The International Comparative Legal Guide to:

Corporate Investigations 2019

3rd Edition

A practical cross-border insight into corporate investigations

Published by Global Legal Group, with contributions from:

Allen & Gledhill LLP
Arthur Cox
AZB & Partners
Bär & Karrer Ltd.
BCL Solicitors LLP
Blake, Cassels & Graydon LLP
Bloomfield Law Practice
Borenius Attorneys Ltd
De Pedraza Abogados, S.L.P.
De Roos & Pen
Debevoise & Plimpton LLP
Dechert LLP
Durrieu Abogados S.C.
Esenyel|Partners Lawyers & Consultants
Felsberg Advogados
Gilbert + Tobin
Hammarskiöld & Co
Kammeradvokaten/Poul Schmith
Kirkland & Ellis International LLP
Lee and Li, Attorneys-at-Law
Morgan, Lewis & Bockius LLP
Navigant Consulting, Inc.
Norton Rose Fulbright
Norton Rose Fulbright South Africa Inc
PLMJ
Rahman Ravelli
Sołtysiński Kawecki & Szlęzak
Stibbe
ŠunjkaLaw
Wikborg Rein

glg
global legal group

global legal group

Contributing Editors
Neil Gerrard & David Kelley, Dechert LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Rachel Williams
Caroline Collingwood

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
January 2019

ISBN 978-1-912509-50-8
ISSN 2398-5623

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

England & Wales

Michael Drury

Richard Reichman

BCL Solicitors LLP

1 The Decision to Conduct an Internal Investigation

1.1 What statutory or regulatory obligations should an entity consider when deciding whether to conduct an internal investigation in your jurisdiction? Are there any consequences for failing to comply with these statutory or regulatory regulations? Are there any regulatory or legal benefits for conducting an investigation?

Although there are no explicit statutory or regulatory obligations pertaining to commencing internal investigations in England and Wales, it is often in an entity's best interests to conduct an internal investigation when wrongdoing is suspected, whether this be criminal or regulatory. This will enable an entity to identify if any criminal offences or regulatory breaches may have been committed at an early stage and to make informed decisions. An obvious benefit of an internal investigation is that it allows the entity to satisfy itself that it has isolated and dealt with the wrongdoing. Additionally, conducting an internal investigation may help an entity decide whether or not to approach a relevant authority with a view to securing a more favourable outcome than would likely be the case having been approached by the authorities in the first instance.

1.2 How should an entity assess the credibility of a whistleblower's complaint and determine whether an internal investigation is necessary? Are there any legal implications for dealing with whistleblowers?

Consideration should be given to whether there is likely to be any other evidence capable of supporting the whistleblower's assertions, such as documentary evidence and the extent to which the whistleblower can personally verify the allegation made. An entity should also consider the context and circumstances in which the whistleblower makes their disclosure; for example, even if they are a disgruntled employee, is the disclosure capable of belief? How much time has passed since the events occurred and what is the explanation for any delay? Is the whistleblower raising the matter for their own personal gain or motive?

A statutory framework exists to protect workers if they blow the whistle on their employer; a whistleblower who makes a qualifying disclosure has the right not to be subjected to any detriment by any act or deliberate failure to act by their employer on the ground that the worker has made a protected disclosure.

1.3 How does outside counsel determine who "the client" is for the purposes of conducting an internal investigation and reporting findings (e.g. the Legal Department, the Chief Compliance Officer, the Board of Directors, the Audit Committee, a special committee, etc.)? What steps must outside counsel take to ensure that the reporting relationship is free of any internal conflicts? When is it appropriate to exclude an in-house attorney, senior executive, or major shareholder who might have an interest in influencing the direction of the investigation?

"The client" will often be determined by who has retained the services of outside lawyers and who has control of the internal investigation. The client should be suitably qualified and hold sufficient seniority within the entity to be in a position to provide instruction, direction and make critical tactical decisions about the course and scope of the investigation and any reporting that may occur. The wider the reporting relationship is, the more difficult it is likely to be for the corporate to assert and maintain privilege, and also to preserve confidentiality. Entities are best advised to set up an investigation team comprising a limited number of individuals. For more complex investigations, it is often advisable to set up a management or steering committee as these create very clear reporting lines.

