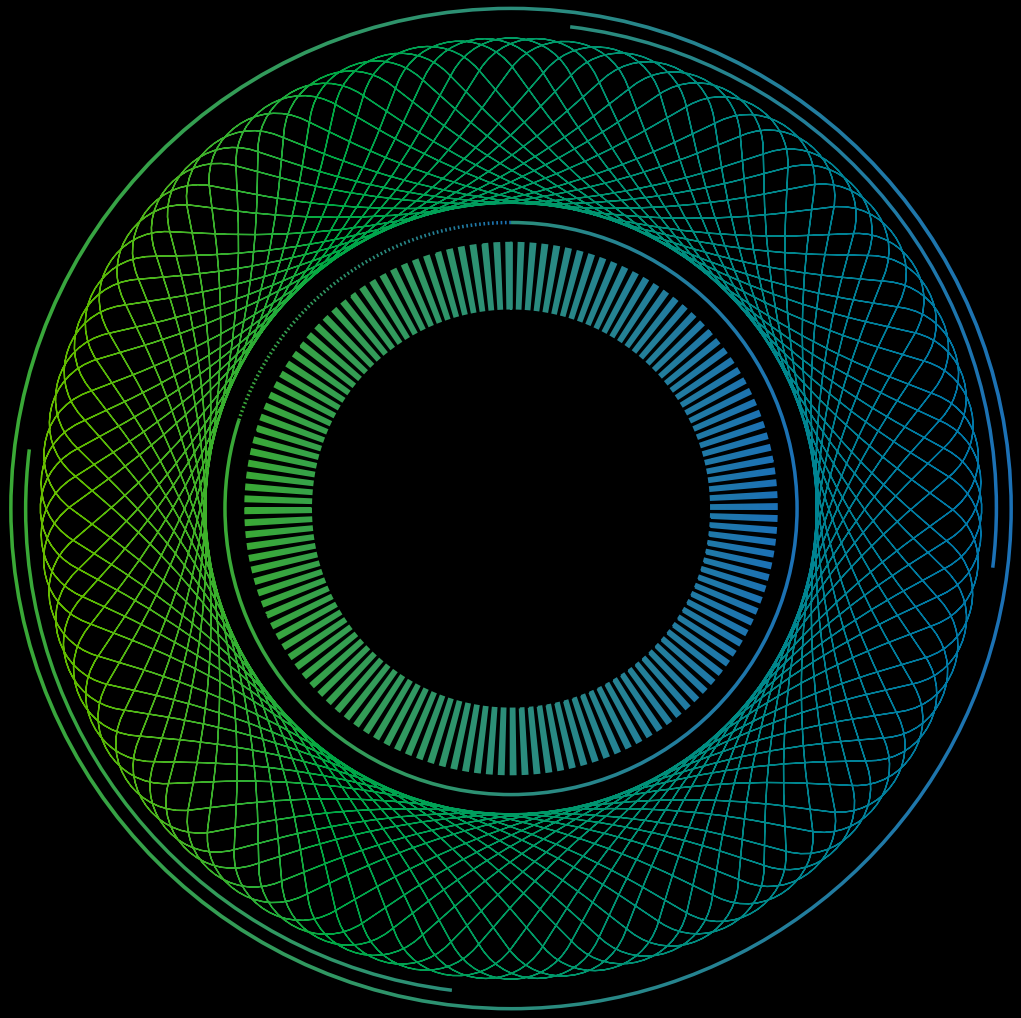
Deloitte.



The nature of fraud is changing
Act now to beat it

Contents

Foreword

As Head of Fraud and Investigations at Deloitte, in recent months it's become increasingly clear to me that fraud is rising steadily up the agenda. Whether against individuals or high-profile corporate failures, fraud is a growing societal and economic issue.

In June 2020 for example, a €1.9bn fraud led to the collapse of the payment processor and financial services provider Wirecard in Germany. There have been numerous other corporate failures due to fraud in the recent past.

The Office for National Statistics (ONS) Crime Survey for England and Wales shows that there were an estimated 4.6 million fraud offences in the year ending March 2021. That's a 24% increase on the 2020 figures. The survey also revealed that fraud and computer misuse offences have risen by over a third in England and Wales, driven largely by the COVID-19 pandemic.

According to Cabinet Office estimates, fraud and error already cost the taxpayer between £29.3bn and £51.8bn annually – and that is before the fraudulent misuse of the government's COVID-19 support schemes are taken into account. As you will no doubt have seen reported, the government furlough and loans schemes have been heavily targeted by fraudsters, with the Department for Business, Energy and Industrial Strategy (BEIS) previously estimating that COVID-19 loan losses due to defaults could cost the taxpayer up to £26bn.

Undeniably, the uncertainty and level of change over the past eighteen months has provided ideal conditions for fraudulent activity. Organisations have been under considerable financial and operational pressure due to lockdowns and the economic environment. A rapid shift in working patterns has provided opportunity, leaving many at risk of having their controls and procedures compromised, at a time when economic conditions provided greater incentive to commit fraud.

This problem is not a new one. Fraud has long been a huge area of concern for individuals, businesses, government and regulators alike. Yet fraudsters continue to evolve their methods with frightening sophistication, with many frauds now driven by online methods such as cyber-attacks, email interception or phishing attempts.

The BEIS consultation on audit reform has proposed specific recommendations around fraud. Similarly, in June 2021 the Law Commission launched a consultation on behalf of the government titled "Seeking views on whether and how the law relating to corporate criminal liability can be improved".

One outcome of this may be the introduction of a 'failure to prevent' offence for forms of economic crime such as fraud, similar to those that exist under the UK Bribery Act 2010 and Criminal Finances Act 2017. Whilst these suggested changes are still under consultation, new legislation is likely to come soon.

At the same time, the government's Economic Crime Plan (2019-22) has set clear ambitions for combining the capabilities and expertise of the public and private sectors to collaborate on a new, cross-system approach to address fraud and economic crime. Action Fraud is due to be replaced by the City of London Police in the near future to improve the development of intelligence and action taken as a result of reported frauds. Whilst much needs to be done this could be a welcome development for the fraud reporting, intelligence and investigation ecosystem.

In summary, there is more scrutiny than ever on organisations with regard to the steps they are taking to manage and mitigate fraud risk. The focus of public scrutiny on how organisations conduct their business and how they interact with the broader community is as never before. It is also key to note that the fraud threat to organisations is more than just financial. Of equal significance is the reputational threat: fraud or misconduct that may be financially immaterial in itself can still cause far-reaching reputational damage and resultant collateral damage.

We are therefore on the cusp of significant change, in terms of how we tackle the threat of fraud in the UK. Change that will impact all organisations across the private and public sector, and should be embraced wholeheartedly if we are to maximise its impact. This is why I'm pleased to have this opportunity to present our research into the very real risks that fraud presents – and the ways in which you can work to combat it.

