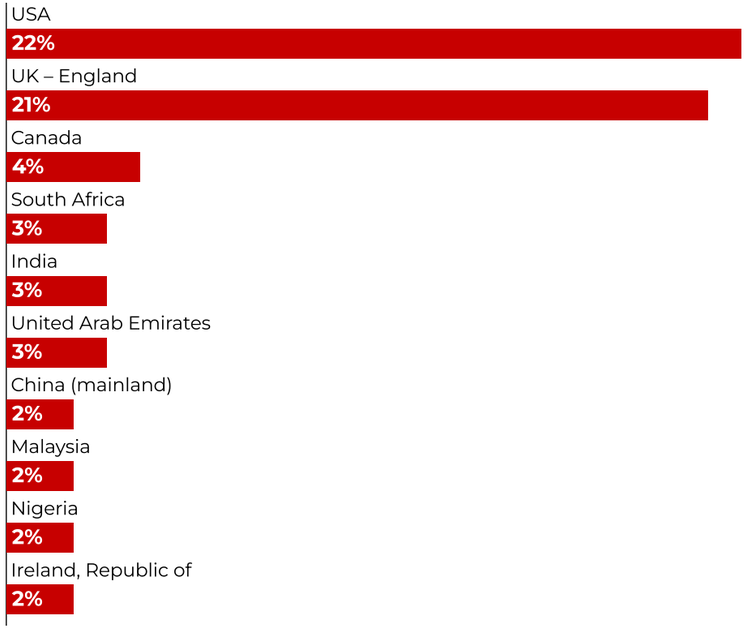
**Organisations and investors employ various frameworks for assessing fraud risk. Understanding how these approaches complement each other helps practitioners select appropriate tools and avoid gaps in their assessments.**

Table A2: Comparing Fraud risk assessment frameworks

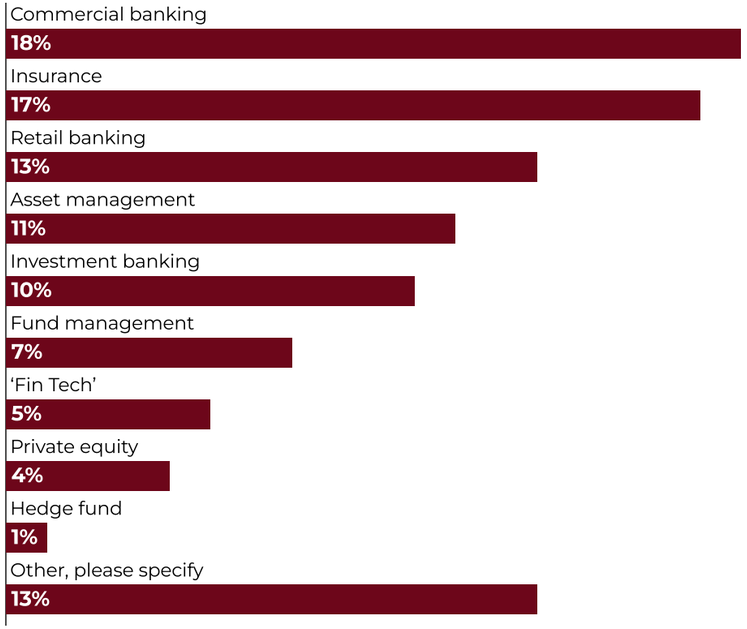
| FRAMEWORK/TOOL | PRIMARY PURPOSE | STRENGTHS | HOW IT COMPLEMENTS OUR RESEARCH |
|---|---|---|---|
| **ACCA/Coalition Survey Prevalence-Materiality Matrix** | Understanding which frauds occur most frequently vs. which cause greatest damage | Captures real-world experience across sectors/ regions; prevents treating all fraud types equally | Provides the 'what to look for' based on sector and context |
| **ACFE Fraud Tree** | Categorising fraud schemes into asset misappropriation, corruption, and financial statement fraud | Comprehensive taxonomy; widely recognised; useful for classification and investigation | Defines fraud types; informs detection and investigation approaches |
| **TI Business Integrity Tool** | Pre-investment due diligence for investors assessing organisational fraud risk maturity | Sector-specific questions; progression from gross to net risk; actionable assessment framework | Operationalises the prevalence-materiality insights into investor due diligence process |
| **TI Corruption Perceptions Index & Contextual Risk Resources** | Understanding country-level corruption and governance risks | Macro-level risk indicators; helps contextualise organisational risk within broader environment | Informs the external risk factors that shape organisational fraud exposure |
| **The IIA's International Professional Practices Framework (IPPF), including the Global Internal Audit Standards** | Integrating fraud risk into internal audit programmes | Focus on assurance role; audit planning; independence considerations | Addresses how internal audit contributes to fraud risk management without becoming default owner |
| **ISO 37001 (Anti-Bribery Management Systems)** | Establishing and certifying anti-bribery programmes | International standard; certification option; structured approach | Provides benchmark for policy frameworks and control maturity |

