INVESTIGATION · BUSINESS AND CORPORATE INVESTIGATION

Corporate Investigations: Purpose and Scope

Companies investigate fraud, misconduct, regulatory breaches and complaints every day. This article explains why corporate investigations are carried out, what they cover, who should run them, how legal and regulatory frameworks shape them, and what distinguishes a credible investigation from a defensive exercise.

ModQu research article · 3,110 words · 25 references (APA 7th edition)

Every organisation of any size will at some point need to find out what happened inside it. An employee reports that a manager is harassing staff. An auditor finds payments that cannot be explained. A regulator asks questions about sales practices. A whistleblower alleges that a contract was won with a bribe. In each case the organisation must decide whether to investigate, who should do it, how far the inquiry should go and what to do with the findings. These are corporate investigations: inquiries carried out by or for an organisation into conduct that affects it.

Corporate investigations differ from police investigations in important ways. They have no powers of arrest or compulsion, they serve the organisation rather than the state, and their outcomes are usually decisions about employment, contracts, controls and disclosure rather than prosecution. Yet they increasingly operate in the shadow of criminal and regulatory enforcement, and their quality can determine whether a company is seen as a responsible actor or as a participant in wrongdoing. This article sets out the purposes of corporate investigations, the kinds of matters they cover, the governance and legal frameworks that shape them, and the features that make them credible.

Why companies investigate

To establish the facts

The basic purpose of any investigation is to find out what happened. Managers and boards cannot make sound decisions about discipline, controls, disclosure or remediation without knowing the facts. A company that acts on rumour, dismissing an employee on the strength of an anonymous complaint or ignoring a credible allegation because it is inconvenient, exposes itself to legal claims and to the continuation of whatever went wrong.

To meet legal and regulatory duties

Many legal frameworks expect, and some require, companies to investigate. In the United States, the Sarbanes-Oxley Act of 2002 requires audit committees of listed companies to establish procedures for receiving and handling complaints about accounting and auditing matters, including confidential and anonymous submissions. The European Union's whistleblower protection directive requires organisations with 50 or more workers to establish internal reporting

channels, acknowledge reports within seven days and provide feedback within three months, which in practice means investigating them (Directive (EU) 2019/1937, 2019). Employment law in many jurisdictions requires a fair investigation before dismissal for misconduct (Acas, 2019).

To manage legal and regulatory exposure

When a company may have broken the law, how it responds affects how prosecutors and regulators treat it. The United States Department of Justice asks prosecutors evaluating a corporate compliance programme whether the company investigated misconduct properly, identified root causes and took remedial action (U.S. Department of Justice, 2023). The United Kingdom's Serious Fraud Office has published guidance describing the cooperation it expects from companies, including preserving evidence, identifying witnesses and avoiding steps that could prejudice its own investigation (Serious Fraud Office, 2019). The UK Bribery Act 2010 created a corporate offence of failing to prevent bribery, with a defence of having adequate procedures, which encourages companies to detect and investigate potential bribery. Companies that self-report and cooperate may receive deferred prosecution agreements or reduced penalties, a development Garrett (2014) traces in detail and critics argue has weakened deterrence (Coffee, 2020).

To protect the organisation and its people

Investigations protect employees who report problems, those who are wrongly accused and those harmed by misconduct. They also protect the organisation's assets and reputation. The Association of Certified Fraud Examiners (2024) estimates that organisations lose around 5% of revenue to occupational fraud each year; its global study of 1,921 cases found that 43% were detected through tips, more than by any other method. An organisation that investigates tips seriously is far more likely to find fraud early.

To learn and improve

Finally, investigations reveal weaknesses in controls, incentives and culture. A finding that one employee stole money is useful; a finding that the theft was possible because one person controlled supplier set-up and payments, and that nobody reviewed their work, is more useful, because it can prevent the next theft. Frameworks for internal control and internal audit treat investigation findings as inputs to the improvement of controls (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013; Institute of Internal Auditors, 2024).