Jules Colborne-Baber
Head of Fraud and Investigations, Deloitte

Our research

Amid such a dynamic and complex fraud landscape, we wanted to explore how different organisations are dealing with the current challenges, and how they are preparing for further potential changes associated with the latest consultations and proposed reforms.

Over the period December 2020 to March 2021, we conducted in-depth qualitative research to obtain a detailed, nuanced understanding of market perspectives on the issue. We recognised a growing appetite for peer insights and knowledge of what constitutes best practice, when it comes to fraud risk management.

Our interviewees were senior level individuals; primarily a mix of audit, compliance, finance, legal and risk roles, from a range of industry sectors. We also captured the board perspective by including Chair of Audit Committee and NED roles.

This report explores the key themes arising from our research and examines the challenges that different organisations are facing as they tackle fraud risk. We find out how they have sought to address these challenges – and try to answer the question "What does good look like?"

"All companies will have a level of fraud, no matter how well they are run – it's a basic cost of doing business. The most serious fraud, however, can damage and even destroy a company."

Why should organisations act now?

There are three main factors that are driving a greater focus on fraud than ever before:

- Heightened awareness due to the number of high-profile corporate failures in recent years, coupled with the sheer volume of highly publicised, pandemic-related fraud incidents;
- Increased motive and opportunity due to the disruption and lasting changes brought about by COVID-19; and
- Evolving legislation – with greater scrutiny from the government, regulators and the public, changes to the legislative landscape are expected.

Heightened awareness

A thorough analysis of our research shows a general agreement that fraud risk has risen in recent years. Interviewees referenced that the number of high-profile corporate failures and fraud related incidents in recent years has led to increased awareness about the potential financial and reputational implications. There is now a greater expectation for boards to be on top of the problem, actively monitoring the risks and challenging the various functional heads on how they are managing and controlling the fraud-related risks that businesses face.

Increased motive and opportunity

In the last year, there have been a number of competing priorities for organisations trying to pivot their business models to cope with the challenges of COVID-19. They have battled for survival, as repeated lockdowns forced them to close or operate in very different ways resulting in lost revenue. And, whilst new supplier and other third-party relationships may have been set up in short order, others have fallen away. Many organisations have been reliant on the government funding schemes introduced to support them through the most challenging months of the pandemic. In particular, companies who have made significant claims on the furlough scheme are aware of the associated reputational risks if it transpires that due process has not been followed. The shift to home working also happened overnight, with increased levels of remote working now the norm. This has made it impossible for many organisations to monitor staff as before, or bring teams or groups of staff together, making it harder to maintain a positive anti-fraud culture.

"With the potential impending introduction of SOX in the UK we are very aware of the need to formalise some of our controls around the response to fraud risk. We are going through a process to document our controls and procedures at the moment."

All of these rapid changes have increased existing risk and created new risks. Even companies which historically considered themselves to have good controls have found it hard to respond. The fact is that COVID-19 has been an accelerator for change in many organisations. It has forced them to reconsider existing policies and procedures, and in particular, against a backdrop of increased levels of cyber-attacks, caused them to put in place more digital controls such as multi-factor authentication and digital approvals procedures. Some have also implemented remote monitoring to oversee staff activity and behaviour, navigating the challenges of how this may be perceived by employees.

Evolving legislation

Following several high profile corporate failures, including as a result of fraudulent financial misreporting, in 2018 and 2019 we saw three high profile reviews:

- John Kingman's review into the Financial Reporting Council, and auditor procurement and remuneration;
- The Competition and Markets Authority's study of the audit market; and
- Sir Donald Brydon's review into the effectiveness of UK audit standards.

The recommendations from these reviews were consolidated in a White Paper released by BEIS titled "Restoring trust in audit and corporate governance", which also introduces a package of measures aimed at improving the UK's audit, corporate reporting and corporate governance systems. These measures are likely to form part of stronger regulation improving the prevention, detection and reporting of fraud. Crucially, they will change how UK companies operate.

In addition to the above, more recently, the Law Commission has also launched a consultation to obtain views on how to improve the law on corporate criminal liability for economic crime areas, including fraud. This may result in 'failure to prevent' offences being brought in similar to those in place from the UK Bribery Act 2010 and Criminal Finances Act 2017.

Among many others, the BEIS white paper makes four proposals with respect to fraud, likely to form the basis of future regulatory requirements:

01. **Fraud risk assessment:** Actions may include undertaking an appropriate fraud risk assessment and responding appropriately to identified risks;

02. **Training & communication:** Promoting an appropriate corporate culture and corporate values;

03. **Implementing controls:** Requirement for directors to assess their own internal controls environment and report on its effectiveness; and

04. **Board-level reporting:** Require directors to report on the steps they have taken to prevent and detect material fraud.

The fourth recommendation is all about management taking responsibility and the importance of taking a proactive, top-down approach to improving protection against fraud risk and preparing for incoming regulatory requirements. It goes beyond compliance. It's also about focusing on good governance, sensible business practice and fostering the right culture to prevent loss and reputational damage. It will require every organisation to take a risk-based approach to reducing and managing fraud risks by ensuring that robust processes and controls are implemented.

Interestingly, among our research participants, there was a general awareness around the implications of the internal controls aspect of the BEIS consultation; however there is mixed implementation at present. In respect of the proposed control, reporting and Directors' statements changes – which have been nicknamed 'UK SOX' after the United States' Sarbanes-Oxley Act – those with a US presence already have much of what is expected in place. Others are starting to think ahead and are taking preparatory steps by documenting their controls and processes. However, many are not there yet.

Whilst there was some apprehension around the costs associated with the enhanced requirements of 'UK SOX', a number of functional heads welcomed the shift in emphasis, which will give them access to budgets to make necessary investment in resources and develop robust fraud risk management frameworks.

Our research suggested that at present, outside of the internal audit function, there are lower levels of engagement with the BEIS white paper. Many are adopting a wait-and-see approach with respect to new regulation, due to the many other pressing issues at hand. However, most acknowledge that ultimately everyone will need to take the issue seriously – particularly all public interest entities (PIEs) in the first instance.

Learnings from our research

From our qualitative dialogue with clients who kindly shared their time, opinions and experiences, it became evident there are significant differences between organisations regarding their position on addressing fraud and fraud risk.

Indeed, the fraud risk management spectrum ranges from proactive at one end to reactive at the other. The former tend to be larger, more mature organisations. The latter, smaller and less mature, or those who have recently undergone rapid business growth and change. However, there remains a number of more mature organisations who are still reactive in their approach to fraud.

Significantly, where a company sits on the spectrum seems to depend on how well they have addressed challenges within five key areas:

- Clarity
- Controls
- Culture
- Communication
- Checks

1. Clarity

The initial challenge: Defining fraud

Defining fraud is crucial to understanding the breadth of risks your organisation is facing; but getting the clarity necessary to do so is difficult. Fraud means different things to different organisations, which means understanding of its scope and associated risks vary considerably. Our research also revealed that the definition of fraud varies by organisation, with a number of factors playing a role.

