A director's guide to conducting internal investigations

Special Report from *Board Agenda* in association with Forvis Mazars

BOARD AGENDA

GOVERNANCE | STRATEGY | RISK | ETHICS

In association with

forvis mazars

Contents

Overview 3

Why investigate? 4

Preparing for an internal investigation 6

Who investigates? 8

Governance & decision-making 10

Co-operating with authorities 11

Obtaining & preserving evidence 13

Witness interviews 15

Disclosure, press & communications 17

Conclusion 18

Overview

TODAY'S COMPANIES FACE unprecedented scrutiny—from regulators, prosecuting authorities, shareholders, investors, the media, employees and the general public. The financial crisis of 2008 kick-started a global revolution in compliance, regulation and corporate governance. In the UK, there has been an aggressive drive towards criminalising corporate misconduct.

As a consequence, there has been a marked increase in companies conducting their own internal investigations, whether in response to a regulatory probe or because the business itself discovers misconduct from within. Either way, an internal investigation must be handled meticulously to avoid legal exposure, regulatory or criminal prosecution and reputational damage, and enable the board to comply with its regulatory and legal obligations.

Yet while these obligations have multiplied, there has been little guidance on how to conduct an internal investigation. A lack of established practice places businesses at an immediate disadvantage in dealing with enforcement bodies.

This guide seeks to empower company directors in dealings with the authorities should an internal investigation become necessary, with an analysis of the key stages of an investigation, common pitfalls to avoid and examples of best practice. Importantly, it outlines how to get the process right from the outset—because a mishandled investigation is most likely to go wrong in the early stages.

The main focus of this guide covers UK (England and Wales) legislation and regulation, but corporate law enforcement is increasingly co-ordinated globally. References are made to other jurisdictions where relevant.

Why investigate?

"There is no doubt that the regulatory environment has grown stronger, which has fuelled a rise in investigations. Corporates are now expected to comply with a host of anti-bribery and anti-corruption laws that can lead to severe sanctions when things go wrong. The regulatory environment for corporates is starting to go the same way as the banks."

Nigel Layton, Head of Investigations, Forvis Mazars

Businesses may need to conduct an internal investigation for a variety of reasons. Typically, it will be the result of criminal behaviour or a breach of regulatory rules.

Examples of corporate misconduct include:

- tax evasion
- bribery and corruption
- antitrust and competition law breaches
- fraud and theft
- falsifying accounts
- money laundering
- insider or irregular trading
- modern slavery offences and child labour
- IT security breaches and data protection
- breaches of business and professional codes of conduct
- inappropriate behaviour, such as complaints following sexual harassment, bullying and aggressive behaviour.

Whether misconduct is criminal or regulatory in nature, the need for an internal investigation will be presented to the board following a triggering event. Common triggering events include:

- notification of wrongdoing by a regulator or criminal investigating body (such as the Serious Fraud Office or HMRC)
- misconduct by an individual that comes to a manager's attention
- irregularities discovered during routine accounting or compliance audits
- wrongdoing by a competitor or peer company, precipitating the need to ensure one's own house is in order
- complaint from a shareholder, other stakeholder or competitor
- technology and cybercrime exposing issues of which a company is previously unaware
- potential or impending civil litigation
- whistleblowing – individuals are protected under the **Public Interest Disclosure Act (PIDA) 1998**. The UK Government is undertaking a review of the whistleblowing framework which will close in autumn 2023.

In England and Wales, there is no statutory or regulatory obligation to conduct an internal investigation but it is often in an organisation's best interest when criminal or regulatory misconduct is suspected.

Preparing for an internal investigation

Every crisis is different and there is no single template for internal investigations. However, there are essential considerations at the outset to ensure an investigation is handled successfully. While it is important to act as soon as a problem comes to light, the investigation process must be planned thoroughly.

It is important that the implications of conducting an investigation are fully understood. These can include cost, reputational damage or the loss of legal professional privilege. The following is a list of first responses should a triggering event occur.