What corporate investigations cover

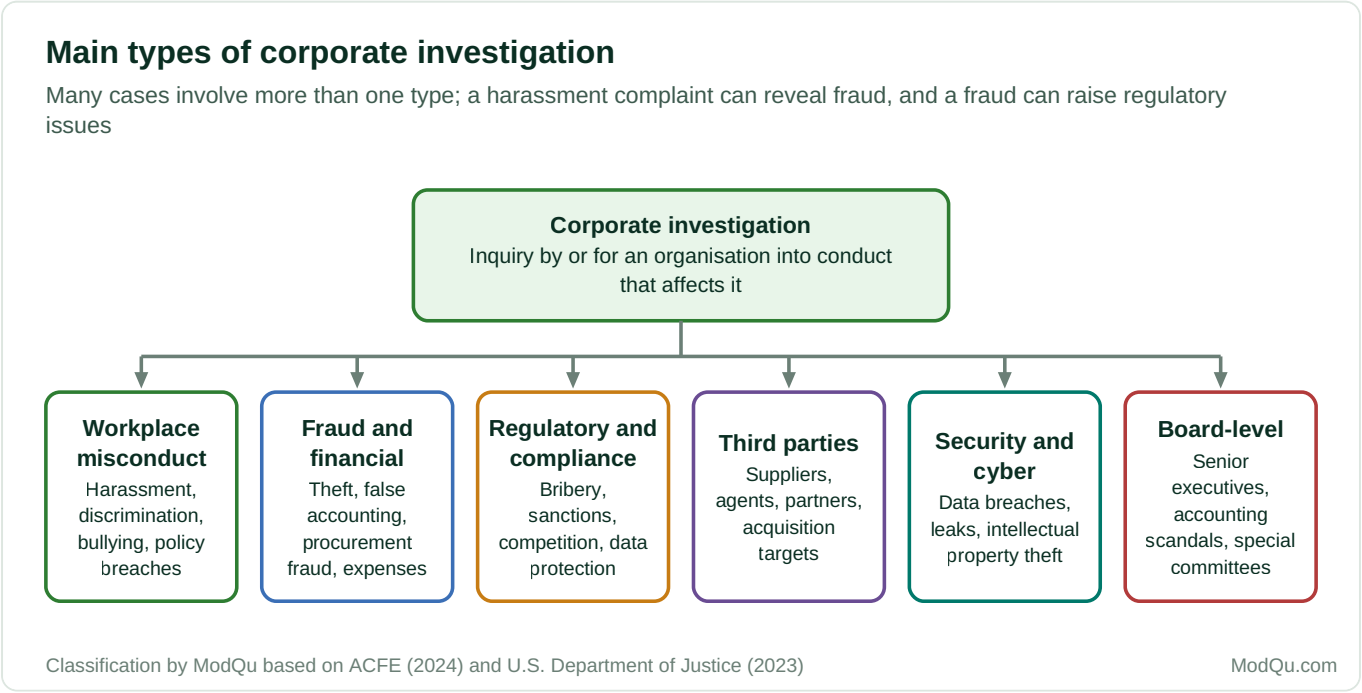


Figure 1. The main kinds of matters that corporate investigations address. Diagram by ModQu.

Workplace misconduct investigations deal with complaints of harassment, discrimination, bullying, health and safety breaches and other violations of policy. They are the most common type in most organisations, and they often turn on witness accounts rather than documents.

Fraud and financial investigations examine theft, false accounting, procurement fraud, expense abuse and similar matters. They rely heavily on records, data analysis and forensic accounting.

Regulatory and compliance investigations address possible breaches of law, such as bribery, sanctions violations, anticompetitive conduct and data protection failures. They are often conducted under legal privilege and with an eye to possible disclosure to authorities.

Third-party investigations examine suppliers, agents, distributors and acquisition targets, either in response to concerns or as part of due diligence.

Security and cyber investigations deal with data breaches, leaks of confidential information and theft of intellectual property.