First, the nature of an individual business is key to how it views fraud. While there are several good practices, there is no simple, one-size-fits-all approach. For example, the emphasis an organisation places on different types of fraud is dependent on whether it is customer-facing or B2B; whether it is regulated; and whether it is listed versus privately owned. Additionally, historical issues and the perceived potential for brand or reputational damage also have an impact – for example, an organisation with a history of fraud arising from accounting manipulation may have a different emphasis to an organisation operating in a sector where fraud in the supply chain is the most common threat faced.

Second, it was particularly striking how much a company's internal structure impacts on the definition of fraud. We will come on to roles and responsibilities later, but some organisations have a disparate structure, with different elements of fraud addressed by different functions (for example, cyber enabled fraud by the CIO and accounting manipulation risk addressed by CFO); whereas others have brought it under one functional lead.

Third, there was a recognition across the board that fraud risk comes from both internal and external sources:

- Internal factors include cash and asset misappropriation (including data) by employees and contractors, fraudulent statements (both financial misreporting and increasingly other types of reporting, such as environmental, social and governance statements) and bribery and corruption – including misconduct by agents and employees, but also conflicts of interest, such as non-arm's length pricing.

- External factors noted include asset misappropriation through external attack and IP theft, and misappropriation of data through cyber-attacks. A high-profile issue which came up repeatedly is supply chain fraud, including the product quality issues that have been the subject of numerous headlines, such as those surrounding food fraud.

What was clear is that fraud itself is seen as an incredibly broad area and one that is hard to define. Many respondents pointed out that the traditional definition is very narrow in some organisations, and this can lead them to fail to identify and address risk accordingly. Internally, there can be a tendency to see fraud simply in terms of individuals benefiting financially from theft or 'cooking the books' for personal gain. Employees do not necessarily think of fraudulent statements nor too-close relationships with suppliers as constituting fraud.

All respondents concurred that it is a complex and dynamic issue that covers a multitude of areas, thus making it immensely difficult to manage. So with no single agreed way to tackle or define fraud, there is considerable management interest in what peers consider to be best practice.

Fraud enabled by cyber channels is feared most

Even companies that consider themselves to have established controls are finding it hard to adjust to digital business channels, the shift in business models and how we work, including remote working and the rise in cyber enabled fraud.

A number of organisations noted that this new, ever-changing and relatively unknown area is rarely within the core expertise of those managing fraud and risk. The feeling of "being unable to cope" is concerning and frightening – especially since cyber-enabled attacks are perceived as the biggest area of fraud growth.

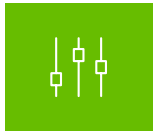
There are many factors contributing to an increase in cyber-enabled fraud. At its core are the levels of sophistication with which fraudsters are able to operate. For example, highly skilled cyber criminals have successfully hacked into many organisations' computer networks from different countries and successfully held them to ransom. Of smaller value but potentially much higher volume, fraudsters are now able to spoof entire email addresses. As a result identifying a man-in-the-middle fraud (where a fraudster intercepts an email chain and persuades a victim to change

"My biggest worry is cyber and data – this will never end. The battle between external threats and internal defence moves so quickly and it's hard to keep up."

"The hardest bit to integrate with everything else is the cyber risk. It's different and technical in a very different way."

bank details or make one-off payments whilst impersonating a senior employee or supplier) is hugely challenging. This has become as much about sensing something not being right as spotting a phoney email address and makes having effective controls in place essential.

In an office environment, networks may be harder for hackers to gain entry to and staff benefit from being able to run things past colleagues around them. But a drive towards home working, which comes with staff increasingly using personal devices (with limited built-in safeguards) and feeling isolated, only plays into fraudsters' hands.



2. Controls:
The importance of Fraud Risk Assessment – and the challenge in getting it right

The first stumbling block many companies say they faced is conducting a fraud risk assessment and defining their risks. There is however, a general consensus that this is an essential foundation to developing a robust approach to fraud, because if you have not identified and understood your risks you cannot be sure you are managing them accordingly.

Organisations are at different stages on their risk assessment journey. For some, a risk assessment cycle is well established, with risks identified and regularly reported to the board. Others do not have a well-established approach, despite recognising the importance of a robust assessment to identify and understand risks. When organisations have undertaken an assessment, it was typically conducted internally by a function head, with internal audit then conducting their assurance work against the identified risks.

Our research was supported by a recent poll we undertook of attendees at a fraud-related webinar, where 65% of our 80 respondents identified that they had not conducted an enterprise-wide fraud risk assessment within the last 12 months. For those that had, COVID-19 was the trigger for deciding to re-evaluate their risks, particularly with existing controls being less effective now the majority of the workforce was working from home.

Though it can be a challenge to devote sufficient time and resources to conduct a risk assessment, it was acknowledged that when events cause fast organisational change, an annual update is not necessarily enough. In fact, the importance of regularly reassessing the risks to check they are current was recognised as key, with some interviewees noting that they operate on both an informal and formal level, with some continually conducting informal risk assessments as part of day-to-day decision making.

We found that those organisations at the more mature stages of identifying and defining risk are often championed by an enlightened new CFO/CEO, or spurred on by a board unsettled by an issue or scandal too close to home.

Balancing use of technology with its impact on employees

Some organisations have implemented remote monitoring of staff – by tracking their computer activity, applying analytics and supervising transactions like home-based credit card handling. Respondents from more process-driven businesses lean towards putting maximum controls in place to eliminate risk to their organisation. Others felt that however good your controls, you cannot eliminate risk where people are involved and therefore their emphasis needs to be on culture and more preventive procedures.

Either way, it is essential that all measures are aligned with an organisation's culture, messaging and how things are communicated internally. For example, there is nervousness about how monitoring and observation is perceived by staff – especially the use of biometric data and remote screen monitoring. Indeed, many of those interviewed expressed concerns about the potential impact on employee morale. For that reason, monitoring of these types need to be justifiable, appropriate and perhaps most important of all, transparent. It is a challenge for internal communication as well as technology.

3. Culture

Led by the CEO and board, the right culture is essential

Interviewees noted that a culture of 'doing the right thing' must be driven from the top, and inevitably the approach to fraud is highly influenced by the attitudes of the board. Both the board and the audit committee need to set the tone and be prepared to challenge what they are being told by function heads and broader management. The most significant examples of internal fraud are felt to have occurred where there has been too much pressure from the top to drive certain results and where there was a culture of turning a blind eye to low-level incidents. Participants felt that the tone from above was most effective when it was part of a set of strong, overarching business principles.