External counsel should make enquiries of the client to satisfy itself that those to whom they are to report are not conflicted – this can be done through, for instance, considering the nature of the allegations to be investigated and who is likely to hold relevant information, and asking those who conceivably have been involved in the matter under investigation to declare any interests. These steps are intended to have the effect of maintaining the credibility of any investigation results with the regulator.

2 Self-Disclosure to Enforcement Authorities

2.1 When considering whether to impose civil or criminal penalties, do law enforcement authorities in your jurisdiction consider an entity's willingness to voluntarily disclose the results of a properly conducted internal investigation? What factors do they consider?

Voluntary disclosure of the results of an internal investigation is an important factor considered by authorities in determining

whether a prosecution is in the public interest, or whether a Deferred Prosecution Agreement (DPA) or civil settlement (or other alternative to prosecution) is appropriate. However, it provides no guarantee that a prosecution will not follow. Instead, it will form part of a case-by-case analysis looking at a range of factors, including the seriousness of the offence, the harm to victims and any history of similar misconduct by the entity.

2.2 When, during an internal investigation, should a disclosure be made to enforcement authorities? What are the steps that should be followed for making a disclosure?

There are a number of scenarios when entities must notify regulators of incidents/misconduct. For example, the General Data Protection Regulation (GDPR) requires that breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data must be reported to the Information Commissioner's Office (ICO) not later than 72 hours after the controller of the data becomes aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned. Similarly, the Financial Conduct Authority (FCA) requires its regulated firms to be open and cooperative, and, for example, to notify the regulator of anything about which it would reasonably expect notice. The Health and Safety Executive (HSE) must be notified of reportable safety incidents under the RIDDOR requirements and entities can be required to notify the Environment Agency of pollution incidents, etc.

Generally, details of any wrongdoing discovered during an internal investigation do not automatically need to be disclosed to enforcement authorities. Prior to any self-report, an entity should carefully consider the desirability and potential consequences (e.g. civil and criminal sanctions). Voluntary disclosure before enforcement authorities are involved may be desirable if the entity is considering cooperating with the authorities in an attempt to achieve a more favourable outcome. It is clear from the *Rolls-Royce* case that failure to self-report is not a barrier to a DPA as long as there are counterbalancing factors, notably complete cooperation and disclosure of materials without pre-conditions (including assertions of legal professional privilege) thereafter. If this is a strategy an entity wants to pursue, wrongdoing should be reported to enforcement authorities within a reasonable time of the offending coming to light.

However, when an investigation report is being prepared, there is an incentive to ensure that a detailed investigation has been undertaken before disclosure of the facts. It is an unattractive proposition to provide details of an internal investigation in haste and without a proper understanding of the conduct, not least because the nature of the wrongdoing may not be apparent until the latter stages of an investigation.

2.3 How, and in what format, should the findings of an internal investigation be reported? Must the findings of an internal investigation be reported in writing? What risks, if any, arise from providing reports in writing?

There is no requirement to provide voluntary disclosure of investigation findings in a specific format, such as in writing, rather than an oral briefing. It is a matter for the entity to decide on the extent and format of any disclosure made. A written report will undoubtedly be viewed more favourably in the context of any enforcement action given it demonstrates cooperation and is likely to contain a more complete examination of the relevant issues and underlying facts with evidential value.

However, there are risks associated with written reports. A report may contain findings or information that are potentially damaging. By disclosing a written report to law enforcement authorities, an entity runs the risk that the information contained in it will be used to open an investigation into the company. Moreover, a written report is open to misinterpretation or misuse, which may be avoided if the results of an internal investigation are presented orally instead.

Ultimately, however, any investigating authorities to whom matters are to be reported will expect materials in writing to be retained and may serve statutory production orders to compel its provision. Any oral report provided will likely be swiftly followed for a request from the enforcement agency for a written report of the same.