Immediate priorities

- Establish the nature of the issue, how it came to light and the possible implications. Is a formal investigation required?
- If an investigation is necessary, establish a clear oversight and governance strategy. Assemble an investigations team and decide reporting lines and board involvement.
- In cases of criminal misconduct, efforts should be made to prevent further offending to avoid allegations that the company is complicit. An exception may arise where conduct must be allowed to continue in order to gather evidence or identify the wrongdoer.
- Preservation of evidence: laptops, mobile phones or hard documentation may need to be seized. Failure to preserve evidence can lead to regulatory, civil or criminal penalties for both the company and its directors.
- Securing assets: if a business is the victim of wrongdoing, such as theft or fraud, it may need to immediately locate assets and seek a freezing injunction before the wrongdoer becomes aware that their conduct has been discovered.
- Reporting: are any immediate notifications required due to legal self-reporting obligations, i.e. to the FCA, or, in the case of listed companies, to the market? In the case of the latter, any disclosures to comply with reporting requirements must be balanced with the danger of reporting too hastily and misleading the market.

"It is crucial to move quickly once fraud or other misconduct is suspected. Organisations should have an investigations expert on speed dial who can advise on immediate priorities and ensure appropriate experts are involved at the onset, be it legal, IT or employment law professionals."

Darya Oglezneva, Director, Forensic and Investigation Services, Forvis Mazars

Setting the scope

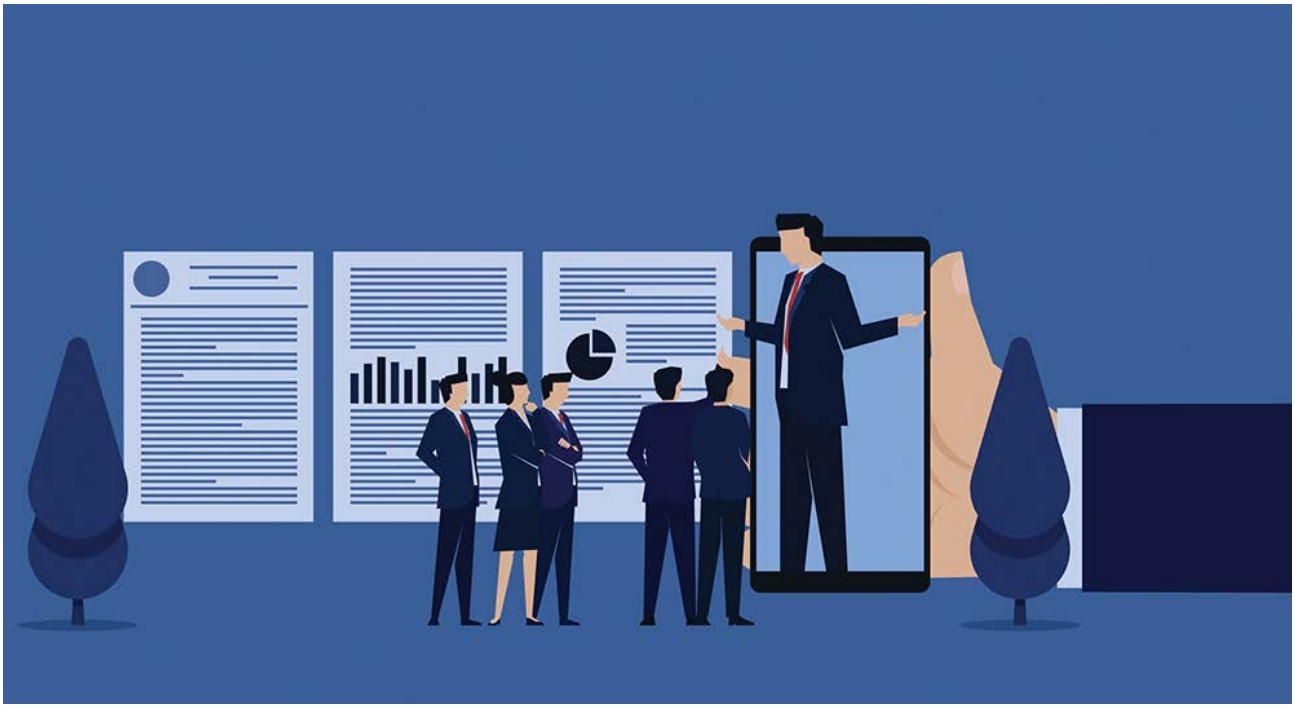
Investigations are not fishing expeditions: they must focus specifically on the event or issue that has come to light. The scope should therefore be tailored to the specific wrongdoing, limited to a date range and the jurisdictions involved, but retain sufficient flexibility to investigate wider issues where they remain within the original goal of the investigation. Where a regulator is already on the scene, it may be necessary to agree the scope of the investigation with them, but care should be taken to negotiate to limit the company's exposure to a wide-ranging investigation. The objective of the investigation is to establish the facts and not to draw conclusions on legal or regulatory liability.