In addition to this, the key risks with respect to culture were noted as:

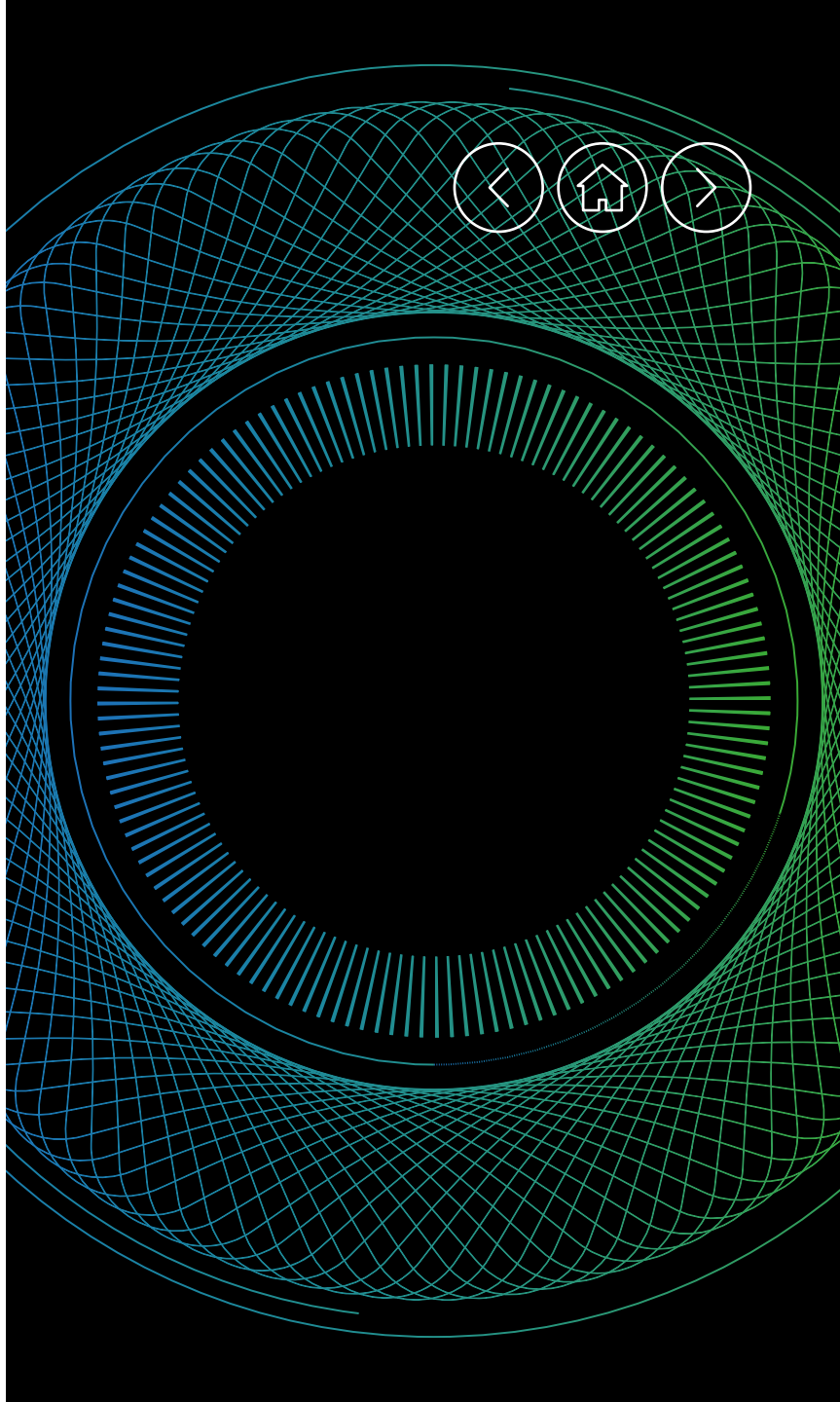
- Complacency – in terms of the board convincing itself that an incident is a 'one-off' and everything is fine;
- Companies who are particularly driven by the attitudes of senior leadership (for example entrepreneurial companies, or those with highly dominant personalities at the helm);
- Complete delegation to function heads who may then struggle to get board attention; and
- Non-existent or ineffective whistleblowing procedures (see below).

There is also a view among some that the consequences of infringements are only an impactful deterrent if made widely known and that a zero-tolerance approach needs to apply to senior as well as junior staff.

Two more points revealed by our research, which we explain further below, included: (i) the importance of staff feeling able to voice their concerns in a confidential and safe manner; and (ii) a company's willingness to invest in solving the fraud risk problem.

(i) A 'speak-up' culture

Interviewees agreed that a speak-up culture should be actively encouraged, with clear structures for doing so, all incidents investigated and the board notified. It is vital that employees are confident that their concerns will be taken seriously without repercussions. To that end, some argued that a whistle-blowing system should be managed independently of the organisation to be effective.



Some also reported a significant reduction in whistle-blowing during the pandemic, perhaps because those working remotely are less likely to raise concerns when they feel physically isolated from their team. Hence it is vital that a 'speak-up' culture is clearly communicated and applauded. This may require regular reinforcement via all appropriate channels, so everyone knows they are right and indeed expected to report their concerns.

Whilst most organisations have some form of whistle-blowing reporting hotline in place, it is essential its existence is well communicated and the reasons for any drop-off in reports at any point in time well understood. This is an area in which some felt they could perform better.

(ii) Willingness to invest

Our research also shows a variance across organisations in terms of their willingness to invest internal resource or seek external help with fraud related risks and issues.

In terms of internal investment, whilst there was a general consensus that to manage fraud risk effectively, risk and audit functions need sufficient resource in terms of people and tools, competing priorities can dampen an organisation's enthusiasm for investing. This brings us back to the attitudes and emphasis placed on fraud risk by senior management; some still rely on individuals or senior stakeholders to set the agenda and question whether this is enough. Organisations who currently manage fraud in a disparate way, with multiple areas taking responsibility, recognised the challenges they face as a result of not having an individual of sufficient seniority and board attention taking ultimate responsibility for fraud risk.

There seems to be less use of external help for fraud and risk management than in some other business processes (for example finance or tax). Historically, there is often a culture of trying to do as much as possible in-house – particularly if companies have a sizeable internal audit function.

However, in part this reluctance to seek external help is due to uncertainty about whether they are currently doing enough and what might be revealed by an external assessment. We found a great deal of interest in what others are doing and "what best practice looks like".

We found that the more proactive companies with fraud high on their agenda are seeking external assessment of how they are doing things, not just what they are doing, and looking for external challenge from outside their own echo chamber. By this they mean:

- An external view on the internal controls;
- Help in areas where they feel they lack internal resource or where the use of specialist skills is more universal (for example, cyber and technology or a forensic review);
- External investigation into high-profile events (like bringing in external help to respond to a major incident, or external assessment of their response to Government COVID schemes);
- Using external skills to learn what others have done (for example the development of a risk assessment and register, or learning about best practice controls and processes); and
- Support in those areas which are recognised as benefiting from more arm's length independence – a few of the companies we spoke to had employed external whistle-blowing facilities.

