Chartered Institute of Internal Auditors

AUDITBOARD

Fraud is on the rise:

Step up to the challenge

July 2022

Foreword

As we write this report, the war in Ukraine rages, inflation in the UK has hit 9%, and the cost of living crisis deepens. Organisations are also grappling with a myriad of other business-critical risks such as supply chain disruption, staff retention, and cyber threats just to name a few. This means that temptations and opportunities for fraud have increased, and fraudsters will take advantage of the situation using ever more sophisticated tools to commit their crimes. So, now more than ever, organisations and internal audit functions must be on the front foot to tackle fraud risk.

Organisations that have not traditionally regarded fraud as a high-risk priority must re-evaluate how they manage and communicate the risk. It is apparent from our research that, although the generic risk of fraud has been recognised as important, the response to it is inconsistent. Our key messages for organisations and internal audit teams are:

1. Internal audit functions should take a much more proactive role in the fight against fraud. In periods of heightened volatility, they should constantly revisit the elements of the fraud triangle (motivation, opportunity, rationalisation) to try and anticipate fraud. They will then be able to really challenge the board and senior management on where the risks may occur.

2. Organisations should conduct regular fraud risk assessments that consider the internal and external factors impacting the business. This is a fundamental step that should not be forgotten.

3. Boards and senior management have an important role to play in developing a positive fraud culture within the organisation, underpinned by the right tone from the top. Internal audit can support this effort by helping raise awareness around fraud and acting as a trusted advisor to the board and senior management on areas that need improvement.

4. Organisations and internal audit functions should be better prepared for the increased scrutiny and accountability on fraud from government, regulators, and the public. They should proactively look out for new rules and regulations on fraud that are coming down the track, and assess how they might impact their business.

We hope that this report acts as a useful prompt and encourages organisations and internal audit functions to raise their game in relation to fraud. As we gear up for more turbulent months and years ahead, now is the time to jump in with both feet and get ahead of the curve.

John Wood

Chief Executive Officer
Chartered Institute of Internal Auditors

Richard Chambers

Senior Internal Audit Advisor
AuditBoard and Former President
and CEO of IIA Global

Contents

About the research and methodology

Over the period February to April 2022, we conducted qualitative research to gather in-depth insights, practical views, and opinions on how organisations, and more specifically internal audit functions, are managing the evolving risk of fraud and preparing for potential changes linked to proposed regulatory reforms.

We conducted five sectoral roundtable discussions attended by a total of 33 participants composed of senior internal auditors, risk professionals and fraud experts from the private, public, and third sectors. We also conducted 18 one-to-one interviews with senior internal auditors and fraud experts to obtain more knowledge of what is happening on the ground and what constitutes best practice. Two of these interviews are presented as case studies of good practice internal audit in relation to fraud.

Organisations represented included: Openreach, John Lewis Partnership, OSB, InterContinental Hotels Group, AuditOne, SSE, Persimmon Homes, Shell, Coca-Cola Hellenic Bottling Company, EY, RSM, NatWest, Santander, Nationwide Building Society, 3i Group, Tesco Bank, Legal & General, Scotland Government, Government Internal Audit Agency, Worcestershire County Council, Warrington Borough Council, Salford City Council, Derbyshire County Council, Foreign Commonwealth Development Office, MIAA, The Orders of St John Care Trust, International Federation of the Red Cross and Red Crescent, Save the Children, St John Ambulance, Newcastle University, Action for Children, Brave Consultancy, Global Fund for Aid Tuberculosis and Malaria, The National Audit Office, and Cifas.

We would like to thank all participants for their time and contributions. Their involvement does not mean that they endorse the contents of this report.

The research also builds on existing literature recently published on fraud, including surveys, articles, industry reports, and thought leadership pieces, which will be referenced throughout the report.

Key takeaways

1. Fraud is on the rise. The disruption caused by the Covid-19 pandemic means that all elements of the fraud triangle have been heightened. This is going to continue because of the impacts of the war in Ukraine, rising inflation and the cost of living crisis.

2. The fraud regulatory landscape is changing too, and we can expect increased scrutiny and accountability from government, regulators, and the public moving forward.

3. The measures included in the BEIS white paper 'Restoring trust in audit and corporate governance' are likely to form part of stronger rules and regulations improving the prevention, detection, and reporting of fraud. Notably, there are increasing regulatory pressures for company directors to take greater responsibility for ensuring there are robust controls in place to prevent and detect fraud. In turn this is likely to mean company directors will require more assurance and comfort from their internal auditors regarding fraud. We would therefore encourage organisations and internal audit functions to reflect on these changes and how they may impact their policies and audit plan.

4. Boards and senior management should conduct a thorough fraud risk assessment, tailored to the business's industry and operations. The assessment should be periodically refreshed in line with the evolving internal and external environment.

5. Internal auditors are primarily responsible for providing objective and independent assurance to the board and senior management that the organisation has conducted an adequate fraud risk assessment and that the internal controls put in place to prevent and detect fraud are effective.

6. However, we believe that internal audit functions should go beyond what is required of them in the International Standards for Professional Internal Auditing (IPPF) and Codes of Practice and take a more proactive, 'big picture' approach to fraud risk. For example, internal audit should constantly revisit the fraud triangle to anticipate fraud, and they should be more vocal and challenge the board and senior management about where the risks may occur.

7. There are many other areas where internal audit can add value in relation to fraud. One increasingly important area is by using their skills and knowledge of the organisation to support data analysis in search of potential anomalies.

8. Boards and senior management have a critical role to play in establishing and implementing a positive fraud prevention and awareness culture across the organisation, underpinned by the right tone from the top. This will act as a powerful preventive control to deter people from committing fraud.

9. Part of developing a positive fraud prevention and awareness culture means encouraging transparency and openness when talking about fraud; establishing speak up channels where employees feel they can raise concerns without fear of retaliation; and delivering the message that internal controls to prevent and detect fraud are there to protect staff as well as the organisation.

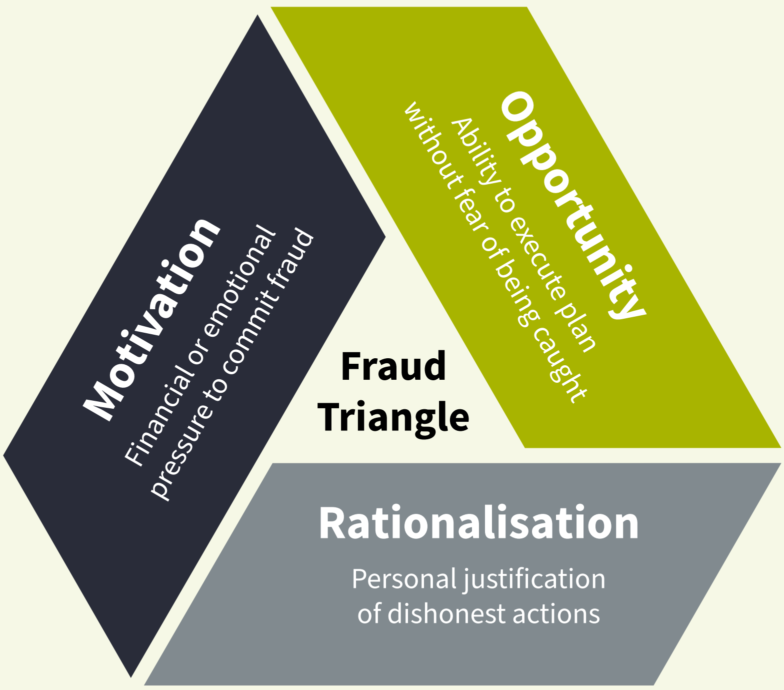
10. Internal audit has an important cultural role to play by helping raise awareness around fraud, promoting whistleblowing best practice, and acting as a trusted advisor to the board and senior management on areas that need improvement.