The investigation plan

A detailed plan should be drafted based on the agreed scope of the investigation and set out the terms of reference. These should include:

- the investigating team, their specific duties and to whom they will report; whether to instruct external lawyers, investigators or other experts
- what each phase of the investigation will cover
- timescale
- the identity of relevant individuals to interview and any employment issues such as disciplinary action or whistleblower protection
- a suggested order of interviews
- how evidence will be preserved, collected and reviewed
- whether the regulator or prosecuting authority should be notified
- any international implications, such as foreign jurisdiction obligations/liability
- how and when to provide updates of progress to the board/committee
- how to revise and implement changes to the plan if needed
- measures needed to ensure data protection, confidentiality and preserve legal professional privilege
- how the final report will be presented, i.e. written or oral
- how to manage communications and PR issues

Who investigates?



The investigating team will commonly comprise a mix of professionals, led by a senior project manager. Factors to consider include the nature and severity of the issue being investigated; the appropriate level of seniority and skills needed to conduct the investigation; issues of independence and conflicts of interest; preservation of legal privilege; and whether external lawyers or other experts, such as forensic accountants, are required.

The team may be drawn from management, the internal audit committee, in-house legal/compliance department, HR and IT personnel, or comprise of external advisers, either for a particular issue or to manage the entire investigation. While it is tempting, for reasons of cost, time and confidentiality to keep the entire investigation in-house, a company should be honest with itself as to whether it has sufficient expertise and resources. There are other advantages to using outside experts.

Using external lawyers and/or forensic investigators

External advisers bring experience, expertise and independence, adding credibility and weight to the investigation and its findings. They also better understand the regulators/prosecutors and the system, and are more likely to have the staff and connections to resource large investigations. External advisers can include lawyers, auditors, forensic accountants, IT/data analysts and private investigators. In the case of external lawyers, they are best placed to preserve crucial legal privilege during the investigation.

"Generally, using outsiders is preferable: they bring independence, objectivity and experience to the investigation and signal to the outside that the investigation has been done properly. If handled purely in-house, issues that arise can easily be swept under the carpet, or key witnesses or documents can be overlooked or may not be considered important at the time."

Nigel Layton, Head of Investigations, Forvis Mazars

Legal privilege

The concept of legal privilege renders all communications between a lawyer and his client *for the purposes of obtaining legal advice* confidential. It does not extend to commercial advice or fact finding. This can be highly significant during internal investigations where outcomes or evidence may later be sought by a regulator, prosecutor or in any subsequent litigation. While privilege applies equally to advice provided by in-house lawyers (with the exception of investigations relating to EU antitrust and competition law), using external lawyers is the most reliable way of ensuring legal privilege and therefore keeping as much of the investigation as possible non-disclosable.

To claim legal privilege during an internal investigation, it must be clear who the "client" is—i.e. the board overseeing the investigation, or the project leader/core team of the investigation. Only communications between the lawyer and client are privileged and do not extend to witnesses or independent third parties, such as forensic accountants, unless it is in anticipation of litigation (known as litigation privilege).

It should be noted that privilege rules differ between jurisdictions and is not recognised in civil law countries, including many EU member states and China, for example.

Investigating team checklist

- A suitably senior project manager.
- Legal advisers, either internal or external (or both).
- IT specialist, to advise on company systems, policies and procedures, and how data can be collected and preserved.
- HR executive, to advise on employment issues relevant to the investigation.
- Internal audit personnel, to advise on the collation and analysis of financial records and its accounting impact.
- Data protection officer, to ensure data protection law issues are considered.
- Specialist expertise, e.g. forensic accountants or investigators.
- Legal privilege protocol.