"You have to invest to prevent hacking and you have to be constantly on top of it – with the right levels of expertise, money and time being devoted to it. It's a bit like Health and Safety – it takes companies a few years to get into the right mindset. Typically CEOs have no idea how unprotected they are."

4. Communication
How can it improve risk management and governance?

We have already touched on how roles, responsibilities and an individual's specific experience can impact an organisation's perspective on fraud. There is a general acknowledgment that having the right people and breadth of skills in place matters more than anything.

Everyone we spoke to reported having previously either worked in a company or with previous leadership in their current company, where the board, CEO or CFO did not pay sufficient attention to fraud risk and NEDs did not ask the right questions. This meant that those in risk functions had to 'paper over the cracks', rather than operate a proactive risk management process.

It was also felt that the wide and varied nature of fraud meant it inevitably crossed multiple functions. Individual organisations structure roles differently – which can make it difficult for NEDs and leadership to benchmark how they are getting on, compared to others.

None of the organisations we spoke to had a nominated risk leader on the board and there was no single view on what constitutes best practice when it comes to organisational structure to address fraud. Many acknowledge the risk of potential blind spots or an overlap in responsibilities. As such, the relationships of the heads of risk and internal audit with the board and non-executives/audit committee is key. At a functional level, responsibilities can sometimes be a question of legacy, with regard to the role or title that has always been responsible for fraud. This is something organisations are beginning to question, given the dynamic landscape.

Communication throughout the organisation is seen as the key to good governance, requiring ongoing training on policies and procedures for staff at all levels. Interviewees noted multiple means of doing this, from written updates to roadshows and online training modules. It was recognised that education reinforces an anti-fraud culture; people need to be reminded about the policies and why they are important. They should also be regularly updated about what actually constitutes fraud.

"The CEO needs to have a very clear vision which is articulated to the leadership team and then used to guide the values statement and the KPIs that are measured. Everyone in the organisation needs to know what is expected of them."

Ensuring risk management is more than a tick-box exercise

Without good communication throughout an organisation there is a danger that risk management becomes a tick-box exercise that is not embedded. Risk management policies and procedures, and the reason they are there, need to be highly visible and understood across the organisation – recognising that it is everyone's responsibility, not just the risk function.

Examples from our research of how this is done in practice included those accountable for fraud risk management speaking directly with management throughout the organisation to ensure they understand the risks and procedures in place. Regular reminders for all employees, for example, through compulsory training modules were also mentioned. These were used to reinforce messages about what constitutes fraud, the policies and procedures in place to mitigate the risks of fraud, why they are important and the consequences of infringement.

"When we launched the whistle blowing facility we had to have a massive comms and awareness campaign to let people know it's right, proper and safe to report any concerns. You have to keep communicating to people so they know it hasn't gone away."

5. Checks
Who controls the controls?

Whilst interviewees universally agreed robust controls can assist in managing risk to an acceptable level, interviewees did identify the challenge of ensuring that the practical execution of these controls does not get in the way of doing business.

Despite the recognised importance of having an effective control framework to tackle fraud, only a minority were using external assistance to ensure anti-fraud controls are designed and operating effectively. The validations they have in place are typically a combination of:

- Challenge from the board/risk committee;
- Proactive audits – either against known risks, or on occasion conducting these randomly to uncover lesser considered risks; and
- Analysis of whistle blowing activity.

More proactive organisations are now looking to use technology and analytics to assist in monitoring, and to identify unusual patterns of behaviour or uncover new risks.

The role of technology

Looking specifically at technology and automation, this was seen by the majority as having a significant role to play in the mitigation of fraud risks – increasingly so, given the growth in remote working. The degree to which it is being used currently varies, with some respondents feeling that automated preventative controls can be relied upon too much, and there should always be a level of human review to check they are working as envisaged and not susceptible to circumnavigation. Further, there is a concern that use of technology needs to be culturally appropriate (for example the concerns around remote screen monitoring). Notwithstanding this, those investing in these tools said they had been able to detect incidences of fraud which they may have otherwise missed.

Our participants noted a number of barriers to making better use of technology:

- Their current IT systems infrastructure – particularly if there are a number of legacy systems;
- Restrictions in their own knowledge, and therefore ability, to make the case for investment, since they may not know "what good looks like";
- Budgets and internal IT resource – lots of competing demands on the IT budget and programming time;
- Analytics tools may result in a reduction in headcount requirements, so there are concerns about loss of team members; and
- Cultural and implementation concerns – the perceived view of 'big brother' monitoring and the employee issues that can arise from this.

Looking for problems

Those we spoke to showed a range in degrees of proactivity in their approach to fraud. Most acknowledged the risk of complacency: that they were looking for known risks, rather than seeking out new ones.

With that in mind, best practice is seen as doing regular, proactive deep dives into risks. Not just looking at areas of concern, but carrying out ongoing audits into new and emerging areas and looking for potential problems. Whether this actually happens largely depends on the resource available, and an organisation's philosophy and approach.

How can an organisation make effective use of technology?

While organisations have well-developed processes to respond to events, more proactive organisations are now looking to transform their operations by monitoring for potential fraud indicators.

Organisations have been investing in their technology and analytics capabilities to make intelligence-led decisions on fraud risk. In many cases, they have voluminous data sets containing indicators and artefacts which, if mined effectively, provide context and evidence of risk, or which could prevent a minor incident escalating into a crisis.

We see Subject Matter Experts (SMEs) in fraud and corruption domains working with forensic and analytical technologies to construct solutions tuned to a specific organisation. These solutions ingest existing internal data sources, enhance it with relevant external data, and apply business analytics to alert the organisation to potentially concerning activity in near real-time.