Introduction

The threat of fraud is one of the most common challenges that organisations face without regard to size, industry, or location. Fraud is on the increase globally and is so devastating that it can bring an organisation completely to its knees. Several high-profile corporate collapses linked to fraud, such as Patisserie Valerie, Carillion, and Wirecard, have made headlines in recent years and shown the financial and reputational impacts of fraud.

In the last two years, businesses have been under considerable financial and operational pressure due to the Covid-19 pandemic. This has created an ideal environment for fraudulent activity, where all elements of the fraud triangle (motivation, opportunity, and rationalisation) in which fraud thrives have been heightened. This is expected to continue – and get worse – as the war in Ukraine rages on, inflation in the UK hits a 40-year high, and the cost of living steadily increases. The world is in turmoil and fraudsters will take advantage of it. So now, more than ever, fraud should be on the radar of all organisations and their internal audit functions.

In its most recent global survey, the Association of Certified Fraud Examiners (ACFE) estimated that organisations lose 5% of their revenue to fraud each year.[1] The 2019 Financial Cost of Fraud report estimates that the cost of fraud for the UK is between £130bn and £190bn a year.[2] What is more, the Office for National Statistics (ONS) says that people are more likely to fall victim to fraud or cyber offences above any other crime. This gives an idea of the magnitude of the problem.



1. Occupational Fraud 2022: A report to the nations, Association of Certified Fraud Examiners.
2. The Financial Cost of Fraud 2019: The latest data from around the world, University of Portsmouth and Crowe.

According to research by Action Fraud, 80% of reported fraud in the UK is cyber enabled as criminals exploit technological advances to defraud organisations and individuals with increased sophistication.[3] A PwC Ireland survey revealed that business fraud was at a record high with 51% of respondents saying they have experienced fraud in the last two years; and cybercrime is by far the most prevalent type of fraud committed in Ireland (69%).[4] The trend is mirrored in Scotland with new government figures revealing a sharp uplift (63%) in fraud cases from April 2020 to March 2021 compared to the previous year.[5]

It is against this backdrop that last year the UK government published its white paper on 'Restoring trust in audit and corporate governance' with specific recommendations around fraud. The recommendations put increased emphasis on the responsibilities of company directors in relation to preventing and detecting fraud. In addition, 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 approach to address fraud and economic crime. The Economic Crime (Transparency and Enforcement) Act 2022 was fast-tracked through Parliament in March this year in reaction to Russia's invasion of Ukraine, and the Queen's Speech in May 2022 included the introduction of an Economic Crime and Corporate Transparency Bill. All of this is likely to result in new legislation and more scrutiny on the steps organisations are taking to manage and mitigate fraud risk.

In this context, closer attention must be paid to businesses' anti-fraud control framework if it is to remain effective in preventing, detecting, and responding to fraud. This leads us to the central question: who is responsible for fraud risk management? Boards have a critical role to play in developing effective governance processes and setting the right tone from the top. These are the foundations of fraud risk management, and the board should ensure that management implements policies that encourage ethical behaviour across the organisation. The board should also monitor the effectiveness of the organisation's fraud risk management programme, and this should be a regular item on its agenda.

Senior management has overall operational responsibility for the design and implementation of the organisation's fraud risk management programme, including conducting fraud risk assessments. It then involves implementing adequate internal controls and reporting to the board on the steps they have taken to prevent and detect fraud. Senior executives are also instrumental in supporting the board in developing a positive fraud awareness and prevention culture across the organisation: fraud is regularly talked about, policies on the consequences of fraud are set and communicated, and employees understand they can raise concerns without fear of retaliation.

Internal auditors, while not directly involved in fraud prevention and detection, have an important role to play in supporting the organisations they serve to better manage and mitigate fraud risks. Mainly, this is by providing independent and objective assurance to the board and senior management that the organisation has an adequate fraud risk management framework and that the internal controls put in place work effectively. But internal audit functions should go beyond what is expected of them in the IPPF and Codes of Practice by being more proactive, less complacent, and by using their unique place in the organisation to add real value. This includes raising awareness about fraud risks and making sure it is on the board's and senior management's radars, and anticipating fraud – rather than waiting for control failures to act. Internal auditors should be reviewing internal and external factors that could drive or heighten the increased risk of fraud or control failure.

This report seeks to offer useful insights and tips on how to tackle fraud risks, and hopefully delivers the message that there are many areas where internal audit functions can prove their worth in the fight against fraud.

3. Fraud crimes trends: 2020-21 Annual Assessment, Action Fraud.
4. Irish Economic Crime Survey 2020, PwC.
5. Fraud cases rise by 63% in 12 months, new police data reveals, Futurescot, 23 April 2021.

What is fraud?

Fraud can be defined as any illegal act characterised by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Fraud is perpetrated by parties and organisations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.[6]

The types of fraud are varied – they can be financial (e.g., inflating sales figures to achieve a bonus) or non-financial (e.g., identity fraud); internal (e.g., payroll fraud) or external (e.g., false insurance claims); cyber enabled (e.g., phishing scam) or not cyber enabled (e.g., cheque fraud). Fraud can be perpetrated by one or more individuals and, according to the ACFE, the median duration of fraud is 12 months before it is detected.[7]

The variety of fraud types has been reflected in our roundtable discussions. For participants from the financial services sector, external fraud such as authorised push payments or consumer fraud are top of their agenda. In the private sector, it could be as varied as fraudulent data breaches, misappropriation of assets, or payment fraud. Internal fraud, such as payroll fraud, has also become more prominent because of people working from home. The third sector faces similar issues, with the added difficulty that some charities and international organisations operate in highly unstable and corrupt environments. In the public sector, the fraudulent misuse of Covid-19 support schemes has made headlines and is something the government is now grappling with.

It was positive to hear that all participants of our roundtable discussions said their organisation had an anti-fraud policy that explicitly mentioned types of fraud. For some, this is part of a wider code of conduct and integrated into other policies, such as terms and conditions or procurement policies.

The multi-dimensional aspect of fraud is important and should be reflected on by organisations and internal audit when considering fraud risks in their business. As a minimum, internal auditors should ensure they understand the different types of fraud and assess whether their organisation has put the relevant controls in place to prevent and mitigate the risk.

According to the ACFE, the median duration of fraud is 12 months before it is detected.

6. Fraud and internal audit: Assurance over fraud controls fundamental to success, IIA Global, April 2019.
7. Occupational Fraud 2022: A report to the nations, Association of Certified Fraud Examiners.

The impact of the COVID-19 pandemic on fraud

The risk of fraud is constantly evolving. In the past two years, the Covid-19 pandemic has created the perfect environment for fraud to thrive. While organisations went into survival mode and faced immense pressures and economic uncertainty, a combination of financial and health threats have made people feel vulnerable – meaning that all the elements of the fraud triangle have been heightened.

As a result, there has been an increase of fraudulent activities during the pandemic, in line with what has been reported in the media. According to analysis by Which?, cases of fraud reported to Action Fraud rose by a third in 2020.[8] Most of the participants of the roundtable discussions agreed that there has been an increase of attempted fraud cases in their organisations. However, in terms of reported cases, the response was mixed. Most of the participants in the private sector didn't see an increase, or if they did, it wasn't a steep one. On the other hand, most participants from the financial services sectors have seen an increase of reported fraud, though mostly from an external perspective. In the public sector, we have seen media headlines reporting how the UK government lost £4.9bn to Covid loan fraud.[9] In response, participants of the public sector roundtables said that they had seen fraud risk assessments now embedded in all new schemes and much more encouragement to also do real time risk assessments to implement policies.

The roundtable discussions offered some further interesting comments. For example, some participants reflected that they had in fact seen a reduction in reported fraud cases at the initial stages of the pandemic, presumably because people's attention was elsewhere. Others commented that the increased rate of fraud discovery could be due to enhanced internal controls put in place because of the pandemic. Finally, one participant also mentioned that most of the fraud they were investigating now took place prior to 2020 – therefore suggesting that while the Covid-19 pandemic certainly had a massive impact on fraud activities, we have not yet seen to what extent.