Governance & decision-making

The role of the board in internal investigations will depend upon the size and seriousness of the misconduct. Smaller, less significant investigations can be delegated to the company's in-house legal, audit or compliance teams, who will report findings to the board. Investigations into serious allegations—those involving significant potential reputational damage, financial loss or legal liability—should be overseen by the board directly, or by a special committee.

Poor governance of the internal investigation is a common pitfall. Board-level involvement in the investigation has the added benefit of demonstrating internally and externally that the business is taking the misconduct seriously.

"A lot of the time, the success of an investigation is down to the resources available to the company. The company should maximise the best possible blend of internal resources partnered with external experts."
Katie Miles, Associate Director, Forensic and Investigation Services, Forvis Mazars

A special committee of the board, comprising independent directors, will be required where a member of the board is potentially implicated in, or conflicted by, the investigation.

The board or committee will be responsible for giving instructions and liaising with the investigations team, and acting upon the findings of the investigation.

To achieve successful oversight of an investigation, directors should ensure:

- investigation and crisis management protocols are in place before an event occurs
- there is regular compliance training for board members
- any director who is part of the investigating team must be independent of the issue or personnel under investigation; ideally, they should be responsible for a separate part of the business
- clear channels of communication are established between the investigating team and the board/special committee
- the board is regularly appraised of material developments in the investigation
- a clear record of deliberations is maintained in order to discharge any directors' fiduciary duties (subject to legal privilege implications, see below)
- legal advice is sought, either internally or externally, on managing the investigation, particularly where a whistleblower, regulator or multi-jurisdictional issues are involved
- when the investigation is concluded, the key findings are discussed by the board together with either in-house or external lawyers to determine the next steps
- any legal obligations to report findings of the investigation to the regulator, prosecutor or general public are met
- the pros and cons of voluntary disclosure of findings are assessed, taking into consideration reputational harm, the impact on existing company transactions, possible litigation or share price. When deciding whether to self-report findings, directors should be aware of their obligations under the **Companies Act 2006** to consider the best interests of the company as a whole when making decisions.

Co-operating with authorities

Not all investigations attract the attention of the regulator or prosecuting authority, and deciding whether to self-report wrongdoing is a major decision. In certain circumstances, there is a legal obligation to report.

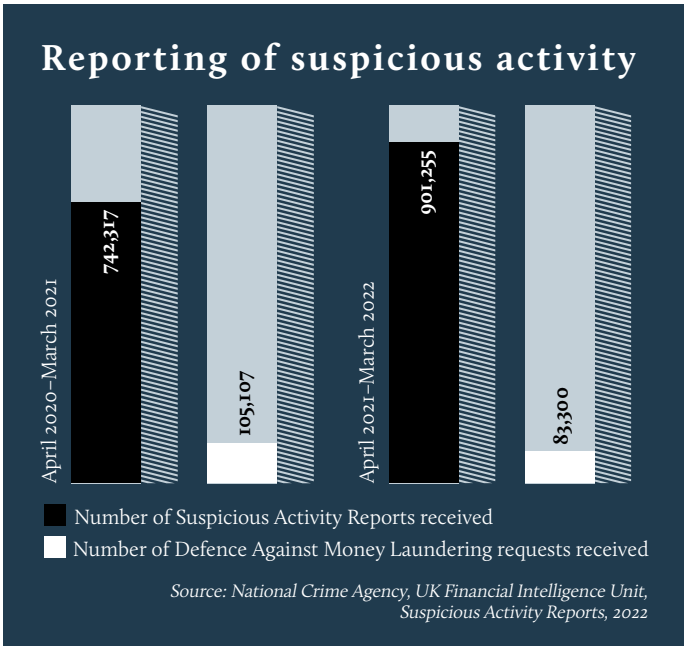
- Financial services companies must disclose to the Financial Conduct Authority (FCA)/Prudential Regulatory Authority (PRA) "anything relating to the firm which the FCA/PRA would reasonably expect notice [thereof]".
- Obligations in relation to financial crime, such as money laundering and terrorist financing, require the filing of a suspicious activity report (SRA) to the National Crime Agency (NCA).
- Breaches of the EU's General Data Protection Regulation (GDPR) may have to be reported to the Information Commissioner's Office within 72 hours.