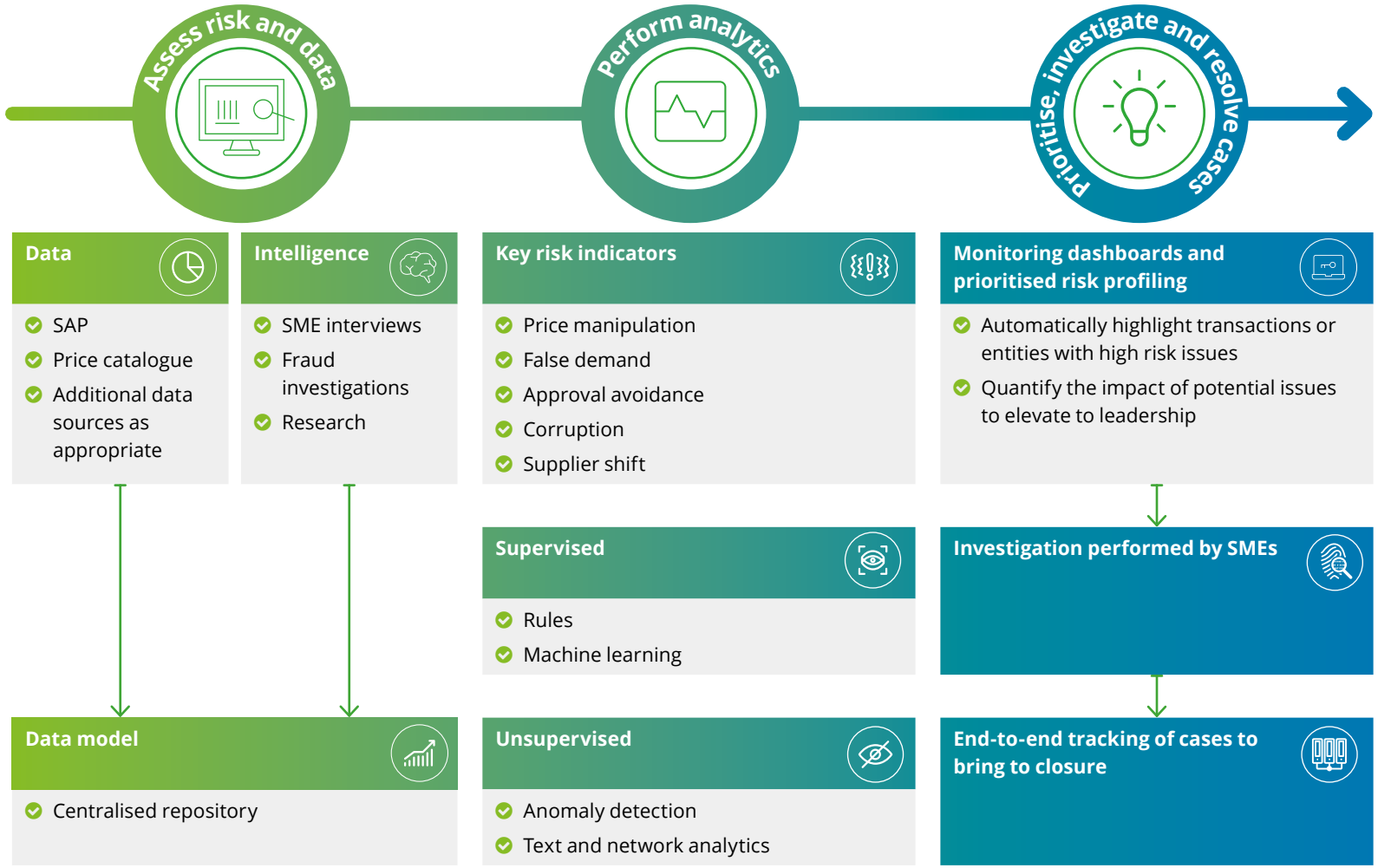
Comprehensive solutions range from simple rule-based alerting, through to anomaly detection using trained models that identify issues as they arise. They make use of Automation, Artificial Intelligence (AI) and Machine Learning (ML) in order to help organisations identify:

- Breaches against known thresholds or controls;
- Further instances of known fraud schemes or similar; and
- Anomalous behaviour that is previously unknown.

In practice, the precise components of a monitoring solution differ for each organisation. But all involve these three, fundamental steps:

1 Assessing the data and risk landscape;
2 Developing analytics that target key identified risks; and
3 Prioritising, investigating and resolving identified anomalies.

The three key components of a monitoring solution



Spotlight on: Developing a Fraud Risk Assessment

In our research, it was widely acknowledged that having a robust Fraud Risk Assessment in place is an essential first step to building an organisation's defences. But how do you go about producing one? Here's our guide to the key steps and considerations:

1. Involve the right people

It is often the first-line Risk and Compliance teams that drive the development of a Fraud Risk Assessment. But to be effective it needs to involve a wider stakeholder group:

- The first line of defence – those at the sharp end of the business – should be actively engaged throughout. Their experience and perspective can ensure key fraud risks and existing controls are identified. It is crucial to get their buy-in to the value of the process, to ensure they will implement any recommendations arising.
- The third line of defence may have insight into how effective existing controls are, and will play an important ongoing role in measuring its design and effectiveness.
- But ultimately, responsibility for having an effective anti-fraud framework in place is down to the board. An accountable executive should be assigned to oversee and approve the Fraud Risk Assessment, and ensure any resulting remedial steps are performed.

"The best practice model is to have maximum collaboration with all the other lines of defence in the organisation, focusing on the key risks and not wasting time on peripherals."

2. Ensure all areas of the business are captured and define the scope of fraud

Whilst your risk register may already include potential fraud risks, it is important to make sure the full activities of the business are captured. In doing so, you should consider all possible sources of risk across your business. You can do this by dividing it into assessment units – Sales, Procurement, Finance & Accounting, HR, IT and Inventory Management etc.

Then consider the potential types of fraud risk, such as:

- Internal fraud like expenses, payroll or procurement fraud, which can result in misappropriation of company assets;
- External fraud risk from your customers; for example, in the financial services industry, application fraud where fraudsters may impersonate victims and apply for a loan on their behalf;
- External fraud risk from suppliers, such as attempted bribery to win a major contract, or fraudulently inflated invoices;
- Manipulation of financial reporting, where a business's financial records could be altered or its financial performance misrepresented, to drive performance-related incentives;
- Fraud risk from cyber attacks; for example through CEO fraud, whereby an email chain can be intercepted as a fraudster impersonates someone in your business or a third party, to direct a fraudulent financial payment;
- Consumer fraud, whereby your own organisation may be impersonated by a fraudster in order to trick victims out of their money, in the belief they are making a payment to you for a service you provide; and,
- Bribery risk; many organisations maximise their efficiency by considering bribery risks as part of their risk assessment. This would include risks related to the winning or retaining of business, dealing with government-related parties or receipt of bribes by individuals within the organisation.

3. Initial information gathering – data sources to consider

There are several sources of information, both quantitative and qualitative, you might consider as a starting point of your risk assessment. For example:

- Quantitative information – financial losses due to fraud, market data or KPIs; and
- Qualitative information – Staff insights (e.g. via internal surveys), internal audit reports, risk registers, customer complaints, whistleblower reports or market trend analyses.

4. The approach to identifying fraud risk and controls

There are a number of techniques you can adopt to conduct fraud risk and control identification:

- **Questionnaire** – an effective way to identify and gauge risk across the business, including in multiple geographies and across all business units, is to distribute a fraud risk and controls survey to multiple individuals or teams. This can be useful to identify additional risks, potential gaps in controls, knowledge gaps of current employees, and it also provides an opportunity for employees to raise points they may not feel comfortable raising in a workshop environment.
- **Workshops** – with different assessment units, these can be an effective way to identify and prioritise fraud risk. They enable participants to interact, and often generate thought-provoking discussions. A high-level view of key controls can be identified effectively at the same time, making this a good way to challenge the first line into thinking about fraud risk.