So, how have internal audit functions responded to the increased risk of fraud? The most common answer is by putting extra layers of controls, especially with more people working remotely. Commenting on this point, Sandeep Das, Head of Internal Audit at St John Ambulance said: "What we need to do now is to consider how these then temporary controls may need to become permanent, as we settle into the new ways of working – and embed fraud risk mitigation into this process."

Ann Maria Keoghan, Senior Audit Manager at NatWest added: "One of the things that we have done this year is to put a financial crime and fraud risk goal on everybody's objectives to try and raise the discussion, asking people to look out for fraud and financial crime in everything that they are doing. It's about increasing the visibility and discussion and challenge to make people think about it in their everyday job and not feel removed from them."

Another impact of the Covid-19 pandemic on fraud is the increased difficulty in conducting audits virtually. According to a few internal

8. Online fraud up by a third in the UK during the pandemic, The Financial Times, 15 July 2021.
9. How the UK government lost £4.9bn to Covid loan fraud, The Guardian, 29 January 2022.

auditors we spoke to as part of the research, it is harder to build rapport behind a screen, read people's body language, or gather information. One of the CAEs we spoke to said: "It's very hard to audit remotely. Interviews are quite formal, and it is hard to get the 'unofficial' sense of people and process. Also, internal team interaction suffers from not sharing information over lunch or coffee."

Working from home has also impacted the visibility of staff knowing who they can talk to if they have an issue or concern. To address this, some organisations have made helplines more visible, for example.

While not all organisations have seen an increase of reported fraud cases during the pandemic, most have seen an increase in fraud attempts. Therefore, it is widely acknowledged that the Covid-19 crisis has created a more fertile ground for fraudsters to commit their crimes. Given the current situation in the world, including the Russian invasion of Ukraine, soaring inflation rates and increased cost of living, this trend is likely not only to continue, but to worsen. As a result, the risk of fraud should be on everybody's agenda, starting with boards and senior management teams who should ensure their organisation is protected against this heightened risk.

Internal auditors have an important role to play here, providing assurance to the board and senior management that the controls are adequate, but also adding value by understanding the fraud landscape and broader picture acting as a trusted advisor. This includes considering the elements of the fraud triangle and real-life scenarios to anticipate fraud. A simple example is that a person at a till may not be tempted to steal £10 when they feel comfortable financially but are far more likely to be tempted to do so if they cannot afford to pay their bills that week.

Questions for internal audit

- Do you use the fraud triangle to anticipate fraud risk within your organisation?
- Have you considered the impacts of the Covid-19 pandemic on fraud risk and has this been discussed with your board and senior management? What about the current geopolitical and economic challenges that we face such as the war in Ukraine and increased cost of living due to rising inflation?
- Have you seen an increase of fraud attempts within your organisation because of the Covid-19 pandemic and how has the organisation responded to this increase?

"I think what the last couple of years has evidenced is that major risks that we might have included previously in a severe but plausible category are going to happen. For me it really is about embedding a more flexible and agile approach to how we think about controls. Fraud risk controls are fundamental controls, whether they are over financial risk or other risks, but we are going to need more flexibility to monitor them more closely, more real time."

Carolyn Clarke, CEO, Brave Consultancy

The regulatory and policy context

Fraud and the law

It is only since the introduction of the Fraud Act 2006 that there has been a statutory definition of the criminal offence of fraud in England, Wales, and Northern Ireland. It defines it in three classes:

- Fraud by false representation;
- Fraud by failing to disclose information;
- Fraud by abuse of position.

In Scotland, fraud is covered under common law and various statutory offences. The main fraud offences are common law fraud, uttering, embezzlement, and statutory fraud. The Criminal Justice (Theft and Fraud Offences) Act 2001 updates and consolidates the law relating to dishonesty and fraud in the Republic of Ireland.

Other pieces of legislation capture fraud-related offences, such as the Bribery Act 2010, or the Criminal Finances Act 2017. Businesses in the UK and Ireland may also be subject to international regulations, such as the Sarbanes-Oxley Act 2002 (SOX) introduced in the United States.

A changing regulatory landscape

Amid increased fraudulent activities and following recent corporate collapses, there have been significant developments in the UK approach to combating fraud. 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 approach to address fraud and economic crime. This, among others, has resulted in the Economic Crime Act 2022. The 2022 Queen's Speech also included an Economic Crime and Corporate Transparency Bill, which aims to strengthen powers to tackle illicit finance and reduce economic crime, including fraud.

In June 2021, the Law Commission launched a consultation on behalf of the government seeking views on whether, and how, the law relating to corporate criminal liability can be improved so that they appropriately capture and punish criminal offences committed by corporations, and their directors or senior management. One outcome could be the introduction of a 'failure to prevent' offence for forms of economic crime such as fraud. This would be a huge step forward and would help raise the profile of fraud, ensuring there is greater engagement in detecting and preventing fraud.

Audit reform: prepare for increased scrutiny and accountability on fraud

Over four years and three reviews after the collapse of Carillion, last year the government published a detailed white paper on 'Restoring trust in audit and corporate governance'. Section 6.4 of the white paper is dedicated to tackling fraud and includes recommendations such as new requirements on company directors of Public Interest Entities (PIEs) to report on the steps they have taken to prevent and detect fraud. The white paper also proposes to strengthen the internal control framework for financial reporting adopting a 'SOX-lite' approach involving certification by company directors signing an internal controls statement.

The UK government has now committed to move forward with some of these reforms with the inclusion of a draft Audit Reform Bill in the 2022 Queen's Speech, starting with the establishment of a new statutory regulator, the Audit, Reporting and Governance Authority (ARGA). The bill is also expected to give ARGA effective powers to enforce company director's financial reporting duties, to supervise corporate reporting, and to oversee and regulate the accountancy and actuarial professions.

It is also worth noting that the bill intends to extend the definition of PIEs and include large companies regardless of whether they are admitted to trading on a regulated market. This means, however, that the new rules won't apply to public sector organisations or small/medium companies in the private and third sector. For these organisations, the rules could provide a benchmark of good practice.

So, are organisations and internal audit functions preparing for the new requirements? Although most of the participants of the roundtable discussions were aware of the white paper, not all organisations are preparing for the proposals. One participant from the private sector said that they had initially worked on the proposals quite aggressively, but now preparations have stalled as they await confirmation of what exactly the government intends to implement. For many, it is a 'wait and see' situation. From an internal audit perspective, one participant from the financial service sector said that they have had discussions around the white paper and have been looking at their key control systems to slowly move towards a 'SOX-lite' approach. Another senior internal auditor said that the white paper was a watching brief. However, for most internal auditors we spoke to, there was no programme of work underway in relation to the recommendations included in the white paper. This was somewhat disappointing given the impact these recommendations could have on the way businesses operate and the opportunity they present in terms of greater recognition and status for the internal audit profession within the wider corporate governance framework.

Whether the measures included in the government white paper become law or not – for example it has now been confirmed that the proposals for a 'SOX-lite' system will now be delivered through revising the UK Corporate Governance Code – we can expect increased scrutiny and accountability on the steps that organisations have taken to prevent and detect fraud. Notably, company directors will be asked to take greater responsibility and a more proactive approach to improving protection against fraud risk by ensuring that robust processes and controls are in place. It is also likely that company directors will seek more independent assurance from internal audit to make sure they comply with the new requirements.

As such, these changes in rules and regulation should be on all organisations' radars. Those falling under the new definition of a PIE should proactively look at how the new requirements may impact the way they operate. Other non-qualifying organisations should see the measures as good practice and consider implementing them within their business on a voluntary basis.

Questions for internal audit

- Do you keep abreast of regulatory changes in relation to fraud and how they may impact your organisation?
- Are you aware of the recommendations included in the BEIS white paper and is your organisation preparing for the potential new requirements?