3 Cooperation with Law Enforcement Authorities

3.1 If an entity is aware that it is the subject or target of a government investigation, is it required to liaise with local authorities before starting an internal investigation? Should it liaise with local authorities even if it is not required to do so?

Entities are not required to liaise with law enforcement authorities before starting an internal investigation but there are benefits to such early engagement and it is viewed favourably and encouraged by them. For instance, if an agency is given the opportunity to comment on the proposed scope and purpose of an investigation then the entity can ensure its report is appropriate. Early engagement may also avoid risks associated with tipping off and "trampling on the crime scene". However, an entity should remain cautious about disclosing information about wrongdoing without first having a proper understanding of the nature or extent of the alleged misconduct. To do so may result in an inappropriate or inaccurate self-report which is not in the interests of any party involved.

3.2 If regulatory or law enforcement authorities are investigating an entity's conduct, does the entity have the ability to help define or limit the scope of a government investigation? If so, how is it best achieved?

Regulators have extensive statutory powers to gather evidence as part of their investigation; for example, to compel entities to answer questions or produce documents.

Engagement with a regulator may help to define or limit the scope of its investigation; guidance can be given regarding the relevance of material and the proportionality of requests for information and documentation.

3.3 Do law enforcement authorities in your jurisdiction tend to coordinate with authorities in other jurisdictions? What strategies can entities adopt if they face investigations in multiple jurisdictions?

The global nature of today's businesses, combined with the increasing availability of extraterritorial statutory powers to obtain evidence and extraterritorial offences, means that jurisdictional issues are becoming more prevalent. Law enforcement authorities in the UK frequently share information with authorities in other jurisdictions through mutual legal assistance agreements or via organisations such as Eurojust, and there are increasing numbers of truly joint investigations by agencies from different states.

Where an entity faces investigation in multiple countries, attention should be given in particular to the rules of privilege that operate in other jurisdictions and the location of evidence or material and any data protection implications, especially for data held within the EU. Entities may consider challenging the extent of a regulator's powers, subject to their intention to cooperate. The recent judgment in *R* (*KBR Inc.) v SFO* confirmed the extraterritorial scope of the SFO's power to compel the production of documents under s.2 of the Criminal Justice Act 1987, in relation to overseas companies with a "*sufficient connection*" to the UK. In addition, the Crime (Overseas Production Orders) Bill is currently making its way through Parliament, which may lead to wider overseas production powers in relation to electronic data. Such statutory powers may reduce the current reliance on mutual legal assistance to obtain evidence from outside the jurisdiction.

4 The Investigation Process

4.1 What steps should typically be included in an investigation plan?

All investigations are different and planning must be approached on a bespoke basis and kept under review. The investigation plan will generally define the subject and scope of the investigation as well as the roles and responsibilities of the investigation team. It may include an outline of what tasks are to be performed, with timelines and rules of engagement (e.g. to preserve confidentiality and privilege).

The investigation plan should ensure that all relevant material is identified, collected and preserved, which will include securing hard copy data and electronic data. How the investigation team will review the data and which individuals should be interviewed will also need to be determined.

4.2 When should companies elicit the assistance of outside counsel or outside resources such as forensic consultants? If outside counsel is used, what criteria or credentials should one seek in retaining outside counsel?

A decision whether to use outside counsel or resources should be made with reference to the nature of the alleged misconduct, the issues to be determined, the kind of expertise required and the relevant experience of the intended resource. In circumstances where government intervention is likely, the independence of outside counsel who can attest to the validity of decisions made or procedures used and do so without being hampered by internal company politics is likely to enhance the credibility of the end result of the investigation.

In the event that non-lawyer experts are used, e.g. forensic accountants, clear rules should be established to ensure that communications back to the client maintain legal privilege as far as possible. This will ensure that, provided the investigation can be properly conducted within the confines of legal professional privilege, the investigation can proceed without the concern that the entity will be required to provide material generated during the investigation to the authorities.