Board-level investigations are commissioned when the conduct of senior executives or the integrity of financial reporting is in question. They are usually overseen by a committee of independent directors and carried out by external lawyers and accountants. The special committee investigation into Enron's partnerships in 2002 (Powers et al., 2002) and the independent directors' report on sales practices at Wells Fargo (Independent Directors of the Board of Wells Fargo & Company, 2017) are well-known examples of investigations whose reports became public documents.

Who investigates

Organisations can use internal teams, external advisers or a combination. The choice depends on the seriousness of the matter, who may be implicated, the expertise required and whether legal privilege is needed.

- **Human resources** typically handles routine workplace complaints, often with trained investigators.
- **Internal audit and compliance** functions handle fraud, control failures and policy breaches. Internal audit standards require auditors to be objective and to have the competence to carry out the work (Institute of Internal Auditors, 2024).
- **Legal departments** direct investigations where legal liability or regulatory exposure is likely, partly to protect the work under legal privilege. In the United States, *Upjohn Co. v. United States* (1981) confirmed that communications between company lawyers and employees made to provide legal advice to the company can be privileged, which is why lawyers conducting interviews give employees an "Upjohn warning" that they represent the company, not the individual.
- **External investigators**, including law firms, forensic accountants and specialist firms, are used when independence, specialist skills or capacity are needed, or when senior management may be implicated.

Independence is the central consideration. An investigation overseen by people whose own conduct is in question, or who have a strong interest in a particular outcome, will lack credibility with regulators, courts and employees, however competent the investigators.

Defining the scope

The scope of a corporate investigation sets out what it will and will not examine. Too narrow a scope can leave obvious questions unanswered and invite the suspicion that the company did not want to know. Too broad a scope can make the investigation slow, expensive and unfocused.

A useful scope statement covers:

- the conduct alleged or suspected;
- the people, business units, locations and time period to be examined;
- the questions the investigation must answer;
- the sources of evidence to be reviewed, such as email, financial systems and devices;
- who will receive the findings and in what form;
- how the scope may be changed if new issues emerge.

Regulators look closely at scope. The Department of Justice asks whether a company's investigations are properly scoped and independent, and whether they identify root causes and systemic issues rather than stopping at the individual wrongdoer (U.S. Department of Justice, 2023). A scope limited to "whether employee X broke the rules" may be adequate for a simple policy breach but not for a scheme that required others to look away.