# Appendix C: Survey respondents and other demographics

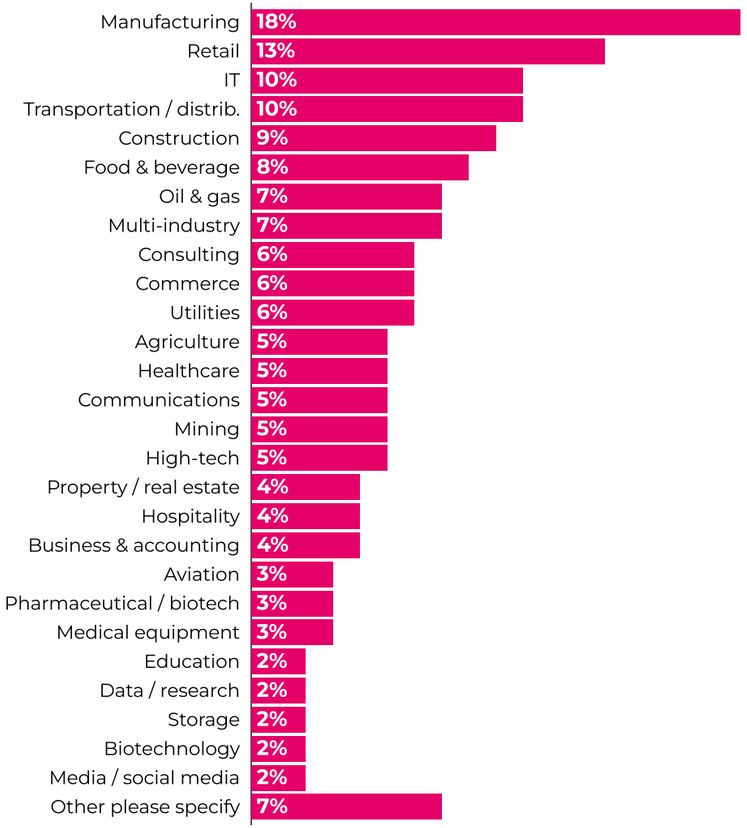
## Top 10 countries



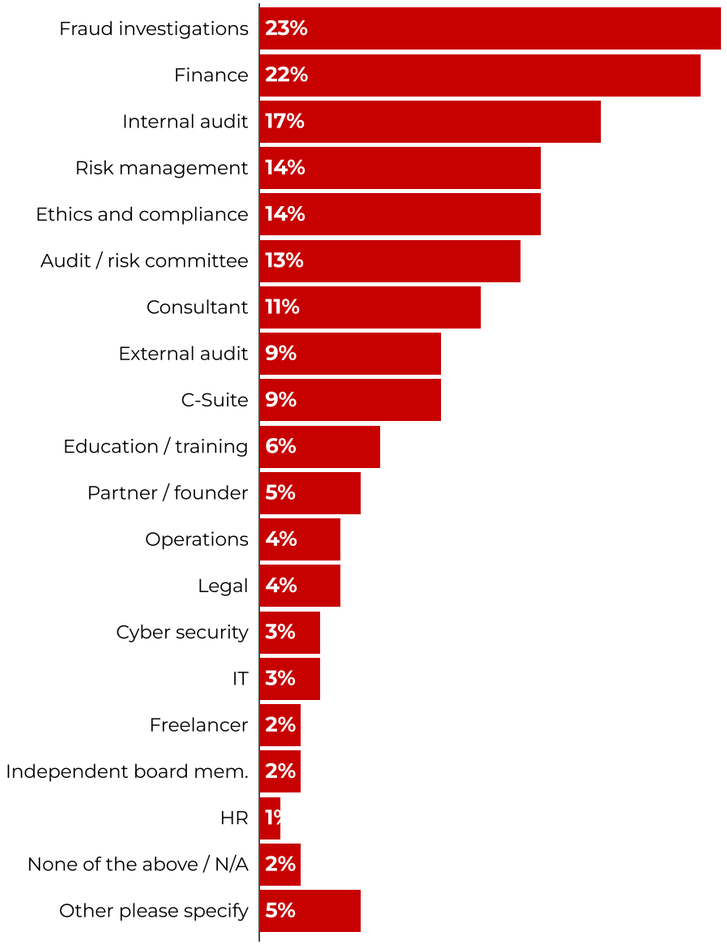

## Sub-sectors – financial services



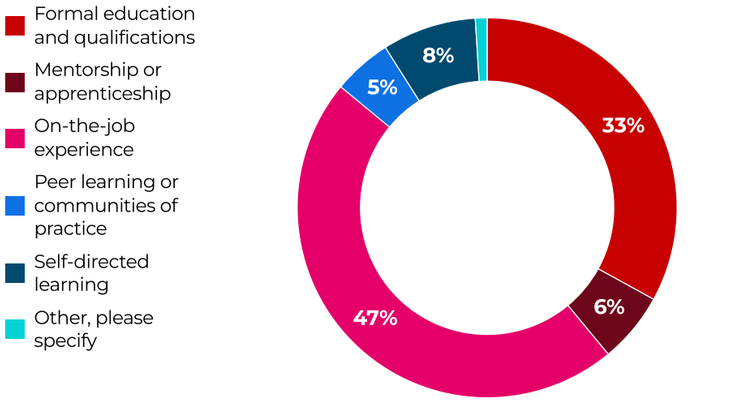

## Industries



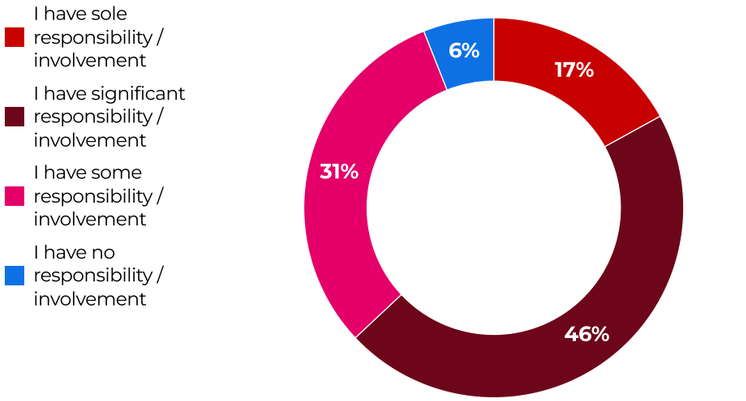
## Function where you work



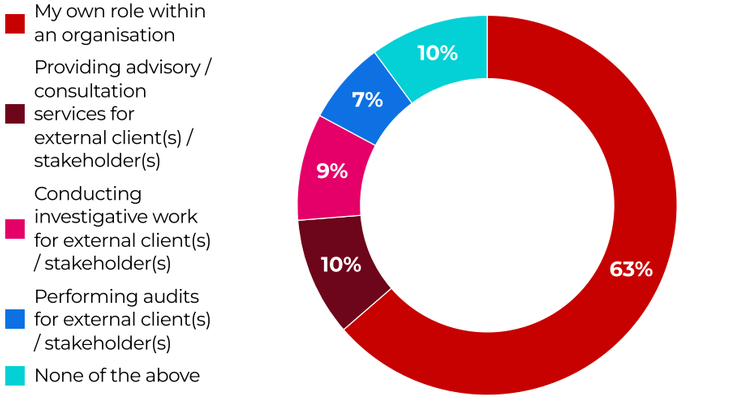

## Learning



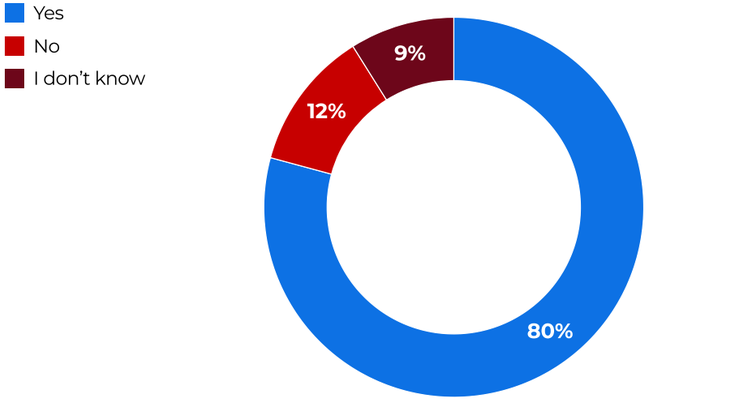

## Describe your day-to-day dealings with fraud




## Perspective – in terms of your role / services you provide




## Do you have any awareness / knowledge of what goes on?



# Appendix D: Further resources

Risk culture: Building resilience and seizing opportunities

Risk cultures in banking: Where next?

Risk cultures in healthcare: The role of accountancy

Way forward on fraud: A multi-stakeholder approach

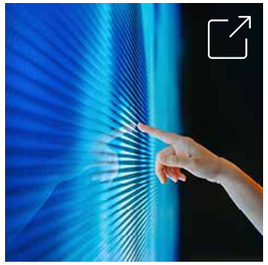
Combatting fraud in a new era of accountability

Combatting fraud – navigating a perfect storm

(ACCA's Accounting for the Future November 2025 conference)

ACCA's risk culture podcast series, including anti-fraud and cybersecurity episodes

Economic crime in a digital age



AI assessments: Enhancing confidence in the use of AI

AI Monitor: Risk and responsibility

# Acknowledgements.


## ACCA's Special Interest Group:

Alastair Goddin
Andi McNeal
Ashu Sharma
Asim Ali Abid
Ben Cattaneo
Benito Ybarra
Bryan Foss
Charis Williams
Claire Jenkins
David Clarke
David Hare
Deborah Poulalion
Dr Roger Miles
Emma Parry
Hoe-Yeong Loke
Jane Walde
James Packer
Jason Piper
Julia Graham
Maheswari Kanniah
Mason Wilder
Monica Young
Pav Gill
Tom Reader
Rachael Johnson
Rupert Evill

ACCA
The Adelphi
1/11 John Adam Street
London WC2N 6AU
United Kingdom

020 7059 5000

accaglobal.com



THINK AHEAD