5 Confidentiality and Attorney-Client Privileges

5.1 Does your jurisdiction recognise the attorney-client, attorney work product, or any other legal privileges in the context of internal investigations? What best practices should be followed to preserve these privileges?

Legal professional privilege falls into two categories: (i) legal advice privilege; and (ii) litigation privilege. Briefly, (i) legal advice privilege attaches to communications between a client and a lawyer in connection with the giving of legal advice; and (ii) litigation privilege attaches to documents created for the dominant purpose of conducting existing or reasonably contemplated adversarial litigation.

The availability of litigation privilege has been scrutinised in a number of cases and, most recently, the Court of Appeal in *SFO v ENRC* overturned a High Court decision which had held that criminal litigation was in prospect at a much later stage than had widely been understood previously. The availability of litigation privilege continues to need to be carefully considered on a fact-specific basis, rather than assuming blanket protection, and may be a factor affecting whether an investigation is desirable and, if so, when and how it is carried out. Evidence should be recorded, for example what litigation was in contemplation and why, to support any subsequent claim.

5.2 Do any privileges or rules of confidentiality apply to interactions between the client and third parties engaged by outside counsel during the investigation (e.g. an accounting firm engaged to perform transaction testing or a document collection vendor)?

As above, litigation privilege may apply to documentation prepared in relation to reasonably contemplated litigation and any communications with third parties would be subject to rules of confidentiality. The use of third parties should be carefully considered and care should be taken to ensure that their work is protected by legal privilege – generally by ensuring instruction is through external counsel appointed to advise on and/or handle the internal investigation – and that measures are in place to guard against inappropriate disclosure.

5.3 Do legal privileges apply equally whether in-house counsel or outside counsel direct the internal investigation?

In short, the answer is yes, except in cases relating to European Union law (typically cartels or anti-corruption cases) where in-house lawyers cannot claim legal professional privilege over internal communications with employees. Although in-house counsel are inevitably closer to the business than external counsel, in the context of legal privilege, the "client", i.e. the corporate entity, is the same and legal privilege applies equally to any communications/material generated during the course of an internal investigation. However, claims of privilege will be easier and clearer if external counsel are instructed as, purely as a matter of perception, they are distinct from the business.

5.4 How can entities protect privileged documents during an internal investigation conducted in your jurisdiction?

All legally privileged material created during the course of an investigation should be marked appropriately (e.g. "*Confidential – Subject to Legal Professional Privilege*") and treated to ensure that privilege is maintained (e.g. not inappropriately disclosed beyond the client team internally or externally).

Legally privileged documents uncovered during an investigation, either produced in the course of obtaining legal advice or in the course of separate litigation, should be separately stored and marked (e.g. "*Legally Privileged*").

5.5 Do enforcement agencies in your jurisdictions keep the results of an internal investigation confidential if such results were voluntarily provided by the entity?

Enforcement agencies will keep the results of any internal investigation confidential unless there is a requirement to share it with another agency or regulator. The same entity may be under investigation for criminal offences whilst simultaneously being under investigation (by a different entity) for regulatory breaches. The extent to which agencies will share information is dependent on their particular memoranda of agreement but there are statutory gateways permitting such exchanges. Before providing any material, it would be prudent for the corporate to consider the risks of onward disclosure and liaise with the enforcement agency as necessary.

6 Data Collection and Data Privacy Issues

6.1 What data protection laws or regulations apply to internal investigations in your jurisdiction?

Any internal investigation needs to respect the requirements of the GDPR and additional provisions applicable under the Data Protection Act 2018. On that basis, "personal data" (broadly data from which a living individual can be identified) needs to be accorded its proper protection under the law and processed lawfully, taking into account the rights of the data subject (the person whom the data identifies) and the lawful bases of processing under the GDPR whilst ensuring the integrity, security and confidentiality of the data at issue. There are exemptions to certain requirements where legal professional privilege is concerned or where regulatory functions or the prevention and detection of crime is engaged.