Organisations' approach to fraud

Fraud is not a standalone risk

Fraud has long been an area of concern for businesses. According to Risk in Focus 2022, our latest annual survey of senior internal auditors across Europe, 20% of respondents said fraud, bribery and the criminal exploitation of disruption was a top 5 risk. Most of the participants of our roundtable discussions indicated that although fraud was not a top 5 risk, it was considered an important one and often appeared as a top 10 risk on the risk register.

However, several participants pointed out that fraud was blended into other risk areas, such as economic or financial crime, financial stability, or cybersecurity. This has been a recurring theme across all the roundtable discussions: fraud is not a standalone risk; it interconnects with a range of other risks. To illustrate this point, Jeremy Lawson, Head of Internal Audit at Persimmon Homes said: "Fraud does not necessarily meet our principle risk definition. We have a separate fraud risk register with about 60 or 70 types of fraud, but this did not justify having fraud as a principal risk in its own right. However, we probably all have cyber security as a principal risk. And what does cyber risk look like if you break it down? It could be a fraudulent mass data breach."

"You can look at risks from a process point of view, in which case every process has fraud risk associated to it. Or you can look at macro risks, such as cybersecurity, which is in itself a fraud risk. Fraud is really a subset of every risk."

Head of Internal Audit from a manufacturing organisation

Fraud risk assessment

When asked whether their organisation had conducted a fraud risk assessment, all participants of our roundtable discussions in the financial services sector responded yes. Nearly all in the private sector did so too and, for some, senior level ownership had been established for each risk. When they did not have a fraud risk assessment, it was either because it was currently being developed, or because they rather refer to an overall risk assessment.

The response was more nuanced in the public and third sectors. Some have a fraud risk assessment both at organisation level and programme level; others have a fraud risk assessment, but it hadn't been recently updated; and others simply did not have one.

Conducting a fraud risk assessment is an important step for organisations to effectively identify and prioritise areas of fraud risk within the business and ensure there are internal controls in place to prevent or detect fraud. The onus is on senior management to carry out the assessment as the first line. Internal audit, on the other hand, can provide assurance that the fraud risk assessment is fit for purpose.

Preventive vs detective internal controls

Once fraud risks have been mapped out, organisations should put in place adequate internal controls to prevent and detect fraud. These controls are varied and will depend on the organisation's risk appetite and tolerance levels, as well as the sector.

Some examples cited by the participants of our roundtable discussions include system controls, data mining, customer verification tools, the screening of third parties before doing business with them, whistleblowing, and fraud training. For many, it is a blend of preventive and detective controls, although for most the balance was on prevention rather than detection.

Main components of a fraud risk assessment (source: AuditBoard)

- **Description of fraud risks:** while fraud risks vary, examples include theft of assets, fraudulent disbursements, manipulation of expenses, and inappropriate journal entries.
- **Likelihood of occurrence:** though granularity can vary, define the probability of the fraud risk as remote to almost certain.
- **Significance to the organisation:** level of significance can also vary, but common categories include inconsequential to material.
- **Identification of anti-Fraud controls:** every organisation has internal controls to prevent fraud, and auditors must examine how robust these are.
- **Assessment of control effectiveness:** label controls as ineffective to very effective.
- **Fraud risk response:** after identifying a fraud risk, determine corrective action activities or additional controls that should be implemented.
- **Responsible person:** decide who will implement controls and mitigation efforts.
- **Monitoring activities:** establish monitoring activities that will be conducted and how frequently they will occur.

Risk appetite vs risk tolerance

When approaching the risk of fraud, it is important to distinguish an organisation's risk appetite and tolerance levels to fraud, as well as making sure that everybody understands the difference. Risk appetite can be described as the number of different types of risk a firm is willing to accept to achieve its objectives. As part of this, organisations recognise that they cannot remove all risks from their business. Risk tolerance, on the other hand, is the amount of acceptable deviation from an organisation's risk appetite. While risk appetite is a broad philosophy that guides an organisation's risk management efforts, risk tolerance is a much more tactical concept that identifies the risk associated with a specific initiative and compares it to the organisation's risk appetite. You can think of an organisation's risk tolerance for a specific initiative as that organisation's willingness to accept the risk that remains after all relevant controls are put in place.[10]

This sparked some interesting conversations during our roundtable discussions. Notably, there was a mixed response in terms of whether the risk appetite on fraud was clearly stated or not in the participants' organisations – for some it was implicit within wider policies, for others the risk appetite for fraud was clearly stated. One participant bluntly pointed out: "If you don't look you don't find. And if you don't find fraud, then you can say you've got a zero tolerance".

It seems that most organisations will openly declare that they have a zero tolerance to fraud, but this is where the confusion lies. According to the above definition, zero tolerance should mean zero instances of fraud. However, is this achievable? The answer is no. Paul Chapman, Deputy Head of Audit and Assurance at John Lewis Partnership commented: "The Partnership has a low appetite for fraud but recognises that as retailer it's almost impossible to prevent fraud from occurring whilst still trading, in spite of investing significant cost and resource in security controls."

In terms of tolerance levels, a few participants compared fraud to health and safety: there's absolutely zero tolerance for anybody to get hurt in the workplace, but how much would it cost to invest in a control system that would ensure this doesn't happen at all? You can't afford it. In fact, it's impossible. So, what organisations seem to mean when they declare they have zero tolerance to fraud is in fact related to the consequences of fraud: if fraud is discovered, the perpetrators will be sanctioned.

On the subject of sanctions, while the consequences of committing fraud are usually clearly stated in organisations' policies, in practice the treatment of guilty employees seems different depending on their importance in the organisation. One head of fraud we spoke to as part of our research commented: "We have had fraud allegations related to different types of employees, but they seem to be treated in different ways depending on their perceived worth."

This is the symptom of a bigger problem: the lack of transparency around fraud, which in turn participates in amplifying the negativities surrounding fraud.

The main lesson here is that fraud is happening. It's not a question of if, but of when and how. Therefore, boards and senior management should take this into consideration when developing their risk appetite and tolerance levels for fraud. Internal audit can assist them by providing independent assurance over the design and effectiveness of the risk appetite framework and tolerance levels. As part of this, internal audit could take a lead in encouraging a healthy debate around how to define tolerance levels and what could a proportionate response look like.

10. 'Risk appetite vs risk tolerance: How are they different?', Techtarget, October 2021.

"I think the least helpful thing we, as internal audit, can do is to adhere to the myth that fraud risk can be zero, this is simply not possible. When we talk about zero tolerance in audit, we are clear that is not zero fraud risk, but it's zero tolerance for people who have committed fraud against the organisation."

Danielle Eadie, Head of Audit, The International Federation of Red Cross and Red Crescent Societies

"It's a challenging one because we would all say there's a zero tolerance and absolutely there is a set of red lines that if they are crossed will cause people to be terminated and we communicate it. At the same time if we ask whether our control systems are set up for zero tolerance, the answer is no. We also have to make it safe for people to report their issues and concerns and the system is never perfect. In other words, consequence appetite, absolutely zero tolerance; but should we assume our control systems set up to zero risk appetite and zero tolerance, I don't think so".

Ken Marnoch, EVP Internal Audit, Shell

Questions for internal audit

- Has your organisation conducted a fraud risk assessment? Is internal audit included in the assessment process?
- Has the fraud risk assessment been recently updated? Have the impacts of the Covid-19 pandemic such as remote working, the changing regulatory landscape, or the rise in inflation been considered?
- Are the results of the fraud risk assessment implemented into the audit planning process?
- Has your organisation established its risk appetite and tolerance levels in relation to fraud?
- Has responsibility for fraud prevention, detection, investigation, response, and awareness been assigned within the organisation?
- Has your organisation established a set of policies and procedures to prevent, detect, and respond to fraud? These could include data analysis to identify potential signs of fraud or fraudulent examples themselves.

The role of internal audit in relation to fraud

Who owns fraud?