The investigation process

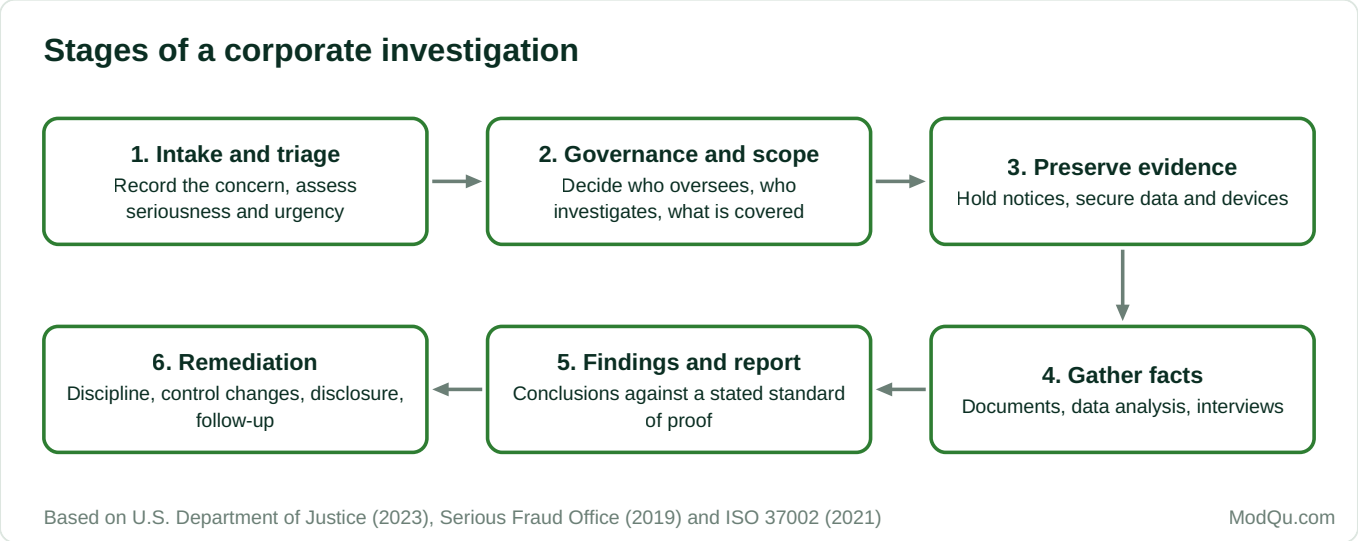


Figure 2. The main stages of a corporate investigation. Evidence preservation should begin as soon as the matter is assessed as credible, often before the scope is final. Diagram by ModQu.

Intake and triage. Reports arrive through hotlines, managers, auditors, regulators, customers and the media. Each should be logged and assessed for credibility, seriousness and urgency. Guidance on whistleblowing management systems recommends a consistent triage process, with clear criteria for deciding which reports need investigation (International Organization for Standardization [ISO], 2021).

Governance and scope. For serious matters, the organisation decides who will oversee the investigation, who will carry it out and how findings will be reported. Conflicts of interest should be identified and managed.

Preserve evidence. Documents, emails, chat messages and devices should be secured before the people involved are alerted. Legal hold notices instruct employees not to delete relevant material. Failure to preserve evidence can itself become a serious issue with regulators.

Gather facts. Investigators review documents, analyse data and interview witnesses and subjects. Interviews should follow fair procedures, give the subject an opportunity to respond to the evidence and be properly recorded.

Findings and report. The investigation reaches conclusions on each question in its scope, stating the evidence relied on and the standard of proof applied, usually the balance of probabilities in employment matters.

Remediation. The organisation decides on discipline, recovery of losses, changes to controls, training, disclosure to regulators or law enforcement, and communication with those affected. The Department of Justice expects remediation to address root causes, not just individuals (U.S. Department of Justice, 2023).

A worked example

The stages are easier to see in a single case. The following example is hypothetical and simplified, but it follows a pattern common in practice.

A regional sales director at a manufacturing company receives an anonymous message through the company hotline. It says that a sales manager in one overseas office has been paying a local "consultant" to win public contracts, and that the consultant passes part of the money to officials. The allegation is specific, it names a person and a type of payment, and if true it would expose the company to liability under anti-bribery law. It is classed as serious.

Because the allegation involves possible bribery of public officials, the general counsel takes charge and reports the matter to the audit committee. External lawyers are appointed so that the work is carried out under legal privilege, and a forensic accounting firm is engaged to analyse payments. The scope statement asks four questions: what payments were made to the consultant, what services were provided in return, who approved the payments, and whether similar arrangements exist in other offices.

Before anyone in the overseas office is told, the IT team preserves email accounts, chat logs and shared drives for the people named, and finance secures the vendor master file and payment records. The forensic accountants then find that the consultant was paid a success fee of eight per cent on each contract won, that invoices described the services only as "market advisory", and that the payments were approved by the sales manager and by a finance officer who later said she had relied on the sales manager's assurances. Due diligence on the consultant had never been completed.

Interviews come next. Witnesses in finance and procurement are interviewed first, and the sales manager last, so that the questions can be based on the documents. The sales manager is told who the lawyers represent, is shown the key documents and is given the chance to explain them. The account offered is that the consultant provided genuine local knowledge and that any payments onward were unknown to the manager.

The report sets out what was established and what was not. On the balance of probabilities, the payments were not supported by evidence of real services, the approval controls had failed, and the sales manager had ignored warning signs. The investigation could not establish where the consultant's money went, because the company had no access to the consultant's bank records. The board decides to dismiss the sales manager, to terminate the consultant, to retrain the finance staff, to require completed due diligence before any intermediary is paid, and to consider self-reporting to the relevant authorities. A review of intermediaries in other offices is added as a second phase. This last step reflects the regulatory expectation that an investigation looks beyond the individual to the system that allowed the conduct (U.S. Department of Justice, 2023).