6.2 Is it a common practice or a legal requirement in your jurisdiction to prepare and issue a document preservation notice to individuals who may have documents related to the issues under investigation? Who should receive such a notice? What types of documents or data should be preserved? How should the investigation be described? How should compliance with the preservation notice be recorded?

Issuing a retention requirement (also known as a "hold notice") for individuals who are (or have been) under confidentiality obligations to the entity undertaking the investigation is generally considered best practice. It is to be anticipated that to the extent that the individual has documents that pertain to the business affairs of the entity they will already be under a legal obligation to hold them subject to the rights of the entity itself. The policies of the entity as to the use and retention of electronic data on media not owned by it for processing data belonging to it (and knowledge about how such policies operated in fact), as well as to the rules concerning the retention of hard copy material, will provide crucial information as to what material might exist. Necessarily, a requirement to preserve materials will require some information to be imparted about the circumstances in which preservation is to take place. That should be sufficient to allow informed retention choices but without disclosing specific details that would give rise to an increased risk of destruction.

6.3 What factors must an entity consider when documents are located in multiple jurisdictions (e.g. bank secrecy laws, data privacy, procedural requirements, etc.)?

Data protection and bank secrecy laws in other jurisdictions remain a key element for consideration, especially as to whether relevant data can be transferred across national borders for the purposes of internal investigations. Well-informed expert (internal or external) counsel qualified in the relevant jurisdiction should be consulted before data is secured and in anticipation of any transfer. Particular care should be taken in relation to data transfers to non-EEA countries where the provisions of Chapter V of the GDPR become relevant. The Privacy Shield principles agreed between the EU and US in 2016 apply where personal data is sent from Europe to the US. Consideration should be given not only to the transfer of data but also to the facts elicited from the data themselves in the form of summaries and reports, etc.

6.4 What types of documents are generally deemed important to collect for an internal investigation by your jurisdiction's enforcement agencies?

Tradition has it that emails provide the most interesting and pertinent evidence. That is no longer true given the increasing variety of social media which are used for communications and which evidence an individual's state of mind and actions taken. It follows that not only should servers holding emails and other electronic data be retained and imaged by experienced professional and independent third parties employed to do so or to oversee the actions of internal staff (who in doing so will meet the necessary standards for preservation of material to evidential standards for the purposes of litigation), but attempts should be made to secure portable electronic devices where storage of relevant data may be on the device itself. Contact with service providers is also important in seeking to retain material held or stored by them that might otherwise not remain in existence because of its ephemeral nature.

6.5 What resources are typically used to collect documents during an internal investigation, and which resources are considered the most efficient?

As above, the employment of an experienced computer forensics team is vital both in demonstrating the integrity and thoroughness of the internal investigation. It is prudent for such a team (perhaps using different team members) to catalogue the material retained and put in place relevant search tools to enable examination of the data (in copy format, preserving a "clean" original version). Liaison with internal and external counsel is crucial and provides an efficient basis for understanding what has happened in the investigation and why the particular steps were taken in it, with a view to being able to explain the scope and integrity of the work undertaken to enforcement authorities that may become engaged.

6.6 When reviewing documents, do judicial or enforcement authorities in your jurisdiction permit the use of predictive coding techniques? What are best practices for reviewing a voluminous document collection in internal investigations?

The volume of electronic material generated in any business means that the review of this material in hard copy format is no longer feasible. Enforcement authorities and lawyers engaged in internal investigations will always use document review platforms (e.g. "Relativity") to search for and review relevant material. Data obtained, usually by imaging the electronic devices, is uploaded on to the review platform in a searchable format so that keyword searches can be run across the data. This process identifies the relevant material for review.

AI-based processing (e.g. deduplication and "threading" of emails to identify the most inclusive email chains for review) and predictive coding (applying human coding decisions to a larger data set) are becoming more frequently used in order to make reviews of large volumes of data manageable. There is nothing about the use of such methods to prevent the material being used or found to be admissible in subsequent proceedings: admissibility questions are dependent to a large extent on the nature of the documents themselves not the means by which they are discovered.