In other circumstances, the decision to self-report is more ambiguous and requires caution. Certainly, if an outside agency is likely to become involved, voluntary disclosure demonstrates transparency and co-operation; may dissuade the authority from launching its own investigation or raid; and is increasingly being taken into account when considering civil or criminal penalties.

Guidelines published by the Serious Fraud Office (SFO) state that organisations wishing to have criminal matters dealt with via a Deferred Prosecution Agreement (DPA) must co-operate fully with their investigation, including providing assistance that goes "above and beyond what is required by law".[1] Early self-reporting is one way of satisfying this criterion.

DPAs

A DPA is an agreement between a prosecuting authority and a company to defer and ultimately avoid prosecution for criminal misconduct if certain conditions are met. DPAs have existed in the US for many years and were introduced into the UK in 2014. They are a growing trend globally. Under the UK's DPA Code of Practice, "considerable weight" will be given to a "genuinely proactive approach" to a company-led investigation when deciding whether to grant a DPA.[2]



International implications

Another trend is the joined-up approach of global regulators and prosecuting authorities, which multinational companies must carefully consider. For example, there is increasing collaboration between the FCA and SFO with their US counterparts, the Securities and Exchange Commission (SEC) and Department of Justice (DoJ). Therefore, when deciding to self-report to one jurisdiction, care must be taken to ensure this does not jeopardise or trigger an investigation in another jurisdiction, and that information shared is consistent across regulators in different countries.

Evidence

Regulators have extensive powers to gather evidence and compel companies and individuals to answer questions. For this reason, the safeguarding of legal privilege during an investigation is crucial to retain as much control as possible. A company may decide to waive privilege for the purposes of co-operating with the investigating authority, but once waived, privilege is lost and cannot be regained in the future.

[1] *Corporate Co-operation Guidance* SFO, 6 August 2019

[2] *Deferred Prosecution Agreements Code of Practice* Serious Fraud Office/Crown Prosecution Service

Obtaining & preserving evidence

The retrieval and review of documentation is a critical aspect of the investigation. The growth of electronic data has made it possible for technology assisted review (TAR) and artificial intelligence (AI) systems to assist with the identification of relevant documents.

An in-house senior IT manager should be included on the investigating team. They have the most comprehensive understanding of the company's IT systems and internal document handling policies. For complex investigations, forensic investigators and/or data handlers should be considered to work alongside the in-house IT team.

The investigation plan should include a structured approach to document collection, review and preservation. Safeguarding potential evidence is key to the integrity of the investigation.

Action plan

- Identify and locate all relevant documentation to ensure that no evidence is missed or destroyed. Document the decision-making process in case justification is required later.
- Collate documents in a reasonable and proportionate way, unless there is risk of destruction or concealment.
- Review company policy on document retention, destruction and back-ups to ensure evidence is not altered or destroyed.
- Seize or copy all relevant hard copy documentation.
- Seize electronic devices, including PCs, laptops, tablets and mobile phones which contain relevant material, including imaging or cloning hard drives.
- Secure or clone the organisation's central hard drives.
- Secure any relevant centrally held documentation, such as risk reports, compliance material, personnel records, CCTV and any other security data.
- Ensure all seized documents/data are quarantined and held securely, while at the same time trying to minimise disruption to the business. Access to the material should be strictly limited and monitored via a log.

A detailed written record of the above steps should be kept.

GDPR and Data Protection Act 2018

All investigations involve processing personal data. Under GDPR, employers can access personal data only if it gives sufficient notice to the employee, although consent is not generally required. It is advisable to seek legal advice if access to data is required without notification, i.e. because to do so would prejudice the investigation.

"With increasingly large volumes of evidence being in electronic form, investigators are faced with a challenge of managing evidence review efficiently. Thankfully, we now have technologies and tools to allow narrowing down the relevant evidence pool and finding that 'needle in the haystack' promptly (if there is one, of course)."

Darya Oglezneva, Director, Forensic and Investigation Services, Forvis Mazars

While GDPR covers all EU jurisdictions, multinationals need to be wary of country laws that may have a higher standard of data protection above and beyond GDPR. For example, France and Germany have stringent rules in relation to informed consent from individuals. GDPR can also apply if EU-related data is stored outside the EU, e.g. on US email servers.