Interviews and fairness to subjects

Interviews are often the most sensitive part of a corporate investigation. Fair procedure therefore depends on the organisation's own policies and on employment law rather than on criminal rules. Guidance for workplace investigations in the United Kingdom recommends that the person under investigation be told of the allegations in enough detail to respond, be given reasonable notice of an interview, and, where policy allows, be accompanied (Acas, 2019).

Order matters. Interviewing documentary witnesses and peripheral staff first allows the investigator to understand the facts before speaking to the subject, and to put specific evidence to the subject rather than general suspicions. The subject should be given a genuine opportunity to answer each point, and the answer should be checked rather than simply recorded. Where lawyers conduct the interview, the Upjohn warning should be given at the start and recorded in the notes, since a misunderstanding about whom the lawyer represents can later undermine both privilege and fairness (*Upjohn Co. v. United States*, 1981).

Reporting the findings

The form of the final report depends on its audience and purpose. A report to the board may be a full written account with appendices of evidence. A report prepared under legal privilege may be delivered orally or as a short summary to avoid waiving privilege. A report that will be published, as some board-level reports have been, must be written with the expectation that every sentence will be read by regulators, litigants and the press.

Whatever the form, a good report separates findings of fact from opinions and recommendations, states the standard of proof applied to each finding, explains which evidence was decisive and why conflicting evidence was rejected, and records the limits of the investigation, such as documents that could not be obtained or witnesses who declined to cooperate. Stating what was not established is as important as stating what was.

Disclosure decisions follow. Depending on the jurisdiction and the conduct, the organisation may need to decide whether to report to a regulator or prosecutor, to notify affected customers or employees, or to make a public statement. These decisions carry legal consequences and are usually taken by the board on legal advice. Prosecutors in several countries give credit to companies that self-report promptly and cooperate fully (Serious Fraud Office, 2019; U.S. Department of Justice, 2023).

Legal constraints

Corporate investigators operate under significant legal limits. They have no power to compel non-employees to cooperate or to search private property. Their access to employees' communications and personal data is governed by employment law, contracts and data protection law, including the General Data Protection Regulation in Europe (Regulation (EU) 2016/679, 2016). Employees who report concerns are protected against retaliation in many jurisdictions, and in the United States the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 created financial awards for whistleblowers who report securities violations to the regulator. Where criminal conduct is suspected, investigators must take care not to prejudice a possible police or prosecutor investigation, for example by alerting suspects or contaminating witness accounts (Serious Fraud Office, 2019).

Culture and reporting

The effectiveness of corporate investigation depends on whether problems are reported in the first place. Dyck et al. (2010), studying fraud at large United States companies, found that employees were among the most important sources of detection, ahead of external auditors and regulators. Yet employees often stay silent. Research on whistleblowing shows that people are more likely to report when they believe the organisation will act on the report and protect them

from retaliation (Miceli et al., 2008). Kaplan and Schultz (2007) found that the availability of an anonymous reporting channel affected people's intentions to report, and Edmondson's (1999) research on psychological safety shows that teams in which people feel safe to raise concerns learn more from errors.

How investigations are handled shapes that belief. Employees who see that reports lead to fair, competent and timely investigations, and that people who report are protected, are more likely to speak up next time. Employees who see reports ignored, leaked or used against the reporter will stay silent. Treviño et al. (2006) review evidence that ethical behaviour in organisations depends heavily on the signals that leaders and systems send, and investigations are among the most visible of those signals.

Understanding why misconduct occurs also matters. Soltes (2016), who interviewed dozens of convicted white-collar offenders, argues that many did not weigh costs and benefits at all but acted on intuition in environments where their conduct had come to seem normal. Investigations that ask how the conduct came to seem acceptable, and not only who was responsible, produce more useful remediation.