As it has already been alluded to, the onus of fraud risk management is on senior management as the first line. The second line facilitates and monitors the implementation of the internal controls framework, while internal audit, as the third line, provide assurance to the board and senior management that the controls put in place to mitigate the risks are effective. The IPPF includes standards that directly relate to fraud, such as:

- 1210.A2 — Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organisation but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.
- 1220.A1 — Internal auditors must exercise due professional care by considering: the extent of work needed to achieve the engagement's objectives; the probability of significant errors, fraud, or noncompliance; the cost of assurance in relation to potential benefits.
- 2060 — The chief audit executive (CAE) must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.
- 2120.A2 — The internal audit activity must evaluate the potential for the occurrence of fraud and the manner in which the organisation manages fraud risk.
- 2210.A2 — Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

Essentially, while it is not internal audit's responsibility to directly identify or detect fraud – this lies with management – it is their job to ensure the organisation has conducted a thorough and up to date fraud risk assessment to find areas that may be exposed to fraud. Then, it is also internal audit's role to encourage managers to put sufficient and adequate controls in place to prevent and detect fraud, as well as to monitor how effective these controls are in practice.

It is often the company's anti-fraud policy, set up by the board and senior management, and their expectation in relation to fraud that will determine the precise role of internal audit and its involvement in fraud prevention, detection, and investigation. This will normally be documented in the Internal Audit Charter, which is reviewed and approved periodically by the audit committee. It is important that internal audit activities are in line with the organisation's risk appetite and tolerance level to fraud, and that internal auditors maintain their independence and hold the appropriate training and qualifications.

"It is really important that the third line doesn't bleed into the first or second lines, but rather complement them by providing independent and objective assurance."

Colin Gray, SVP Risk & Assurance, InterContinental Hotels Group

Training and qualifications

Standard 1210.A2 explicitly states that internal audit must have sufficient knowledge to evaluate the risk of fraud. This includes understanding the characteristics of fraud, the specific techniques, schemes, and scenarios to commit fraud. Internal auditors should also use their skills in data analytics to identify trends and patterns that suggest fraudulent activity.

If internal auditors are involved in fraud investigation, it is imperative that they hold the proper qualifications such as the fraud examiner certification. A lack of qualification in this area could dangerously jeopardise the investigation and lead to disastrous outcomes for the organisation. For example, one of the people we spoke to as part of the research recalled a situation where internal auditors had been involved in a fraud investigation and did not follow adequate process when interviewing the alleged fraudster. When the case went to court, the internal auditor giving evidence was strongly criticised by the judge before the case was thrown out.

The internal audit function has an important role to play in helping keep their organisation on the front foot for fraud. To do this, internal auditors need to continually update their own knowledge of fraud. Therefore, regular training is important and internal audit functions should keep up the pace here as much as they can.

Where can internal audit add value?

While the role of internal audit in relation to fraud is clearly stated in the standards, we believe these requirements should be seen as the minimum expectation. The Chartered IIA recognises that, depending on the maturity of organisations, as well as the resources available, not all internal audit functions will carry out the same amount of activity around fraud. However, wherever possible, we would like to encourage internal audit functions to go above and beyond the standards and take a more proactive approach to fraud. There are many areas where internal auditors can add value to the organisation they serve in relation to fraud.

Firstly, internal audit is well placed to challenge the board and senior management to make sure the topic of fraud is alive and considered. Internal auditors should consider being more vocal about where fraud risks may occur and should flag up the areas of the business that are prone to them. When having these discussions, internal audit should take into consideration the fraud triangle and try to anticipate fraud. This involves understanding the environment in which the business operates as well as economic, social, geopolitical, and other external factors. For example, as we write this report, inflation just hit 9% and the cost of living is steadily rising. This heightened financial pressure on people will increase the likelihood of fraud. We are also experiencing a high staff turnover – the so-called 'Great Reshuffle' – and so organisations are losing knowledge and expertise. This means organisations are at higher risk while new joiners get to grips with the internal controls. So, internal auditors should ask themselves where their organisation is with regards to the fraud triangle and whether their internal controls are adequate. Internal audit can add real value here, by proactively monitoring their organisation's environment and anticipate fraud, rather than waiting for it to happen.

Another area where internal auditors can add value is by making sure that the other lines understand the "why" question. It is not enough to just run processes and controls; they need to understand why they are running them. Some of the senior internal auditors we spoke to as part of the roundtable discussions recognised this scenario where some people in the organisation seem to only follow processes. But they don't understand that what they are doing is a control. This is where internal audit is important, by asking further questions, maintaining their professional scepticism to get to the bottom of things, and not just believing what people tell them. Internal audit can help drive this curiosity across the business so that people really think about the processes and challenge them.

One participant of our roundtable discussions also pointed out the role of internal audit in challenging people's mindset on fraud, notably by highlighting that it is a safeguarding issue. The problem they raised was around senior management pushing back on additional internal controls because "they trust their staff" and that it would be dispiriting to put in place extra controls. But the response from internal audit should be: do you know the exact personal circumstances of all your employees? Do you know if an employee or one of their relatives might be in a position where they need costly medical care? Probably not. So, if you are giving employees an opportunity and they are desperate, it is an untenable choice. This also comes back to the fraud triangle mentioned earlier.

Internal auditors can also use their skills and knowledge of the organisation to support data analysis in search of potential anomalies. Indeed, data monitoring and data analytics tools are becoming increasingly more effective at reducing fraud loss and duration by detecting fraud schemes through unusual trends and patterns. Examples of data analysis activities are varied. In the retail sector, it could be looking for trends in till activity and identifying unusual refunds at certain times of day, by certain staff, and authorised by the same supervisor. In the oil and gas industry, using drones equipped with heat sensors to monitor human activity around parts of a pipeline at times when people should be onsite, and comparing this data against records of attendance, might help uncover anomalies. In a nutshell, data analysis is powerful because it can identify hidden relationships among people, organisations, and events; identify suspicious transactions; assess the effectiveness of internal controls; and monitor fraud threats and vulnerabilities.

Interestingly, a few internal auditors we spoke to mentioned that, according to them, where internal audit can add value is in the investigation of fraud. For example, one Head of Internal Audit said: "In my organisation, internal audit is involved in the investigation of suspected fraud. The alternatives are not as effective: management should not investigate fraud in their own operational areas, and our organisation, like many others, does not have a strong 'second line' (unlike, for example, the financial services sector, where there is a clear 'three lines' model). External investigators do not always have sufficient knowledge or understanding of our business and the different types of non-financial fraud that are possible, and may not be able to respond promptly. Internal Audit know the business, but are independent of it. We can also add value by feeding forward after the investigation, considering where and why the controls failed, and we work with management to make sure the controls are strengthened to prevent the failure/fraud from happening again."

The Chartered IIA recognises that not all organisations have the resources to afford a second line fraud investigation team and so, provided that they have the right qualifications, internal auditors can provide a suitable alternative, as long as they can remain independent and objective.

Finally, internal audit can add real value via their helicopter view of the business which allows them to join the dots. For example, there could be some isolated controls failures which, if put together, could present a huge opportunity for fraud. Internal auditors can pick-up on that and encourage the board and senior management to take appropriate action. To illustrate this point, Sue Davis, Internal Audit Manager at The Orders of St John Care Trust said: "I believe the value I can provide is actually trying to understand what is happening and how, joining those dots in reporting and logging an investigation, and resolving the issues. I can then take that to the executive and the audit committee for them to decide what actions need to be taken to strengthen the controls."

Top Tips

for internal auditors in relation to fraud

"I always see the role of the third line to be sceptical in the trust, verification and assurance we provide on systems. Our role is to ask not 'what if' but 'what when' and 'how do you know' types of questions and looking at the system from a total effectiveness point of view. No system is perfect and too often when you ask 'what if' the response you get are all the reasons why something won't happen as oppose to real reflection on the capability and resilience of the system. The third line is fantastic when it builds the capability of the first line who are actually managing the risks 24/7 365 days a year. That's where our role can make a significant and sustained difference."