Legal privilege

Great care must be taken in document handling to protect legal privilege. Privilege in a document is lost if the document ceases to be confidential. Therefore, it is imperative that privileged documents are not widely circulated, even within the organisation, and where they must be shared, the recipient should agree to treat them as confidential. Standard wording, such as marking documents and covering emails as "privileged and confidential" can assist in reinforcing confidentiality. In the case of criminal investigations, the use of legal privilege is increasingly being challenged by prosecuting bodies such as the SFO.

Employees and third parties

An organisation can only access documentation that belongs to it, so it has no power to obtain material belonging to employees or third parties. In respect of searching personal space, i.e. an employee's desk or email account, the Staff Handbook should be consulted for any specific provisions, although searches are usually permitted in cases of regulatory or criminal breaches. Intercepting communications on a public network (e.g. Gmail) is a criminal offence, as is intercepting communications on a private network without proper corporate authority. Accessing an employee's private mobile phone without their consent is also a criminal offence.

"The minute you access electronic data, you may be effectively changing that data without even being aware. This lack of awareness and understanding of computer and digital forensics is a big issue that can cause investigations to go wrong."

Katie Miles, Associate Director, Forensic and Investigation Services, Forvis Mazars

Witness interviews

Interviewing employees is a key component of any investigation, and care must be taken to adhere to employment law obligations.

Identifying who to interview and in what order should arise from preliminary enquiries and document research, and will almost certainly include all those involved in the basic facts. As with document searches, the decision-making process of who and when to interview should be clearly recorded for the purposes of future justification.

Current employees are likely to be compelled to co-operate with an investigation under the terms of their employment contract. Individuals regulated by the FCA are required to act with integrity at all times, including providing their employer with a full and truthful account during interview. Failure to do so can result in withdrawal of their fitness to continue in a regulatory role.

Senior management may well be entitled to legal representation if they are required to be interviewed under the terms of their employment contract, possibly financed by Directors and Officer's insurance. FCA-regulated firms should interview senior managers with responsibility for the relevant business function, even if not directly involved, since the FCA prioritises senior manager conduct.

Former employees and third parties are more difficult to compel to be interviewed, except where former employees may have a contractual obligation to assist even after leaving the company. Seeking to interview outsiders also risks revealing the existence of the investigation

Whistleblowers must not be discriminated against as a result of their disclosure. The investigating team/interviewer must make it clear at the outset of the interview that they are aware of the whistleblower's status and the protection this affords them. The interviewer should also remind the whistleblower that, while their evidence may form part of a report to authorities, the report will seek to maintain their anonymity.

Investigating authorities are not usually consulted prior to staff interviews, with the exception of the SFO co-operation guidelines, which specifically require organisations to consult them before interviewing witnesses or suspects to avoid prejudicing any subsequent SFO investigation.[1]

Interview checklist

- Ensure the witness understands the basis for the interview: its purpose and the potential use of the information provided, as this can impact upon admissibility in any subsequent proceedings.
- Aim for consistency—all interviews should be conducted by the same team.
- Consider interviewing from the bottom up: the most junior to the most senior employees, so the picture is clear when the senior employee(s) is interviewed.
- Keep a written record of the key facts provided by the interview as opposed to a verbatim transcript.
- It is good practice to give an 'Upjohn warning' to remind the witness that any lawyers present represent the company and not the witness, that privilege* in the interview belongs to the company and not to the witness and that the company may later decide to waive privilege and disclose the interview to investigating authorities.
- Remind the witness of the confidential nature of the interview.
- Discourage witnesses from keeping their own notes of the interview as these will not be within the control of the company.
- Continue to review the list of interviewees, which will inevitably grow as the investigation develops.

** Witness interviews do not attract legal privilege because they are fact-finding exercises. The exception is when they are conducted with a view to litigation or the likelihood of litigation.*

"Investigation meetings are often difficult and emotional, especially for someone who raised a complaint or is under investigation. A courteous investigator following a structured process, by pre-planning their initial questions, will reduce unnecessary stress and help keep the interview on the right track."