"A sound compliance programme should start with a formal risk assessment, rather than relying on key stakeholders to identify risks based on their own perceptions, but we are not there yet."

- **Fraud risk framework reviews** – including policies, procedures, controls and risk appetite statements – a review of existing fraud (and/or wider economic crime) risk policies, procedures and documented controls can enable you to identify the existing measures in place.
- **Walkthroughs** – whilst workshops are useful for identifying overarching risks, conducting detailed walkthroughs with product or system owners whilst adopting a fraudster's mindset, can make identifying vulnerabilities easier.

5. Analysis and control mapping

The above steps enable the identification of a business' key fraud risks.

Initially, it is good practice to consider fraud risk at an inherent level – in other words, before the application of controls. This is usually done by analysing the impact and likelihood. Once complete, it is then important to consider the existing controls in place to mitigate these risks.
These should be mapped against the risks, whilst considering both their design and operational effectiveness. This enables the remaining level of fraud risk to be assessed and prioritised, by identifying exploitable vulnerabilities and helping to combat them.

6. Documentation

Once the analysis and control mapping is complete, key fraud risks and controls can be documented in an easy-to-understand form. Typically this is done in a risk and controls matrix, grouped by operating unit or function, and will include:

- Description of the fraud risk
- Inherent risk rating (considering both likelihood of its occurrence and impact)
- Description of controls in place to mitigate the risk
- Residual risk
- Recommendations (to address this residual risk)

Fraud risk assessment template

Fraud risk	Impact	Liklihood	Controls	Residual risk	Recommendations
Description of fraud risk	High/Medium/ Low	High/Medium/ Low	Description of controls in place to mitigate risk	Description of residual risk (i.e. due to missing or ineffective control)	Potential remedial measures to address residual risk

High level heatmaps can then be produced that show the residual likelihood and impact of every fraud risk identified.

Fraud risk assessment heatmap

Each number in the chart below represents a different type of fraud risk. For example, fraud risk 'one' might refer to the risk of financial misstatement fraud, which per the diagram would have a likelihood of 'possible' and a 'significant' impact. The range of risks will be different for every organisation.

Likelihood	Impact: Insignificant	Minor	Moderate	Significant	Major
Almost certain					
Likely		8, 15, 16, 18	2	4, 23	
Possible	9	7, 9	5, 6, 11	1	
Unlikely		3, 14, 21	10, 19, 20, 22	13, 17	
Rare			12		

7. Remedial measures and recommendations

On completion of your Fraud Risk Assessment, you will have a set of prioritised recommendations to close any remaining vulnerabilities. It is important to develop a clear action plan to execute these recommendations; one with the necessary board-level oversight (usually reporting through a board sub-committee, such as Audit & Risk). The Fraud Risk Assessment will also help your organisation to develop its management information and KPIs around fraud.

The steps outlined will enable directors to demonstrate clearly that they have considered the fraud risk to their business, and taken measures to close areas of vulnerability, thus satisfying their obligations under the Corporate Governance Code. Above all, a Fraud Risk Assessment should remain a dynamic live document – one that is updated on an ongoing basis to support your fraud management efforts.

"One of the struggles is how undefined fraud can be which makes it hard to have a heat map of where to go next. The NEDs are engaged but until it is clear what fraud entails it is hard to have complete buy in."

Reactive vs proactive fraud management

Where does your organisation sit on the fraud risk management spectrum?

There is a general sense that it is hard to identify any acceptable level of fraud risk exposure; there is always more one can do. We also observed a real spectrum of how proactively or reactively organisations address the issue. As you read about some of the challenges our interviewees have encountered, it may help to identify where your organisation sits on this spectrum.

Definition: In reactive companies, risks are poorly defined and understood, even if some controls are in place. The Head of Risk or Internal Audit function may not fully understand the breadth of the problem, or may struggle to get the board sufficiently engaged. Those with a more proactive approach have well defined risks, although the challenge is to design and implement systems in the right way, and ensure that the controls and culture are in place throughout the organisation.

Risk assessment: Some more proactive companies also talked about reviewing these frequently. In more reactive organisations, there has often been a significant exercise to identify risks initially, though these are rarely updated unless a problem arises. Where organisations are more developed, they talk about future-proofing risks rather than just trying to keep on top of known ones. It was noted that new senior personnel can often prompt positive re-evaluation, for example by identifying risks and gaps. An important first step in tackling fraud effectively.

Not surprisingly, events causing fast organisational change are the hardest to cope with. COVID-19 caused many organisations to revaluate their risks, particularly in relation to employees working from home. Sometimes they simply had no choice but to be reactive. Nobody can pre-empt the unexpected, but you can at least make sure you have processes in place to manage it as effectively as possible.

Culturally, reactive companies are often more entrepreneurial, with a CEO or board who does not prioritise or fully understand the risks and set the tone accordingly. They may be organisations that have been through a lot of change and growth and are struggling to keep up. Proactive companies have a greater degree of board scrutiny and challenge – including NEDs who ask the right questions. They have clear values and a strong anti-fraud culture, in some cases as a result of having had fingers burnt in the past.