Ken Marnoch, EVP Internal Audit, Shell

"Try to understand how processes and controls can be abused. It's not so much a top tip, as the standards require it to be part of our process, but it's an important step. It's a sad thing internal auditors would probably be excellent fraudsters, but thankfully we've chosen the right path, haven't we?"

Jeremy Lawson, Head of Internal Audit, Persimmon Homes

"Assume that fraud is happening, not that it might happen. While it's not possible to detect all fraud and we need to be realistic about this, don't become complacent. Don't be naïve and think that fraud doesn't happen to your organisation. It happens everywhere and the likelihood is that it is happening, but it hasn't been found yet."

Danielle Eadie, Head of Audit, The International Federation of Red Cross and Red Crescent Societies

"Don't stop asking about the basics! It's easy to think of controls around changes to supplier details as routine and well established, but many organisations are still falling victim to mandate fraud."

Vanessa Clark, Risk, Assurance and Compliance Lead, Action for Children

"I think establishing consistency on what we mean by fraud across the organisation is important. If we are not clear on that, then this causes problems in terms of the collection of data and reporting of fraud."

Zac O'Neil, Head of Counter Fraud Profession, Scotland Government

Where do internal auditors go to report fraud?

Both the Internal Audit Financial Services Code of Practice and Internal Audit Code of Practice (private and third sector) state that the primary reporting line for the chief audit executive (CAE) should be to the chair of the audit committee, and the secondary reporting line to ‘someone who promotes, supports and protects internal audit’s independent and objective voice’ – commonly, this is the CEO or another member of senior management.

This question around internal audit’s reporting line is particularly important in the context of fraud, given the recent fraud scandals involving chief financial officers for example. Most participants of our roundtable discussions said that they would report fraud in accordance with the Chartered IIA Codes, meaning to the chair of the audit committee or a senior member of executive management. However, some participants pointed out that the reporting routes depended on the nature of the fraud (internal vs external), as well as who the alleged fraudsters were (senior executive vs junior member of staff). In addition to the audit committee chair and the CEO, other routes include whistleblowing channels, the external auditor, and the police.

Most CAEs who participated in the financial services roundtable discussion said they had a clear reporting line to the CEO or the chief risk officer. One participant also mentioned an individual accountability process which looks at misconduct by individuals, which is led by the chief regulatory officer. In the third sector, some participants would also refer to a Serious Incident Group to discuss issues around safeguarding or the need to report the fraud to the Charity Commission for example. In the public sector, the reporting routes seem to differ from organisation to organisation. For some internal audit functions the first port of call is the external auditors, for others it is the counter-fraud team. One participant from the public sector roundtable discussion highlighted that for local authorities, if all else fails within the Council, the prescribed authority to report fraud is the National Audit Office (NAO). However, according to a report published by the NAO recently, not many local authorities mentioned the NAO in their policies as an avenue to report fraud. So, there seems to be a lack of communication there.

One participant to the roundtable discussions also underlined the importance of developing and maintaining a good relationship with the audit committee chair and chair of the board so that if CAEs need to have a difficult conversation – for example about a senior member of the executive team who has allegedly committed fraud – they can do this more sensitively. The onus is also on the chairs of the board and audit committee to ensure the chief audit executive feels comfortable coming to them about these issues.

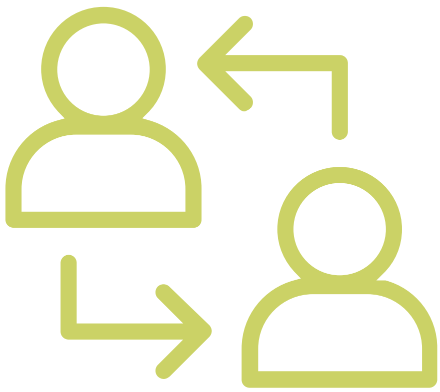
Relationship with the external auditors

Recent corporate collapses have put the role of external auditors in the spotlight and Sir Donald Brydon's review into the quality and effectiveness of audit noted a perceived expectation gap related to the external auditor's responsibility for fraud. Are external auditors doing enough to detect it? In 2021, the Financial Reporting Council revised International Standard on Auditing (UK) 240 The auditor's responsibilities relating to fraud in an audit of financial statement to provide clarity about the external auditor's obligations on fraud. One of these obligations is for the external auditor to obtain reasonable assurance about whether the financial statements are free from material misstatement due to fraud. External auditors are required to exercise professional scepticism to achieve this goal. Recommendations included in the BEIS white paper follow this trend, and it is expected that external auditors will be subject to more scrutiny and accountability in relation to fraud detection moving forward.

External auditors can make appropriate use of internal audit reports and findings to get a better sense of a company's approach to key risks such as fraud. As such, both the Internal Audit Financial Services Code of Practice and Internal Audit Code of Practice recommend that the CAE and the partner responsible for external audit should ensure appropriate and regular communication and sharing of information. The relationship between internal audit and external audit is also something that Sir Donald Brydon looked at as part of his review, encouraging the sharing of relevant knowledge at the start of setting the audit plan and assessing the environment in which an audit is to take place.

In practice, the relationship between internal and external audit seems to differ depending on the sector. During our roundtable discussions, most CAEs from the financial services and public sectors said the relationship with the external auditor was good and they had regular meetings and engagement. On the other hand, most of the CAEs from the non-financial services sector we spoke to said that their relationship with the external auditor in relation to fraud was cool. They mostly see the external auditor as non-engaging and carrying out a tick-boxing exercise. One participant of our third sector roundtable discussion mentioned that, in relation to fraud, the external auditor seemed to be more interested in compliance rather than risk management, which made the internal audit function's conversation with them challenging. Some other participants highlighted that, although they had to notify the external auditor if fraud had been detected, they didn't seem to engage a lot on fraud prevention discussions.

Overall, it seems that external auditors are interested in hearing about fraud once it has occurred but are less probing in terms of what processes and controls have been put in place to prevent fraud. In the spirit of sharing information, we would like to encourage CAEs to proactively engage with the external auditor. This includes taking a lead in explaining the steps that the organisation has taken to both prevent and detect fraud, as well as ensuring there is frequent communication and dialogue between the two functions.



Questions for internal audit

- Does the internal audit charter mention internal audit's roles and responsibilities in relation to fraud?
- Do you frequently discuss fraud with the board and senior management?
- Do you have sufficient knowledge of fraud to challenge the board and senior management on their ability to assess fraud risk?
- Are periodic fraud awareness and training programmes provided to internal auditors so that they are up to date on the latest trends?
- Do you think people in the organisation understand why the anti-fraud processes and controls exists? What can you do to help drive this curiosity?
- Do you regularly engage and meet with the external auditor? If not, what can you do to ensure there is a more open, constructive, and cooperative relationship with the external auditor with regards to fraud?
- Where do you think you can add value to your organisation in relation to fraud?

Developing a positive fraud awareness and prevention culture

Setting the right tone at the top

A root cause of almost every major fraud scandal is dysfunction in the organisation's corporate culture. This is because a poor, unhealthy corporate culture encourages various types of misconduct, including fraud. According to the ACFE Report of the Nations 2020, the wrong tone from the top was the primary risk factor in 22% of all financial statement frauds.[11] 10% of respondents to the 2021 survey also said that the wrong tone from the top was the primary internal control weakness that contributed to internal fraud.[12] On the other hand, many studies have shown that a strong, ethical culture, underpinned by the right tone from the top, can act as a bulwark against the pressure of the fraud triangle that often leads to fraud and corruption.[13] So, boards and senior management have an important role here, developing a strong tone from the top and supportive culture that will encourage employees to choose the right path.

For boards and senior management, fostering the right tone from the top includes initiating and respecting anti-fraud policies, processes, and controls (lead by example, as opposed to a 'do as I say and not as I do' attitude); staying approachable and available; discussing fraud-related issues openly and transparently with employees knowing there won't be any retaliation if they raise concerns. The consequences for employees involved in fraudulent activities should also be clearly communicated and acted on in a transparent way. Often, it seems, fraudsters are terminated and the real reasons for their termination are hushed up. Of course, there might be some confidentiality issues or other reasons not to divulge the fraud. On the other hand, making an example by announcing the termination of the fraudulent employee could work as a deterrent control. In any case, boards and senior management should encourage transparency and openness when talking about fraud as this will help increase awareness and eventually lead to better fraud prevention and detection.