ACAS[2]

[1] *Corporate Co-operation Guidance* SFO, 6 August 2019

[2] *Conducting Workplace Investigations* ACAS, June 2019

Disclosure, press & communications

The investigation report

At the conclusion of the investigation, a key question is whether to produce a written report or provide an oral account to the board. A written account may contain highly sensitive information, possibly exposing poor conduct by employees or inadequacies of corporate governance; it would be valuable to any third party seeking to bring a claim against the company; and be of considerable interest to the press, shareholders and the public. On the other hand, putting conclusions in writing is the best way to demonstrate that a thorough, independent and focused investigation has taken place. Such a report will also be viewed more favourably by a regulator when deciding how co-operative an organisation has been.

One solution is to have the report prepared by lawyers in order to obtain legal privilege over the report, and then ensure that circulation is restricted to prevent loss of privilege. The report could be provided just to the investigating team (if they are the "client" for legal privilege purposes) who would report orally to the board.

Reporting obligations

Depending upon the regulator and the findings of the investigation, legal advice should be sought on obligations to report. Listed companies have duties imposed by the FCA and Listing Rules to report issues to the market, but extreme care should be taken in the timing of such a report.

Again, depending on the nature of the investigation, it may be appropriate to report conduct to an enforcement agency such as the NCA, SFO, FCA or HMRC. There is no obligation to report criminal conduct to the police, although a company may wish to send out the right message to other employees; it may also be a requirement of an insurance policy. For more on reporting obligations, see the **'Co-operating with authorities'** section of this guide.

UK tax gap

The difference between tax that should be paid and what is actually paid

5.1%

2021-22

Tackling avoidance and evasion

£731.1bn

total tax revenues

£30.8bn

additional tax generated through tackling avoidance evasion and other non-compliance

Source: HM Revenue & Customs 2021-22 Annual Report and Accounts

Internal communications

A communications protocol should be established at the outset of the investigation and followed throughout the investigating process. The existence of any investigation should be kept confidential as far as possible, and should generally be disclosed only on a "need to know" basis. The investigation team should have clear reporting lines to the board.

External communications

Where an investigation risks becoming public knowledge, companies should consider engaging PR consultants to handle communications. A well-prepared statement confirming that an investigation is taking place is less damaging than a reactive response. Senior officers, including the board, should be advised how to comment on enquiries.

Conclusion

Growing regulatory powers, increased compliance awareness and the expansion of companies into developing markets are all fuelling a rise in corporate internal investigations. So, too, is the hike in whistleblowing, as employees grow acutely aware of today's high standards of accountability and responsibility, and are empowered by legal protections. While there is never an obligation to conduct an internal investigation, it is often in the company's best interest when business-critical misconduct is discovered.

However, an investigation can be a reputational and financial minefield if handled inadequately. Planning is therefore vital. Don't wait for a triggering event to occur—implement a protocol now for handling investigations should the need ever arise, and consider ongoing training for the board and senior management. For complex, high-stakes or cross-border investigations, hiring external experts will greatly aid the navigation of intricate legal and regulatory obligations and ensure the best possible outcome.

Poor oversight is the single most common pitfall. Board involvement in more serious investigations keeps a rein on the process and sends a clear message that a company is taking the misconduct seriously. It also adds credibility to the investigation and its findings. A clear record of the decision-making process, from the very outset, is paramount to ensure the integrity of the investigation.

By addressing problems in a swift, well-planned and robust manner, the board can protect a company's reputation, financial and legal position and even dissuade a regulator or prosecutor from taking further action.

A director's guide to conducting internal investigations

Contacts

Nigel Layton, Head of Investigations
Email: nigel.layton@mazars.co.uk
Tel: +44 (0)7785 244331

Darya Oglezneva, Director, Forensic and Investigation Services
Email: darya.oglezneva@mazars.co.uk
Tel: +44 (0)7583 041140

Katie Miles, Associate Director, Forensic and Investigation Services
Email: katie.miles@mazars.co.uk
Tel: +44 (0)7881 283928

www.forvismazars.co.uk

Trevor Pryer, Executive Director
Email: trevorpryer@boardagenda.com
Tel: London +44 203 151 2653

www.boardagenda.com

November 2024