7 Witness Interviews

7.1 What local laws or regulations apply to interviews of employees, former employees, or third parties? What authorities, if any, do entities need to consult before initiating witness interviews?

Although current employees will be expected, by virtue of the terms of their contracts of employment, to comply with internal investigations, former employees or third parties may be more difficult to interview as there is no threat of disciplinary proceedings for failing to cooperate with the entity's internal investigation.

Ordinarily, the authorities do not need to be consulted before initiating witness interviews, save that it may be prudent to do so in cases where the authorities have already been notified that an internal investigation is afoot (for example, where a self-report has been made).

7.2 Are employees required to cooperate with their employer's internal investigation? When and under what circumstances may they decline to participate in a witness interview?

Employees cannot be compelled to attend an investigation interview, but failing to attend or cooperate with an investigation without reasonable excuse may mean that they are acting in breach of relevant duties towards their employer. A failure to attend an interview may therefore lead to disciplinary proceedings being brought against that employee.

7.3 Is an entity required to provide legal representation to witnesses prior to interviews? If so, under what circumstances must an entity provide legal representation for witnesses?

An entity is not required to provide legal representation to witnesses, although a witness cannot be prevented from seeking legal advice. However, the entity retains the control of the investigation and so it may determine who can or cannot attend internal investigation interviews, i.e. lawyers for the witness can be prevented from attending. If an entity is considering providing legal representation, careful thought must be given to the attendant costs and delays that this may entail; in some circumstances, an entity's Directors & Officers insurance policy may provide for legal fees for certain witnesses, but thought should be given to the overall fairness if only some employees are provided with legal representation by the entity.

7.4 What are best practices for conducting witness interviews in your jurisdiction?

Interviewers should, where possible, be consistent so as to avoid any difficulties when comparing and contrasting different accounts. A variation of the "Upjohn Warning" should be provided to interviewees at the commencement of an interview, namely: a warning that tells the interviewee that the lawyers involved are advising the entity and not the individual interviewee; a brief explanation of the background of the investigation; a request to be clear when the interviewee is making a statement of fact or is speculating or stating a belief; and to remind the interviewee of the need for confidentiality and not to discuss matters with their colleagues or senior management. A record of the interview should be made in the form of a summary of the key facts rather than a *verbatim* transcript.

7.5 What cultural factors should interviewers be aware of when conducting interviews in your jurisdiction?

There may be a culture at an entity of suppressing information or frowning upon whistleblowing. Each interviewee should be encouraged to answer questions to the best of their ability, and questioning should not take the form of a hostile interrogation. Such practices will help an interviewer obtain relevant information where the culture of the entity may otherwise inhibit interviewees. It should be borne in mind that employees may be reluctant to share information or be truthful for reasons independent to the internal investigation, such as concern for job security. Adopting a sensitive approach may reduce the likelihood of this occurring.

7.6 When interviewing a whistleblower, how can an entity protect the interests of the company while upholding the rights of the whistleblower?

Provided an entity can demonstrate that it has not discriminated against the whistleblower because of their disclosure (see question 1.2 above), it is unlikely that it can be said to have breached the whistleblower's rights. It is imperative that the investigation team is comprised of individuals who are completely independent from the areas of the business which are the subject of the investigation as this demonstrates that the concerns raised by the whistleblower are being taken seriously and thoroughly investigated. The entity should clarify in any interview with a whistleblower that its lawyers are acting for the entity and not the individual, but also make it clear that the entity is aware of the whistleblower's status and that their disclosure is protected.

7.7 Can employees in your jurisdiction request to review or revise statements they have made or are the statements closed?

Any information provided during the course of an internal

investigation, usually through a fact-finding meeting, can be presented to the employee for verification. As stated at question 7.4 above, a record of any meeting should be made in the form of a summary of the key facts rather than a *verbatim* transcript.

7.8 Does your jurisdiction require that enforcement authorities or a witness' legal representative be present during witness interviews for internal investigations?