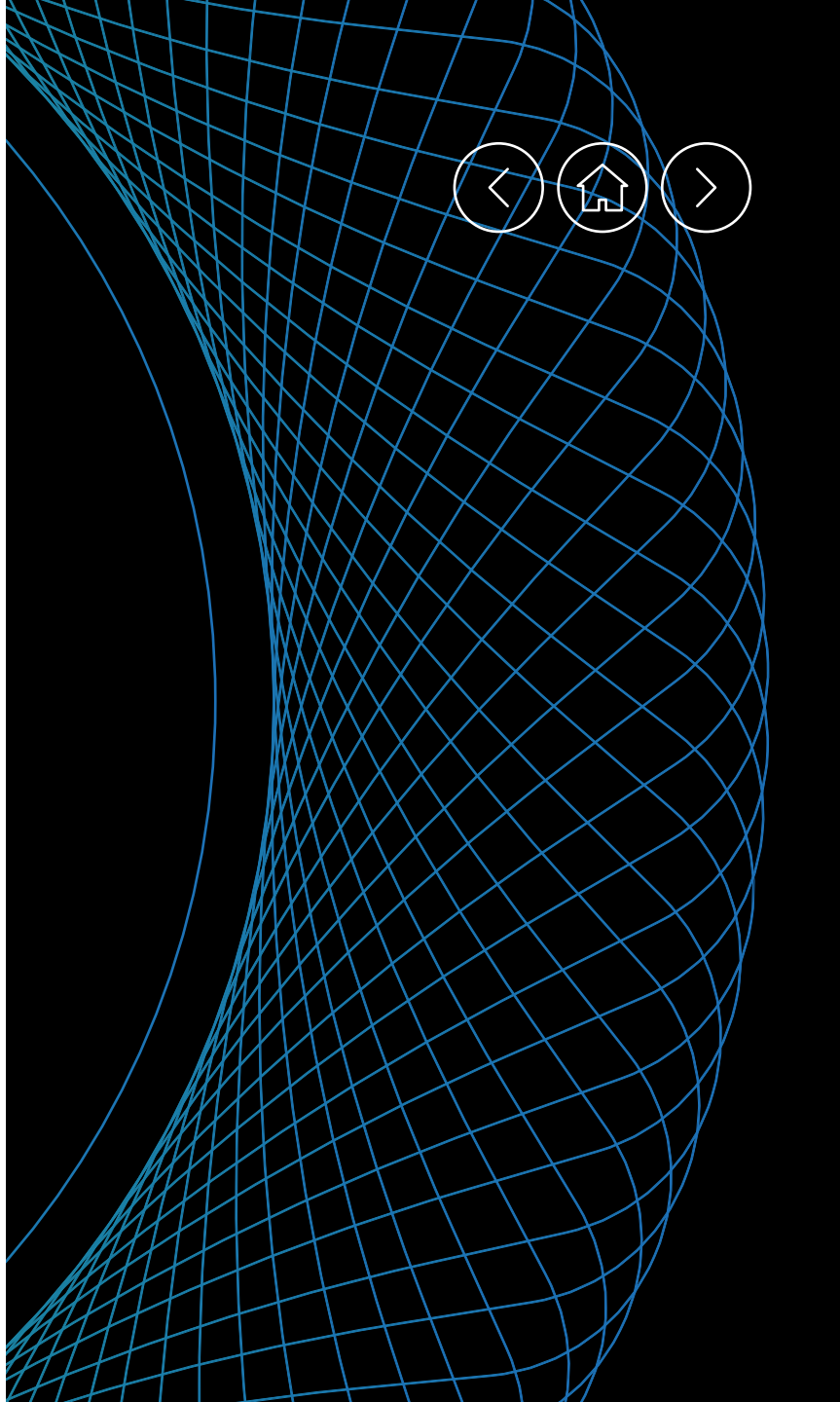
The organisational approach of a company affects the way it responds, including its ability to seek external help or invest in their fraud prevention and detection capabilities. They often feel they have no choice but to be reactive, placing more emphasis on checks and dealing with issues as they arise.

Many find it hard to secure the necessary budget, arguing for investment in technology and internal support. They are heavily dependent on those in risk functions convincing the board to invest.

Responsibilities and governance: In reactive companies, boards merely sought reassurance that this was in hand and had a higher degree of complacency. They were relying on functional heads to get this right, whereas proactive companies have regular reporting by heads into the board. The board itself is considered to be the main driver behind a positive organisational culture, or the lack of.

The longer a board has been in place, the greater the danger of complacency or being side-tracked by more pressing issues. This is surely something we can all relate to, in the light of Brexit and COVID-19.

Overall, the organisations we spoke to had fraud risk firmly on their agenda. But equally, there was a consensus that they could, and should, do more.



A range of approaches to fraud management

REACTIVE CULTURE ← → **PROACTIVE CULTURE**

"We have spent a huge amount of time, as a board and audit committee, talking about Brexit and associated risks. We have not been as proactive as we should have been at reviewing new regulations and associated risk. It's very easy to say 'We will deal with that tomorrow'."

"We are quite fragmented at present. We have internal audit, compliance and procurement, but we are not as joined up as we should be. The risk is the number of stakeholders that fraud covers, without anyone being responsible for the entity."

"The NEDs are engaged but until it is clear what fraud entails it is hard to have complete buy in."

"We don't check to see if fraud has happened, we check to see if fraud could happen. When it does happen it's usually the result of a confluence of things and that makes it hard to design out of the system."

"We are challenged by the board on a regular basis on the approach we take to each risk and the rank of the risks identified. We are regularly challenged on which risks are identified and the need to be creative and focus on future risks."

Main reactive characteristics:

- A lack of clarity
- Risk assessments are rarely updated
- Risks are not fully understood and not prioritised
- Higher degree of complacency
- No clear leadership

Main proactive characteristics:

- Risks are well defined
- Risk assessments are reviewed regularly
- Clear values and a strong anti fraud culture
- Greater degree of board scrutiny and challenge
- Full segregation of duties/lines of defence set up

Conclusion

Clearly fraud presents an enormous challenge and will continue to have a huge impact on all aspects of our society, on government, business and on citizens.

With the re-emphasised focus on fraud outlined by the government in their most recent Economic Crime Plan Statement of Progress, as well as potential regulatory changes that may follow the BEIS consultation, now is the time to reassess and re-evaluate your organisation's approach to managing fraud risk.

That is the bigger picture. But we must also keep sight of the fact that the **fight against fraud starts in the boardroom**, with the right culture, people, controls and expertise leading from the top. Without an anti-fraud culture from top to bottom an organisation will remain vulnerable.

That, ultimately, is "what good looks like".

We have also learnt that organisational self-awareness is key. Like personal self-awareness, positive change is achieved by honest appraisal, accompanied by a willingness to challenge, adapt and know when to seek outside help. By proactively and objectively assessing and evolving anti-fraud culture and processes from the top-down, it is easier to implement essential change.

Equally vital is hiring the best people. Ones who know what best practice looks like, and who are prepared to work together across functions and without barriers to achieve a shared goal. An organisation also needs to grant access to the necessary resources to invest in culture, the systems, solutions, controls and training that will make it hard to carry out fraud in the first place. Of course, this may mean bringing in third party support; actively seeking external challenge in the way things are done, and filling those skills and knowledge gaps any organisation may have.

The aim and effect of this is to design fraud out of the system, by concentrating on ongoing, proactive prevention rather than ad hoc reaction. That is what all organisations should aspire to, in order to win the fight against fraud. Whether it is 100% achievable, in the real world of personality-led boards, departmental politics and unforeseen global crises, is another matter.

However, any move in the right direction must be a worthwhile step in the essential fight against fraud.

"A lot of people want to achieve fraud detection. We are not interested in this – we want fraud prevention. And we are doing everything possible to achieve this."

Contacts

Jules Colborne-Baber
Head of Fraud and Investigations, Deloitte

+44 (0)7803 207417
jcolbornebaber@deloitte.co.uk

Amber Andrade
Director, Forensic

+44 (0)7900 135365
amandrade@deloitte.co.uk

Simon Cuerden
Partner, Forensic

+44 (0)7920 501641
scuerden@deloitte.co.uk

James Meadowcroft
Director, Risk Advisory

+44 (0)7946 650551
jmeadowcroft@deloitte.co.uk

Deloitte.

Designed and produced by 368 at Deloitte. J20065-2