What makes an investigation credible

Drawing on regulatory guidance and practice, several features distinguish a credible corporate investigation from a defensive exercise:

1. **Independence.** The people overseeing and conducting the investigation are free from conflicts of interest and from pressure to reach a particular result.
2. **Competence.** Investigators have the skills required, including interviewing, forensic accounting, data analysis and knowledge of the relevant law.
3. **Appropriate scope.** The scope matches the seriousness of the allegations and is expanded when evidence warrants it.
4. **Evidence preservation.** Relevant material is secured promptly and completely.
5. **Fairness.** Subjects are told of the allegations and given a real opportunity to respond; witnesses are protected.
6. **Documentation.** The work is recorded well enough to be reviewed by a regulator or court.
7. **Root cause analysis.** The investigation asks how the conduct was possible and why it was not detected sooner.
8. **Follow-through.** Findings lead to action, and the action is checked.

Standards and guidance increasingly reflect these expectations, including the anti-bribery management system standard ISO 37001 (ISO, 2016) and guidance on internal fraud control (Wells, 2017).

Conclusion

Corporate investigations are a core function of modern organisations, not an occasional response to scandal. They establish facts, meet legal duties, manage regulatory exposure, protect people and reveal weaknesses that can be fixed. Their value depends on independence, competence, fairness and a willingness to follow the evidence wherever it leads, including towards senior people and systemic failures. Organisations that treat investigation as a disciplined process for generating reliable knowledge about themselves, rather than as a way to manage embarrassment, are better placed to prevent the next problem and to be believed when they say they have dealt with the last one.

References

Acas. (2019). *Conducting workplace investigations*. Advisory, Conciliation and Arbitration Service.

Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. https://www.acfe.com/RTTN

Bribery Act 2010, c. 23 (UK).

Coffee, J. C., Jr. (2020). *Corporate crime and punishment: The crisis of underenforcement*. Berrett-Koehler.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control — Integrated framework*. COSO.

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. (2019). *Official Journal of the European Union, L 305*, 17–56.

Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

Dyck, A., Morse, A., & Zingales, L. (2010). Who blows the whistle on corporate fraud? *The Journal of Finance, 65*(6), 2213–2253. https://doi.org/10.1111/j.1540-6261.2010.01614.x

Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly, 44*(2), 350–383. https://doi.org/10.2307/2666999

Garrett, B. L. (2014). *Too big to jail: How prosecutors compromise with corporations*. Harvard University Press.

Independent Directors of the Board of Wells Fargo & Company. (2017). *Sales practices investigation report*. Wells Fargo & Company.

Institute of Internal Auditors. (2024). *Global internal audit standards*. The IIA.

International Organization for Standardization. (2016). *Anti-bribery management systems — Requirements with guidance for use* (ISO Standard No. 37001:2016).

International Organization for Standardization. (2021). *Whistleblowing management systems — Guidelines* (ISO Standard No. 37002:2021).

Kaplan, S. E., & Schultz, J. J. (2007). Intentions to report questionable acts: An examination of the influence of anonymous reporting channel, internal audit quality, and setting. *Journal of Business Ethics, 71*(2), 109–124. https://doi.org/10.1007/s10551-006-0021-6

Miceli, M. P., Near, J. P., & Dworkin, T. M. (2008). *Whistle-blowing in organizations*. Routledge.

Powers, W. C., Jr., Troubh, R. S., & Winokur, H. S., Jr. (2002). *Report of investigation by the Special Investigative Committee of the Board of Directors of Enron Corp*. Enron Corp.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union, L 119*, 1–88.

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002).

Serious Fraud Office. (2019). *Corporate co-operation guidance*. SFO.

Soltes, E. (2016). *Why they do it: Inside the mind of the white-collar criminal*. PublicAffairs.

Treviño, L. K., Weaver, G. R., & Reynolds, S. J. (2006). Behavioral ethics in organizations: A review. *Journal of Management, 32*(6), 951–990. https://doi.org/10.1177/0149206306294258

Upjohn Co. v. United States, 449 U.S. 383 (1981).

U.S. Department of Justice. (2023). *Evaluation of corporate compliance programs*. Criminal Division.

Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection* (5th ed.). Wiley.