There is no requirement that the enforcement authorities or a witness' legal representative are present for witness interviews in these circumstances.

Where a self-report has been made or there has otherwise been a level of coordination with any authority, the entity will wish to consider liaising with the authority (and may have been requested to do so following the self-report) regarding the conduct of witness interviews. The investigating authority may well wish to interview individuals before the internal investigation interviews have commenced, in which case the internal interviews may have to be deferred or abandoned.

Companies engaging in cooperative self-reporting, for example with a view to obtaining a DPA, may find themselves under pressure to waive privilege in relation to existing interview notes, or, if there has been early engagement, encouraged to progress any ongoing interviews in a way which ensures that they are not protected by legal privilege.

8 Investigation Report

8.1 How should the investigation report be structured and what topics should it address?

Before producing a written investigation report, consideration may be given to whether the key findings should be presented orally to the client. It may be that an oral report is all that is required and this will avoid creating a report/record over which arguments as to privilege may then arise – in addition, the ability to circulate an oral presentation is limited (although board minutes recording such presentations should make clear where appropriate the parts of any board meeting subject to legal professional privilege).

A written investigation report will usually contain an introduction (describing the background to the investigation), a summary of the relevant regulatory regime or circumstances in which the misconduct arises, details of the investigative steps and findings and a summary of any improvements or remedial action which has been taken.

Acknowledgment

The authors would like to acknowledge the invaluable contributions of their colleagues Julian Hayes and Natasha Sammy in the preparation of this chapter.

Michael Drury
BCL Solicitors LLP
51 Lincoln's Inn Fields
London, WC2A 3LZ
United Kingdom

Tel: +44 207 430 2277
Email: mdrury@bcl.com
URL: www.bcl.com

Michael Drury was formerly Director for Legal Affairs at GCHQ before joining BCL as a partner in 2010. He has specific expertise in national security cases (he is developed vetted) and in cases with high-profile political dimensions. His expertise in foreign relations, his experience advising a corporate client as an in-house lawyer at GCHQ and his background in serious fraud mean that he is particularly well suited to dealing with matters in corporate crime, whether acting for individuals or corporates. Having conducted inquiries both in government and for clients at BCL, he is well placed to lead multi-disciplinary teams and produce investigation strategies. He is ranked in Band 3 in *Chambers 2017 Financial Crime: Individuals.*

Richard Reichman
BCL Solicitors LLP
51 Lincoln's Inn Fields
London, WC2A 3LZ
United Kingdom

Tel: +44 207 430 2277
Email: rreichman@bcl.com
URL: www.bcl.com

Richard Reichman is a partner specialising in corporate crime, financial crime and regulatory investigations. He is recommended by *The Legal 500* for his "*extensive experience*" and being "*extremely thorough and appreciat[ing] the big picture issues".*

He has experience in a broad range of regulatory offences, such as health and safety (generally following major or fatal incidents), environmental, food safety, fire safety and trading, as well as financial offences such as fraud, bribery, insider dealing and money laundering. Richard is involved in cases involving cybercrime (for example, computer-specific offences such as hacking) or a technological dimension. He has acted for victims of cybersecurity breaches and advises regarding data protection issues falling within the scope of the Information Commissioner's Office.

Before joining BCL, Richard trained and qualified into a leading national firm before moving to an international firm, gaining comprehensive experience in complex, high-value and multi-jurisdictional matters.

BCL Solicitors LLP

BCL is a market-leading law firm specialising in domestic and international corporate crime, financial crime, regulatory enforcement, AML/ABC compliance and general crime.

The firm is top-ranked by *The Legal 500* and *Chambers and Partners*, the two leading directories of legal services ranking the best law firms and lawyers in the world.

Many of our lawyers are also recognised sector leaders, and comprise expert litigators and advocates drawn from specialist criminal law firms and barristers' chambers, commercial law firms, key positions in the main prosecuting authorities and the Government Legal Service.

BCL provides discreet, effective and expert advice to corporations, governments, public bodies, public figures, senior executives and high-net-worth individuals.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com