A positive fraud culture should also deliver the message that internal controls to prevent and detect fraud are there to protect staff as well as the organisation. Indeed, anti-fraud processes and controls protect people from temptation, coercion, and accusation. Failure to recognise this properly and give staff awareness of the risks they are running and why controls exist can be damaging and, in some cases, dangerous. For example, one participant to the roundtable discussions recalled a situation where a manager had let staff have time away from the building. This meant that during this time he had sole access to some files, which was never allowed. As a result, this made him the number one suspect when a customer reported £100K missing from his account.

When we asked participants of the roundtable discussions whether they thought their organisations had set the right tone at the top, we heard mixed messages. Some participants said they thought their board and senior management had set a strong tone at the top with fraud embedded in policies and publicity materials; and fraud was talked about widely across the whole of the organisation. Others said they had a good fraud culture but that it wasn't led by the right tone from the top – rather by the tone from the bottom with managers talking about fraud with their teams for example.

Most participants, however, agree that fraud is a topic that overall is being talked about more openly than it used to be. One reason

11. Report of the Nations 2020, ACFE.
12. Report of the Nations 2022, ACFE.
13. Assessing Corporate Culture: A proactive approach to deter misconduct, Anti-fraud collaboration, March 2020.

mentioned by a few participants is that there has been a shift in people's sense of responsibility with regards to fraud. Andrea Deegan, Fraud Risk Services Director at RSM said: "During the pandemic, we have seen an increase in the use of and range of channels for reporting fraud as people seem to feel more responsible to report wrongdoings. Perhaps it is because people are more exposed to fraud in their day-to-day lives and therefore it is on their radar. Perhaps it is also because people have been under considerable pressure during Covid and have less sympathy for those committing fraud."

Removing the negativities attached to fraud

While boards and senior management are instrumental in developing the right tone from the top which feeds into developing a positive fraud culture, internal audit also has a role in helping remove the negativities attached to fraud. Most of the people we spoke to as part of this research agree that, historically, fraud has been – and sometimes still is – an uncomfortable topic of conversation. A topic that people usually try to avoid because it is synonymous to many negative words such as treachery, deception, trickery, or cheating. So, how to turn fraud into a safer, less negative topic?

Firstly, as one participant of our roundtable discussions said, it is important to recognise that fraud doesn't only lead to financial, material, or reputational loss. There is also a human impact in the sense that behind every fraud there is a person. So, depersonalising the processes and procedures when talking about fraud can help relieve some of the negativity attached to it. In the same vein, another participant highlighted that there was a real nervousness about sharing lessons learned about fraud, because no one wants to admit that the controls in their department failed. Internal audit can add real value here by anonymising the instances and talking about the themes and trends and ultimately carry out the lessons learnt exercise.

Another area where internal audit has a cultural role to play is by encouraging people to talk about fraud, because the more we do, the more comfortable people will get talking about it. One CAE we spoke to mentioned that since they have started to talk about fraud more, they have seen an increase in allegations – something they see as a positive. It is also important for the internal audit function not to appear as 'policing' fraud, but rather be seen as a safe place so that when they visit business departments people feel they can come to them and raise issues and concerns. This is one of the reasons why most roundtable participants said they weren't conducting surprise audits, as it would damage their relationship and trust with other functions.

Encouraging staff to speak up

There is a symbiotic relationship between whistleblowing and an organisation's culture. Indeed, effective internal whistleblowing – or speak up – arrangements are an important component of a healthy corporate culture. But these also depend on a culture that encourages concerns to be raised, without fear of the consequences. According to the ACFE 2022 Report of the Nations, 42% of frauds were detected by tip-offs, so whistleblowing is an important tool to identify fraud. The report also highlights that not all tip-offs about suspected fraud are reported through a formal reporting mechanism such as whistleblowing hotlines. 30% of whistleblowers who do not use hotline mechanisms are most likely to report their concerns to their direct supervisor, followed by 15% to executives, 12% to internal audit and, 12% to the fraud investigation team.[14]

The responsibility of establishing and operating effective internal whistleblowing procedures lies with the executive, reporting to the board. However, given internal audit's independence and objectivity, the function is often involved in whistleblowing arrangements such as in a triage role, as a channel of communication or by carrying out investigations. When the internal audit function is not involved in these roles, then their main responsibility is to review the design and effectiveness of the whistleblowing arrangements in place within the business and providing the board with assurances that the policies and procedures are effective.

Here again, internal auditors have an important role to play as a trusted advisor to the board and critical friend to the organisation by promoting whistleblowing best practice and advising on change where it is needed. This includes raising awareness of the need for well-designed and operating speak up mechanisms.

Questions for internal audit

- Has the board and senior management set a clear tone from the top in relation to fraud, including initiating and respecting anti-fraud policies, as well as processes and controls?
- Is fraud being discussed openly and transparently within the organisation?
- Have the consequences of fraud been clearly communicated to staff?
- Do senior management promote fraud awareness and training within the organisation?
- Have clear routes been established for employees to raise concerns? Are these routes working effectively?
- Are people encouraged to speak up within the organisation?
- Do you, as an internal audit function, play your part in improving the organisation's fraud culture? For example, by helping raise awareness around fraud?

14. Report of the Nations 2022, ACFE.

Conclusion

The fraud risk landscape is changing. Recent corporate collapses and the many instances of fraud reported in the media daily have heightened people's awareness of fraud. The disruption caused by the Covid-19 pandemic has increased the motivation and opportunity to commit fraud, and this trend will only continue due to the current economic, geopolitical, and social pressures we are facing. The potential changes to corporate governance rules and regulations are also the sign of a willingness to intensify scrutiny and accountability over the steps that organisations are taking to tackle fraud. As such, organisations and internal audit should take the issue seriously.

Developing a robust fraud risk assessment and setting up clear fraud policies within the business are the first imperative steps that management should take and share with the board. Fostering a positive fraud culture across the organisation is also something that boards and executive management should think about, making sure that fraud is talked about openly and transparently, that employees feel comfortable raising concerns, and have the appropriate channels to do so.

We would like to encourage internal audit teams to view fraud not as a box-ticking exercise but an opportunity to show their value to the organisations they serve. Anticipating fraud by thinking outside the box and putting yourselves in the shoes of a fraudster is one element of that. Making sure that the topic is live and discussed at board level is another, and that the board understands and considers the factors that could heighten the elements of the fraud triangle. Across the business, internal audit activities can also add real value by ensuring people understand why they are running the processes and controls.

It was somewhat disappointing to hear that very few of the organisations we spoke to as part of this research have prepared for the potential new rules and regulations coming our way. We would have at least expected all organisations that fall under the new definition of a PIE to have done some work on the proposals included in the BEIS white paper and consider how these might impact their business. Overall, we believe that organisations and internal audit should be better prepared for the increased scrutiny and accountability on fraud from government, regulators, and the public, and reflect this within their policies and audit plan.

Fraud isn't a new risk. But it is constantly evolving, and it is time for organisations and internal audit to step-up to the plate.

Case study:

Sandeep Das, Head of Internal Audit, St John Ambulance

St John Ambulance is a first aid and health response charity with 1500+ employees and 30,000+ volunteers. They work closely with the NHS, providing support to the ambulance service and on the Covid vaccination programme, as well as first aid training, supplies and youth programmes, and as such they need to comply with the NHS Counter Fraud Authority (NHSCFA) Standards. This means that counter-fraud has always been there in the background as something they have to adhere to. However, there was a need to think about fraud across the whole of the organisation, not just the services they provide to the NHS. Being a charity, they don't have the resources for establishing a dedicated fraud team, so they had to think creatively on how to better tackle fraud.

The arrival of a new Head of Internal Audit and new Head of Risk and Policy helped shape how the organisation approached fraud risk management. One outcome was the development of a Board Assurance Framework, which is an enhancement of the risk management tool they used. Fraud is still one of their top risks, but because of the new approach, they are now better at assigning responsibilities and actions, as well as tracking progress.

Another outcome was the creation of a counter-fraud working group – an initiative proposed by Sandeep Das, Head of Internal Audit, after seeing it work well in other organisations. Sandeep also chairs the group. At the moment, the group includes employees from internal audit, finance, procurement, IT and the shared services function. They meet every two months and talk about the organisation's counter-fraud strategy, current fraud risks – whether they are internal or external for example - and how to raise awareness about fraud. They also work as a group to draft and submit the organisation's annual report required by the NHS Counter Fraud Authority. According to Sandeep, the group has been very successful in getting people involved and more focused around fraud risks. From an internal audit perspective, it has also been very helpful in gathering information, especially in the context of the pandemic with people mostly working remotely.

In addition to extending the membership of the group to include other departments such as HR, another objective of the group is to work on better raising awareness around fraud in the organisation. Mainly, this is about developing a more cohesive approach. At the moment, each department do their own awareness raising – for example internal audit would publish some posts and messages every quarter on fraud risks, while the IT department was doing the same about cyber scams and phishing emails. They believe a more cohesive, joined up approach would be more beneficial and are currently thinking about questions such as how often to publish, where do they need to focus awareness on, and who's going to be responsible for the posts. Once this strategy has been implemented, the next step will be to analyse whether the awareness activity is working: Are people reading the posts, do they understand what they mean, are people taking action? They believe that awareness raising is very important as it contributes to fraud prevention and detection.

In terms of whistleblowing, this is a responsibility of the internal audit function. So, when people have concerns, they go directly to Internal Audit. Other channels exist, however, for example they have Freedom to Speak Up Guardians (FTSU). These are a mix of employees and volunteers. People with concerns may go to one of the FTSU Guardians – who are listed on the intranet – who will advise the best course of action. The FTSU Guardians help triage the concerns – if it is a whistleblower then they will direct them to Internal Audit. According to Sandeep, part of making sure people feel safe raising concerns came through refreshing the organisation's policies and getting managers to talk about these policies to their teams.

Case study:

Danielle Eadie, Head of Audit, The International Federation of Red Cross and Red Crescent Societies (IFRC)

The International Federation of Red Cross and Red Crescent Societies (IFRC) is an international organisation, employing over 2,000 people across the globe. It has five Regional Offices, as well as an Office in Geneva, which support country delegations across the world. IFRC's core business is responding to short and protracted humanitarian crises, including extreme weather events and displacement and migration. They often operate in fragile environments, with low levels of human development and high levels of corruption. From an internal audit perspective, oversight can be a challenge, as the organisation operates globally, in countries that are not always easily accessible. The level of accountability for fraud, integrity issues, and financial loss is very high, with most of the organisation's money comes from its members (Red Cross and Red Crescent National Societies) and donors. This also means that fraud represents a huge reputational risk.

According to Danielle, when it comes to fraud, the link between risk and objectives is very important. Fraud is one of IFRC's top 10 risks and, as such, is scrutinised by the Global Leadership Team and the Audit and Risk Commission regularly. At the same time, because of the work IFRC do, they have to respond to situations very quickly because lives are at stake. So, looking at their main objective, which is to get to places and save lives, they need to think of fraud within that framework and find the right balance of controls. From an internal audit perspective, because fraud is one of the organisation's top 10 risk and that a high level of accountability to communities and donors is required, every audit will have some element of fraud risk testing in it.

The internal audit team sits under the Director of the Office of Internal Audit and Investigations and there is an internal audit team and an investigations team reporting to the same Director. The two teams have separate workstreams and two separate charters, that keep the roles of the team very clear and separate, and also help safeguard the independence of both teams. Despite being separate, both teams work very closely on day-to-day work, talk about themes and trends and share information at their weekly management and team meetings.

One practical example of this information sharing is the internal audit team's annual audit planning, where they take into consideration the analysis of the investigations team, looking at where they are getting fraud cases, and the common types of fraud. Before starting any individual audit, the internal audit team get a briefing from the relevant Regional Investigator (or Head of Investigations) on the country context, key corruption indicators, and what types of fraud cases and near-misses there have been.

While it is not internal audit's primary mandate to identify fraud and corruption, and it is important to make that clear, according to Danielle, there has been occasions where the internal audit team has identified fraud while doing audit work. When that happens, or when they have identified control failures that could led to fraud, they feed that to the investigations team or raise a case on the internal whistleblowing and case management system. This usually follows a conversation where the investigations take make a judgement on whether a case should be opened and both teams consider whether additional audit testing or analysis would be more beneficial, if they don't have enough evidence to start an investigation.

The teams occasionally do joint missions, where they will deliver joint integrity training and carry out complementary audit and proactive fraud work. An auditor may also work on an investigation, or an investigator may join an audit but when this happens, the individuals 'loses' their respective auditor/investigator hat and is acting in a different role. This allows for staff and personal development and appropriate training and qualifications are ensured.

According to Danielle, this collaborative model is hugely beneficial as it enhances the quality of data that they can feed to management, provides a more nuanced understanding of risk, and provides better quality assurance overall.

The teams occasionally do joint work, where an auditor may work on an investigation, or an investigator may join an audit. When this happens, the individuals lose their respective auditor/investigator hat so that independence is conserved. These exercises are mainly done in a personal development capacity and appropriate training and qualifications are ensured.

Appendix and useful resources

1. Occupational Fraud 2022: A report to the nations, Association of Certified Fraud Examiners
2. Fraud crime trends: 2020-21 Annual Assessment, Action Fraud
3. Fraud and internal audit: Assurance over fraud controls fundamental to success, The Institute of Internal Auditors, April 2019
4. Position Paper: Internal audit and corrupt practices, Chartered Institute of Internal Auditors UK & Ireland
5. Technical Guidance: Fraud, Chartered Institute of Internal Auditors UK & Ireland (membership subscription required)
6. Technical Guidance: Auditing counter-fraud strategy, Chartered Institute of Internal Auditors UK & Ireland (membership subscription required)
7. Technical Guidance: Fraud risk assessment, Chartered Institute of Internal Auditors UK & Ireland (membership subscription required)
8. Internal audit's role in fraud risk management, Kroll & The Institute of Internal Auditors, July 2020
9. Global Fraud and Risk Report 2021/22, Kroll &The Institute of Internal Auditors
10. The nature of fraud is changing, Deloitte
11. Protecting the perimeter: the rise of external fraud, PwC's Global Economic Crime and Fraud Survey 2022
12. What is a fraud risk assessment? And why do I need one?, Audit Board, April 2021

About the Chartered Institute of Internal Auditors

The Chartered Institute of Internal Auditors is the only professional body dedicated exclusively to training, supporting and representing internal auditors in the UK and Ireland.

We have 10,000 members in all sectors of the economy.

First established in 1948, we obtained our Royal Charter in 2010. Over 2,000 members are Chartered Internal Auditors and have earned the designation CMIIA. About 1,000 of our members hold the position of head of internal audit and the majority of FTSE 100 companies are represented among our membership.

Members are part of a global network of 200,000 members in 170 countries, all working to the same International Standards and Code of Ethics.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management.

More than 30% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2 and Gartner Peer Insights, and was recently ranked for the third year in a row as one of the fastest-growing technology companies in North America by Deloitte.

To learn more, please visit: www.auditboard.com

Stay connected

Chartered Institute of Internal Auditors

Wimbledon Business Centre
The Old Town Hall
4 Queen's Road
Wimbledon
SW19 8YB

tel **020 7498 0101**
email **info@iia.org.uk**

Chartered Institute of Internal Auditors

AUDITBOARD